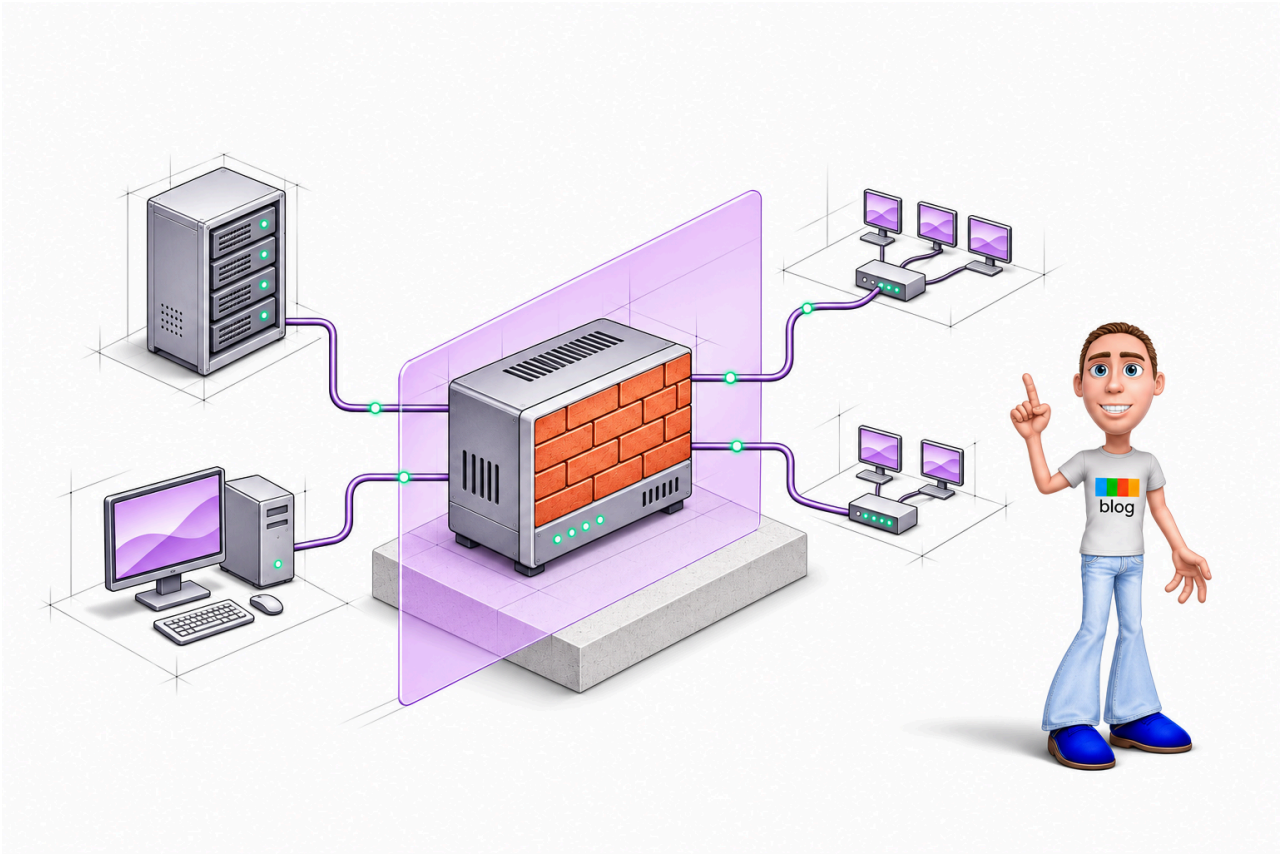
PALENTINO.ES

Manual técnico y práctico
para el software pfSense® Plus

Administración por menús y pantallas

Configuración · Supervisión · Diagnóstico



Óscar de la Cuesta Campillo

palentino.es

105 capítulos · 8 partes

Publicación independiente sin afiliación ni respaldo de Netgate o ESF

Primera edición · Noviembre de 2026

Créditos y autoría

Óscar de la Cuesta Campillo

Ingeniero Informático · Autor de palentino.es

Soy autor de palentino.es, donde comparto contenidos sobre sistemas, redes, programación, seguridad e inteligencia artificial. En este libro he elegido una organización de consulta que acompaña al administrador ante cada menú, formulario y herramienta de diagnóstico.

Autor y dirección editorial

Óscar de la Cuesta Campillo. Selección del enfoque práctico, organización de la obra y dirección editorial.

Web y perfil profesional

Blog: https://www.palentino.es/

LinkedIn: https://www.linkedin.com/in/oscardelacuesta

Edición e ilustraciones

Redacción y maquetación asistidas por herramientas de inteligencia artificial. Personaje de portada: imagen facilitada por el autor. Ilustración de portada: composición creada con asistencia de IA para esta edición a partir de ese personaje.

Derechos sobre esta edición

© 2026 Óscar de la Cuesta Campillo, por sus aportaciones originales y la edición de esta obra. Los contenidos y marcas de terceros conservan sus propios titulares y condiciones de uso; la atribución del libro no los incorpora a los derechos del autor.

Referencia bibliográfica sugerida

De la Cuesta Campillo, Óscar (2026). Manual técnico y práctico para el software pfSense Plus. Publicación independiente. Primera edición.

Marcas y derechos de terceros

Esta publicación es una obra independiente de formación y consulta. No está publicada, patrocinada, certificada ni avalada por Electric Sheep Fencing LLC, Rubicon Communications LLC o Netgate.

Menciones de marcas

pfSense® es una marca registrada de Electric Sheep Fencing LLC. Netgate® es una marca registrada de Rubicon Communications LLC. Las demás denominaciones de productos pertenecen a sus respectivos titulares y se utilizan para identificar las tecnologías tratadas.

El nombre del software identifica el objeto de estudio. La portada emplea una ilustración creada para esta edición y no utiliza los logotipos oficiales de pfSense ni de Netgate. La presencia de una marca en el texto no expresa una relación comercial, una certificación ni una recomendación de su titular.

Fuentes y materiales

La documentación de Netgate y las demás fuentes técnicas se identifican en los capítulos mediante enlaces a sus páginas originales. Las denominaciones de campos, los comandos y los mensajes de interfaz se conservan cuando resultan necesarios para explicar una función. Los esquemas y ejemplos tienen finalidad didáctica.

Las marcas, la interfaz, el software y los materiales externos conservan sus derechos y sus licencias. Su mención o enlace no transfiere derechos sobre ellos. La cita de una fuente no sustituye los permisos que pueda exigir la reproducción de sus textos, imágenes o código.

Alcance técnico

La información debe contrastarse con la versión instalada y la documentación vigente. Los ejemplos de redes y configuraciones son didácticos y no describen una infraestructura real. Las pruebas y las acciones de administración deben realizarse sobre equipos y redes propios o para los que se disponga de autorización.

Referencias para estas menciones

Política de marcas del proyecto pfSense

Marcas y directrices de Netgate

Texto refundido de la Ley de Propiedad Intelectual

Referencias de las políticas y normas consultadas el 18 de noviembre de 2026.

Presentación

Este es un libro técnico y práctico organizado por los menús y pantallas del software pfSense® Plus. Lo he preparado para consultarlo mientras se administra un firewall: localizar una función, comprender sus controles, decidir qué cambiar y comprobar el resultado.

El recorrido consta de 105 capítulos distribuidos en ocho partes. Abarca la administración del sistema, las interfaces, el firewall, los servicios, las VPN, las vistas de estado, las herramientas de diagnóstico y la ayuda. Cada capítulo se centra en un apartado de la interfaz y permite volver a él cuando aparece una duda concreta.

La práctica se desarrolla campo a campo y tarea a tarea. Las explicaciones relacionan el valor de una opción con sus efectos, sus dependencias y las comprobaciones que ayudan a validar un cambio. Las tablas permiten comparar controles y resultados; los procedimientos muestran cómo abordar situaciones habituales de administración.

Los fundamentos técnicos aparecen donde hacen falta para tomar una decisión. Al estudiar una regla se explica el tráfico al que afecta; al revisar una VPN se conectan negociación, rutas y permisos; al utilizar una herramienta de diagnóstico se delimita qué demuestra su salida y qué pruebas siguen siendo necesarias.

Se puede leer el libro de forma ordenada o acudir directamente al capítulo relacionado con una pantalla. El índice conserva los nombres de los menús y enlaza con los capítulos. Para una incidencia conviene revisar también los componentes relacionados, ya que el origen del problema puede encontrarse fuera del formulario abierto.

El manual está dirigido a administradores de sistemas y redes, responsables de IT, técnicos de soporte, integradores y estudiantes con conocimientos básicos de direccionamiento IP. El objetivo es que el lector pueda realizar una tarea con criterio, interpretar lo que observa y verificar las consecuencias de su intervención.

Los ejemplos son didácticos y las referencias permiten ampliar o contrastar la explicación. La combinación de consulta, práctica y verificación es el método de trabajo que da sentido a esta obra.

Prefacio

He concebido este manual como una herramienta de trabajo. Al administrar un firewall, la duda suele aparecer delante de una opción concreta: qué valor corresponde introducir, qué efecto tiene una casilla o qué significa el estado que presenta un servicio. Para responder con criterio hace falta comprender el contexto de esa pantalla y sus relaciones con el resto del sistema.

Por esa razón, el libro está organizado por apartados de la interfaz. Los capítulos desarrollan las funciones que el administrador encuentra en su recorrido por los menús. Los fundamentos técnicos acompañan a las decisiones prácticas, y las comprobaciones permiten contrastar lo configurado con lo que realmente ocurre en la red.

Me interesa especialmente que la lectura ayude a distinguir observación e interpretación. Un indicador es una evidencia dentro de un contexto. Antes de convertirlo en un diagnóstico conviene saber desde dónde se ha medido, qué componente lo produce y qué otras comprobaciones son necesarias. Esta forma de trabajar aparece en los capítulos de configuración y resulta esencial en Status y Diagnostics.

El mismo criterio se aplica a los cambios. Ajustar una interfaz, modificar una regla o actuar sobre un servicio puede afectar a comunicaciones que no se ven en el formulario abierto. Los procedimientos deben leerse completos y relacionarse con el diseño de la red, las dependencias de la función y la posibilidad de recuperar el acceso si el resultado no es el esperado.

He procurado mantener las denominaciones de los menús y campos para que el lector pueda orientarse en la interfaz, acompañándolas de explicaciones en español. La organización favorece la consulta de un problema concreto sin perder de vista los capítulos relacionados. Las referencias técnicas permiten ampliar la lectura y comprobar diferencias entre versiones.

Este enfoque exige práctica. Leer un apartado ayuda a entender una función; comprobarla en un entorno adecuado permite reconocer sus resultados y sus límites. El valor de un manual técnico está en facilitar ese trabajo con información clara, procedimientos comprensibles y pruebas que permitan evaluar lo ocurrido.

Óscar de la Cuesta Campillo

Introducción

El software pfSense® Plus reúne funciones de firewall, encaminamiento y servicios de red que se administran desde una interfaz web. La operación de esa plataforma requiere relacionar configuraciones y resultados: las interfaces definen conectividad, las rutas determinan caminos, las reglas condicionan el tráfico y los servicios añaden funciones de infraestructura.

El manual aborda esos elementos siguiendo los menús y pantallas. Cada capítulo delimita una función y la conecta con las tareas que permite realizar. El orden de los capítulos es una organización de consulta; no constituye una secuencia que deba ejecutarse de principio a fin sobre un equipo en producción.

Configuración

Los capítulos de System, Interfaces, Firewall, Services y VPN explican parámetros y decisiones de diseño. Antes de aplicar un procedimiento conviene identificar qué comunicaciones dependen de la función y qué pruebas permitirán verificar el resultado.

Supervisión

Status permite observar servicios, interfaces, registros y métricas. Sus vistas aportan contexto operativo y ayudan a localizar el componente que requiere una investigación más concreta. Algunos controles de estas páginas ejecutan acciones de mantenimiento; deben distinguirse de la consulta de información.

Diagnóstico

Diagnostics reúne herramientas para investigar direcciones, rutas, procesos, estados y paquetes. Sus resultados deben interpretarse desde el origen de la prueba, la familia IP, el protocolo y el período de observación. Una prueba aislada rara vez valida por completo un servicio.

Versiones y plataforma

Los controles disponibles pueden cambiar según la versión de pfSense Plus, el hardware y los paquetes instalados. Las referencias de cada capítulo ayudan a contrastar esos cambios. Una función descrita en documentación de otra edición o versión debe verificarse antes de trasladarla al sistema administrado.

Entornos y datos de ejemplo

Los ejemplos de direccionamiento, nombres y topologías son didácticos. No describen una instalación real ni deben copiarse como un diseño universal. Cuando se utilizan direcciones o identificadores, su función es permitir comprender el procedimiento manteniendo la confidencialidad de cualquier infraestructura.

Cómo utilizar este manual

Consultar por pantalla

Localizar el menú y el nombre de la función en el índice. Los títulos mantienen la nomenclatura de la interfaz para facilitar el acceso. La numeración de capítulos permite relacionar el índice con las explicaciones y con las referencias entre apartados.

Leer el alcance antes de actuar

Comprobar qué resuelve la función y qué queda fuera de su alcance. Una vista vacía, un servicio deshabilitado o un campo que no aparece pueden responder a la configuración existente. La ausencia de un elemento no debe interpretarse automáticamente como una avería.

Relacionar opciones y dependencias

Revisar los capítulos de los componentes relacionados. Una VPN depende de rutas y reglas; un servicio de nombres puede requerir comprobar el DNS del cliente y del firewall por separado; una publicación NAT necesita validar el recorrido externo y su retorno.

Verificar con pruebas pertinentes

Definir qué resultado se espera y desde qué origen se debe comprobar. Comparar la configuración con registros, estados, capturas y pruebas de aplicación cuando corresponda. Registrar las condiciones de las mediciones permite comparar resultados sin confundir escenarios distintos.

Preparar cambios recuperables

Antes de una acción que pueda interrumpir comunicaciones, revisar las indicaciones del capítulo, conservar la configuración necesaria y prever una vía de recuperación. La verificación posterior debe cubrir el servicio afectado y el acceso administrativo.

Usar las referencias

Los enlaces de cada capítulo permiten ampliar conceptos y contrastar procedimientos. Las condiciones de soporte, los requisitos de una función y la información de versiones deben consultarse en sus fuentes vigentes cuando afecten a una decisión operativa.

Convenciones

Las rutas de menú se representan con el signo →. Los nombres de campos se conservan en su idioma de interfaz cuando ayudan a localizarlos. Los comandos y salidas se presentan con tipografía monoespaciada. Las ilustraciones explican estructuras y relaciones; no constituyen una reproducción de una infraestructura concreta.

Índice general

Consulta por menús y funciones. Las entradas enlazan con los capítulos.

Créditos y autoría 2

Marcas y derechos de terceros 3

Presentación 4

Prefacio 5

Introducción 6

Cómo utilizar este manual 7

Parte I Orientación y administración del sistema 11

01 Pantalla principal y Dashboard 11
02 System → Advanced → Admin Access 18
03 System → Advanced → Netgate Nexus 27
04 System → Advanced → Firewall & NAT 34
05 System → Advanced → Networking 45
06 System → Advanced → Miscellaneous 53
07 System → Advanced → System Tunables 62
08 System → Advanced → Notifications 71
09 System → Boot Environments 80
10 System → Certificates → Authorities 88
11 System → Certificates → Certificates 95
12 System → Certificates → Revocation 102
13 System → General Setup 107
14 System → High Availability 113
15 System → Package Manager → Installed Packages 120
16 System → Package Manager → Available Packages 127
17 System → Register 136
18 System → Routing → Gateways 141
19 System → Routing → Static Routes 148
20 System → Routing → Gateway Groups 154
21 Setup Wizard → Bienvenida 161
22 System → Update 165
23 System → User Manager 171

Parte II Interfaces 177

24 Interfaces → Introducción general 177
25 Interfaces → Assignments 181
26 Interfaces → Switch 196
27 Interfaces → WAN 208
28 Interfaces → LAN 220
29 Interfaces → WAN secundaria 232

Parte III Firewall 244

30 Firewall → Introducción general 244
31 Firewall → Aliases 254
32 Firewall → NAT 265
33 Firewall → Packet Flow Data 277
34 Firewall → Rules 287

35 Firewall → Schedules....300
36 Firewall → Traffic Shaper....308
37 Firewall → Virtual IPs....319

Parte IV Services....329

38 Services → Introducción general....329
39 Services → Auto Configuration Backup....339
40 Services → Captive Portal....349
41 Services → DHCP Relay....359
42 Services → DHCP Server....368
43 Services → DHCPv6 Relay y DHCPv6 Server....379
44 Services → DNS Forwarder....389
45 Services → DNS Resolver....400
46 Services → Dynamic DNS....412
47 Services → IGMP Proxy....422
48 Services → NTP....432
49 Services → PPPoE Server....444
50 Services → Router Advertisement....454
51 Services → SNMP....464
52 Services → UPnP IGD & PCP....473
53 Services → Wake-on-LAN....483

Parte V VPN....492

54 VPN → Introducción general....492
55 VPN → AWS VPC VPN Wizard....503
56 VPN → IPsec....513
57 VPN → IPsec Export: Apple Profile....526
58 VPN → IPsec Export: Windows PowerShell....534
59 VPN → L2TP....544
60 VPN → OpenVPN....553
61 VPN → WireGuard....569

Parte VI Status....580

62 Status → Introducción general....580
63 Status → Captive Portal....590
64 Status → CARP (failover)....599
65 Status → Dashboard....609
66 Status → DHCP Leases....620
67 Status → DHCPv6 Leases....629
68 Status → DNS Resolver....639
69 Status → Filter Reload....649
70 Status → Gateways....657
71 Status → Interfaces....665
72 Status → IPsec....674
73 Status → Monitoring....684
74 Status → NTP....694
75 Status → OpenVPN....703
76 Status → Queues....711
77 Status → Services....719
78 Status → System Logs....727
79 Status → Traffic Graph....736
80 Status → UPnP IGD & PCP....743

Parte VII Diagnostics....751
81 Diagnostics → Introducción general....751
82 Diagnostics → ARP Table....758
83 Diagnostics → Authentication....764
84 Diagnostics → Backup & Restore....772
85 Diagnostics → Command Prompt....781
86 Diagnostics → Edit File....788
87 Diagnostics → Factory Defaults....794
88 Diagnostics → Halt System....802
89 Diagnostics → Limiter Info....809
90 Diagnostics → NDP Table....816
91 Diagnostics → Packet Capture....824
92 Diagnostics → pfInfo....833
93 Diagnostics → pfTop....843
94 Diagnostics → Ping....852
95 Diagnostics → Reboot....860
96 Diagnostics → Routes....868
97 Diagnostics → S.M.A.R.T. Status....876
98 Diagnostics → Sockets....883
99 Diagnostics → States....891
100 Diagnostics → States Summary....899
101 Diagnostics → System Activity....906
102 Diagnostics → Tables....913
103 Diagnostics → Test Port....920
104 Diagnostics → Traceroute....929
Parte VIII Help....937
105 Help....937

Parte I Orientación y administración del sistema

01 Pantalla principal y Dashboard

El Dashboard es la pantalla principal de la interfaz web de pfSense Plus y la primera vista de trabajo para comprobar el estado general del firewall. Reúne paneles denominados widgets que muestran información sobre el sistema, la red y los servicios. Se pueden añadir, retirar, minimizar y mover para ajustar el área de supervisión.

OBJETIVO DE ESTA PANTALLA
Interpretar los indicadores antes de modificar nada: saber qué se ve, qué significa, qué no demuestra y a qué apartado acudir para obtener una respuesta más precisa.

1.1. Ubicación de los elementos

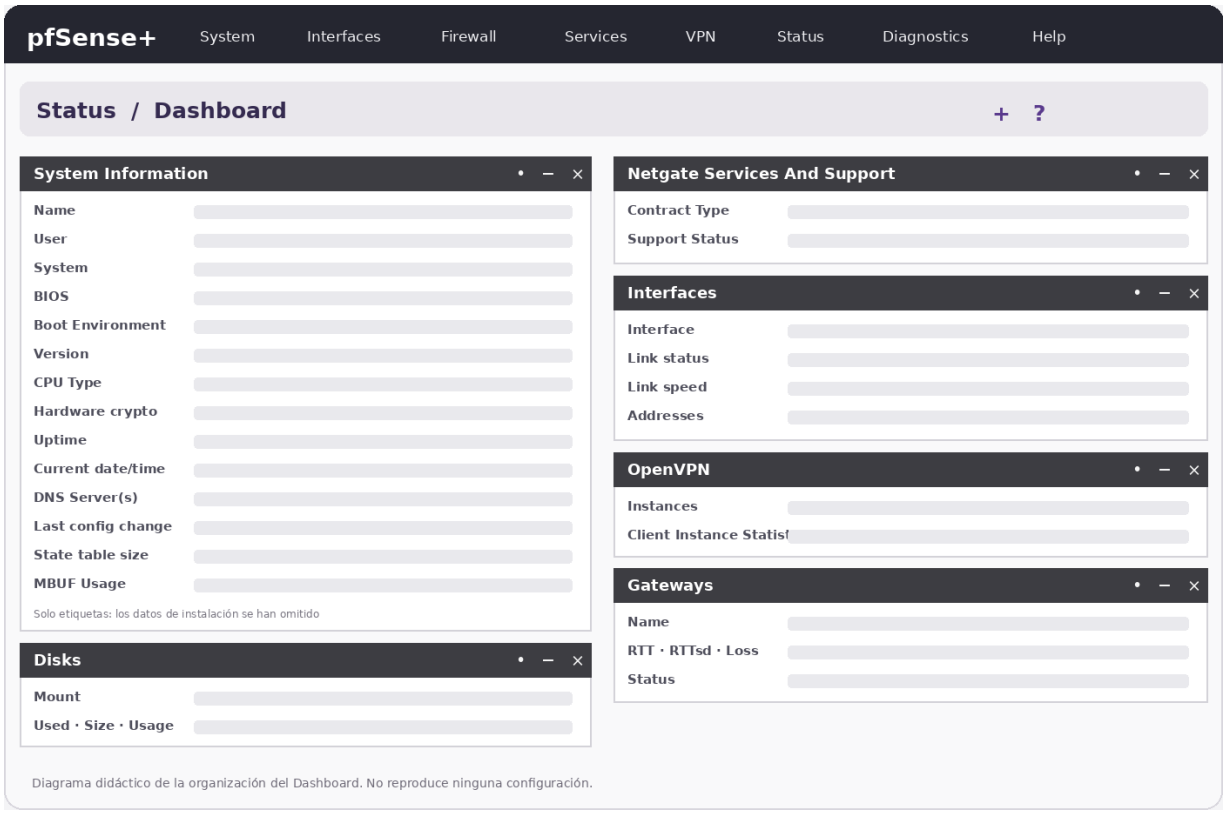


Figura 1. Organización del Dashboard y distribución de sus widgets principales. Representación esquemática sin valores de configuración.

1.1.1. Barra superior de navegación

El menú superior agrupa las áreas principales: System (administración), Interfaces (conectividad), Firewall (filtrado y NAT), Services (servicios de red), VPN (túneles), Status (supervisión), Diagnostics (diagnóstico) y Help (ayuda). El conjunto exacto de opciones depende de la versión y de los componentes disponibles.

1.1.2. Ruta de navegación y controles

La franja superior del contenido identifica la ubicación “Status / Dashboard”. El símbolo + abre la lista de widgets disponibles. Cada panel dispone de controles propios para configurarlo, minimizarlo o retirarlo del área de trabajo, según lo permitido por ese widget.

1.2. System Information

Este widget resume la identidad lógica del firewall, su software y varios indicadores operativos. Reúne datos descriptivos (que cambian poco) y métricas de funcionamiento (que varían en el tiempo). Su lectura no debe confundirse con una prueba global de conectividad.

1.2.1. Identificación, software y arranque

Campo	Qué representa	Para qué sirve
Name	Nombre completo configurado del sistema.	Identificar el equipo al gestionar múltiples dispositivos.
User	Cuenta que está viendo la interfaz y origen de autenticación.	Confirmar la sesión administrativa que se está usando.
System	Tipo de plataforma o equipo reconocido; puede incluir identificadores del dispositivo.	Reconocer hardware o entorno virtual, sin publicar identificadores.
BIOS	Información del firmware de arranque, si se obtiene.	Relacionar características de plataforma con soporte y diagnóstico.
Boot Environment	Entorno ZFS desde el que se ha iniciado y previsto para el próximo arranque, si es compatible.	Revisar entornos de arranque y recuperación.
Version	Versión del software, arquitectura, compilación, sistema base y aviso de actualización.	Planificar compatibilidad y mantenimiento; no actualizar sin evaluar el impacto.

Nota sobre Boot Environment. Si este campo no aparece, no debe deducirse que existe un fallo: su presencia depende del soporte de entornos ZFS. Un entorno elegido para el próximo arranque puede no coincidir con el que está ejecutándose en ese momento.

1.2.2. Procesamiento y criptografía

Campo	Lectura	Advertencia
CPU Type	Modelo, arquitectura, núcleos o procesadores lógicos, según plataforma.	Es una descripción, no un indicador de rendimiento por sí solo.
Hardware crypto	Algoritmos y capacidades criptográficas acelerables por hardware.	La presencia de una capacidad no significa que todas las VPN la utilicen.
Uptime	Tiempo transcurrido desde el último arranque.	Un reinicio inesperado requiere correlación con registros y mantenimiento.

1.2.3. Tiempo, DNS y configuración

Campo	Interpretación práctica
Current date/time	Fecha, hora y zona horaria del firewall. Deben ser coherentes para analizar registros y eventos.
DNS Server(s)	Servidores DNS configurados u obtenidos automáticamente para el propio sistema. Que aparezcan listados no prueba que resuelvan correctamente.
Last config change	Momento del último cambio registrado en la configuración. Ayuda a investigar incidencias aparecidas tras una modificación.

1.2.4. Recursos y estados

Indicador	Qué mide	Cómo interpretarlo
State table size	Estados de conexiones almacenados frente al máximo configurado.	Un valor cercano al límite requiere investigar sesiones, tráfico y dimensionamiento.
MBUF Usage	Uso de búferes de memoria de la pila de red.	La proximidad al límite puede revelar presión sobre recursos de red.
Load Average	Carga media del sistema en varios intervalos.	Es una señal de trabajo acumulado, no un porcentaje de CPU.
CPU usage	Porcentaje de tiempo de CPU utilizado.	Importan los picos repetidos y la carga sostenida; la vista del panel también consume recursos.

Indicador	Qué mide	Cómo interpretarlo
Memory usage	Memoria utilizada por el sistema.	Debe interpretarse considerando cachés y comportamiento real, no solo el porcentaje.
Swap usage	Memoria de intercambio, cuando exista.	Un uso persistente acompañado de lentitud puede indicar presión de memoria.
Temperature	Lectura térmica, si el hardware la ofrece.	La disponibilidad del sensor depende del dispositivo.

1.2.5. Qué comprobar antes de actuar

La identidad del sistema, la versión instalada y el tiempo desde el último reinicio.

La coherencia de fecha y hora cuando se investigan registros.

Si la carga, la memoria, los MBUF y los estados muestran presión sostenida, no solamente un instante aislado.

Si la actualización anunciada está aprobada para el entorno; la existencia de un aviso no obliga a actualizar en ese momento.

ERROR QUE DEBE EVITARSE
No interpretar una barra de CPU o memoria aislada como diagnóstico definitivo. Confirmar tendencias, registros y experiencia de los usuarios antes de cambiar parámetros.

1.3. Netgate Services and Support

Este widget informa sobre el estado del soporte asociado al equipo y ofrece referencias de asistencia de Netgate. Su contenido puede variar en función del dispositivo y del contrato.

Elemento	Significado	Utilidad
Contract Type	Modalidad de soporte reconocida para la instancia.	Conocer el alcance de asistencia disponible.
Support Status	Situación de soporte comunicada por el servicio correspondiente.	Comprobar si existen condiciones de soporte vigentes.
Actualización del panel	Consulta o refresco de información de servicio.	Revisar datos mostrados sin confundirlos con monitorización WAN.

Un estado de soporte favorable no significa que el tráfico o las conexiones del firewall funcionen correctamente. Se trata de información administrativa y de servicio.

1.4. Interfaces

Resume las interfaces asignadas al firewall. La pantalla detallada para profundizar es Status → Interfaces. Este widget diferencia el tipo/nombre de interfaz, el estado del enlace, su velocidad negociada y las direcciones asociadas cuando aparecen disponibles.

Elemento	Qué indica	Qué NO demuestra
Nombre de interfaz	La etiqueta lógica configurada para un puerto o interfaz.	No garantiza que corresponda a una toma física concreta sin verificar asignación.
Indicador de enlace	Si existe o no enlace según el dispositivo y controlador.	No prueba acceso a Internet ni a una aplicación.
Velocidad / dúplex	Condiciones negociadas con el extremo de red, si hay datos.	No representa la velocidad real de una conexión a Internet.
Direcciones	Información de direccionamiento asociada a la interfaz.	No garantiza que exista ruta de ida y vuelta hacia otros destinos.

Ventaja principal. Detectar de un vistazo una interfaz sin enlace o una negociación que merece revisión. Si la conectividad falla con el enlace activo, el siguiente paso es observar gateways, rutas, DNS y reglas.

1.5. OpenVPN

El widget OpenVPN muestra el estado de las instancias configuradas, tanto de servidor como de cliente. Según el modo de conexión, puede presentar sesiones activas, nombres de instancias, horas de conexión y datos de conexión remota. Estos elementos no deben reproducirse en materiales publicados.

Campo / área	Qué significa	Uso práctico
Instancia	Túnel o servicio OpenVPN configurado.	Saber qué servicio se está supervisando.
Client Instance Statistics	Información resumida de la instancia cliente, si corresponde.	Observar estado y datos de la sesión.
Remote/Virtual IP	Direcciones del extremo remoto o de la red virtual, si aparecen.	Investigar conectividad sin publicar dichas direcciones.
Indicador de estado	Estado comunicado para la instancia o sesión.	Realizar una primera comprobación de continuidad.

DISTINCIÓN FUNDAMENTAL
VPN activa ≠ servicio remoto accesible. Un túnel establecido puede coexistir con rutas incorrectas, bloqueos de firewall o problemas en el destino.

1.6. Gateways

El widget Gateways resume los resultados de monitorización de las puertas de enlace. Es especialmente valioso para diferenciar un enlace físico activo de una ruta que parece disponible desde el punto de observación configurado.

Columna	Significado	Lectura correcta
Name	Nombre lógico del gateway.	Identifica el objeto monitorizado, no el proveedor real por sí mismo.
RTT	Tiempo de ida y vuelta de las pruebas hacia el destino monitorizado.	Latencia de esa ruta de comprobación, no de toda Internet.
RTTsd	Desviación estándar del tiempo de respuesta.	Indica variación de latencia; valores más altos sugieren inestabilidad.
Loss	Porcentaje de pérdida de paquetes de las pruebas.	Una pérdida puede venir de la ruta, del destino o de limitaciones de ICMP.
Status	Resultado del estado de supervisión del gateway.	Debe contrastarse con una prueba funcional real.

1.6.1. Estados y situaciones

Estado visible	Interpretación prudente	Siguiente paso
Online	La monitorización considera disponible la puerta de enlace.	Probar tráfico real y DNS si los usuarios tienen problemas.
Warning	Se han alcanzado condiciones de aviso de la supervisión.	Revisar RTT, variación y pérdida, y comprobar persistencia.
Down / Offline	La supervisión ha declarado una condición de indisponibilidad.	Revisar monitor, interfaz, ruta y conectividad del destino.
Unknown / Pending / Gathering Data	El panel aún no dispone de un estado concluyente o está recopilando información.	Esperar la lectura y revisar el detalle; no asumir una caída.

Las denominaciones concretas pueden variar con la versión y el contexto. Para el diagnóstico completo, consultar Status → Gateways y las herramientas de Diagnostics.

Multi-WAN. Un gateway considerado disponible no garantiza por sí solo que la conmutación por error esté bien diseñada: intervienen grupos de gateways, prioridades, monitorización y reglas de política de enrutamiento.

1.7. Disks

Este widget presenta capacidad, espacio usado y distribución del almacenamiento local. Según el sistema de archivos puede incluir puntos de montaje y conjuntos de datos ZFS expandibles.

Campo	Función	Ventaja práctica
Mount	Punto de montaje o elemento de almacenamiento.	Localizar la ubicación cuyo uso se revisa.
Used	Espacio ocupado.	Detectar crecimiento anómalo.
Size	Capacidad del volumen o conjunto de datos.	Contextualizar el consumo.
Usage	Relación entre ocupado y total, normalmente en barra o porcentaje.	Advertir presión sobre almacenamiento antes de agotar espacio.

Cuando el almacenamiento se aproxima a su capacidad, pueden verse afectados registros, tareas de mantenimiento o actualizaciones. La investigación debe identificar el origen del consumo antes de eliminar archivos.

1.8. Personalizar la pantalla principal

Los widgets son elementos de presentación y supervisión. Ocultar un widget no deshabilita el servicio que representa. Esta separación permite reorganizar la pantalla sin alterar el funcionamiento del firewall.

1.8.1. Añadir un widget

Abrir Status → Dashboard.

Pulsar + en los controles de la franja superior.

Elegir el nombre del widget en la lista de disponibles.

Comprobar que aparece en el Dashboard; recolocarlo si es necesario.

Guardar la distribución cuando aparezca el control de guardar.

1.8.2. Mover o cambiar la visualización

Control	Acción	Efecto
Barra de título	Arrastrar y soltar en otra posición o columna.	Cambia solamente la disposición del panel.
Llave de herramientas	Abrir ajustes cuando el widget disponga de ellos.	Modifica cómo se muestra o actualiza ese widget.
Símbolo −	Minimizar el contenido del panel.	Deja visible su cabecera sin eliminarlo.
Símbolo + del widget minimizado	Expandirlo de nuevo.	Recupera su visualización.
Símbolo ×	Quitar el widget del Dashboard.	No detiene el servicio subyacente.
Guardar distribución	Conservar la nueva organización.	Mantiene los cambios de presentación.

Según la configuración de usuario y versión, el número de columnas y otras preferencias del Dashboard pueden gestionarse desde System → General Setup o mediante opciones del perfil de usuario.

1.9. Ejercicio de lectura sin modificar la configuración

Este ejercicio consiste en interpretar los indicadores del Dashboard sin modificar la configuración. Debe realizarse en un entorno autorizado y sin registrar ni compartir identificadores internos, direcciones u otros datos sensibles.

Acceder a Status → Dashboard y reconocer las áreas de navegación.

Identificar en System Information qué elementos son estáticos y cuáles cambian con el tiempo.

Distinguir el estado del enlace de Interfaces del estado de monitorización de Gateways.

Localizar los datos que expresan carga o consumo de recursos y evitar conclusiones por una lectura aislada.

Comprobar si hay widgets de servicios que requieran supervisión especial, sin publicar sus identificadores.

Localizar los controles para añadir, minimizar y quitar widgets; no reiniciar servicios ni alterar reglas.

Cerrar el ejercicio redactando solamente observaciones técnicas generales, sin exportar datos del dispositivo.

1.10. Diagnóstico inicial: tres preguntas importantes

1.10.1. ¿Hay enlace, pero no servicio?

Si una interfaz indica enlace activo, verificar primero el estado del gateway correspondiente; después comprobar resolución de nombres, rutas y reglas. El Dashboard orienta la investigación, pero la prueba del servicio debe realizarse con herramientas adecuadas.

1.10.2. ¿La VPN figura conectada, pero no hay acceso?

Diferenciar la existencia del túnel del acceso de extremo a extremo. Investigar rutas de ambos lados, redes anunciadas, reglas de firewall, traducción de direcciones cuando corresponda y disponibilidad del destino.

1.10.3. ¿Aparece un recurso alto?

No intervenir solo por el color de una barra. Observar persistencia, revisar registros y correlacionar con síntomas. Es preferible confirmar la causa que aplicar ajustes a ciegas.

1.11. Errores frecuentes

Interpretación incorrecta	Interpretación adecuada
“La interfaz está Up: Internet funciona”.	El enlace es solo una parte de la conectividad; hay que probar gateway, DNS y destino.
“La VPN muestra una sesión: todo el tráfico pasa”.	El túnel puede estar activo y fallar las rutas o reglas.
“Hay memoria ocupada: falta RAM”.	Es necesario evaluar caché, swap y comportamiento del sistema.
“Un gateway Pending significa que está caído”.	Ese estado puede indicar falta temporal de datos suficientes.
“Quitar el widget desactiva el servicio”.	Quitar el widget modifica la vista, no la ejecución del servicio.
“Hay una actualización: debo aplicarla inmediatamente”.	La actualización requiere planificación, copia de seguridad y evaluación de compatibilidad.

1.12. Lista de verificación

☐ Reconozco la navegación superior y la ruta Status → Dashboard.

☐ Sé localizar los seis widgets tratados en este capítulo.

☐ Puedo explicar RTT, RTTsd, Loss, State table size y MBUF Usage.

☐ Distingo datos de soporte, estado del enlace y supervisión de conectividad.

☐ Sé añadir y reorganizar widgets sin confundirlo con cambios de servicio.

☐ No he copiado ni publicado información de ninguna instalación.

1.13. Resumen del capítulo

La pantalla principal es una herramienta de observación. Aporta contexto y permite decidir qué revisar primero, pero no sustituye las pruebas de conectividad, los registros ni las páginas detalladas de estado. La calidad de la administración depende de relacionar los indicadores en lugar de confiar en una única cifra o icono.

El método empleado a lo largo de esta obra consiste en localizar cada función, comprender sus opciones, valorar sus ventajas y comprobar las consecuencias reales de su uso. La explicación técnica se mantiene separada de los datos particulares de cualquier instalación.

Fuentes técnicas consultadas

Dashboard — Netgate Documentation
https://docs.netgate.com/pfsense/en/latest/monitoring/dashboard.html

Available Widgets — Netgate Documentation
https://docs.netgate.com/pfsense/en/latest/monitoring/dashboard-widgets.html

Managing Widgets — Netgate Documentation
https://docs.netgate.com/pfsense/en/latest/monitoring/dashboard-manage.html

Gateway Status — Netgate Documentation
https://docs.netgate.com/pfsense/en/latest/monitoring/status/gateways.html

Boot Environment Status — Netgate Documentation
https://docs.netgate.com/pfsense/en/latest/backup/zfsbe/status.html

CLAVE DE APRENDIZAJE
El Dashboard constituye una vista de supervisión. Para confirmar la causa de una incidencia, sus indicadores deben contrastarse con las páginas de estado, los registros y las herramientas de diagnóstico correspondientes.

02 System → Advanced → Admin Access

Control de acceso web, SSH, protección de inicios de sesión y consola local.

Esta pantalla concentra parámetros que afectan directamente a la disponibilidad y seguridad de las vías de administración del firewall. Conocer la función de cada campo evita cambios innecesarios y permite recuperar el acceso ante una incidencia.

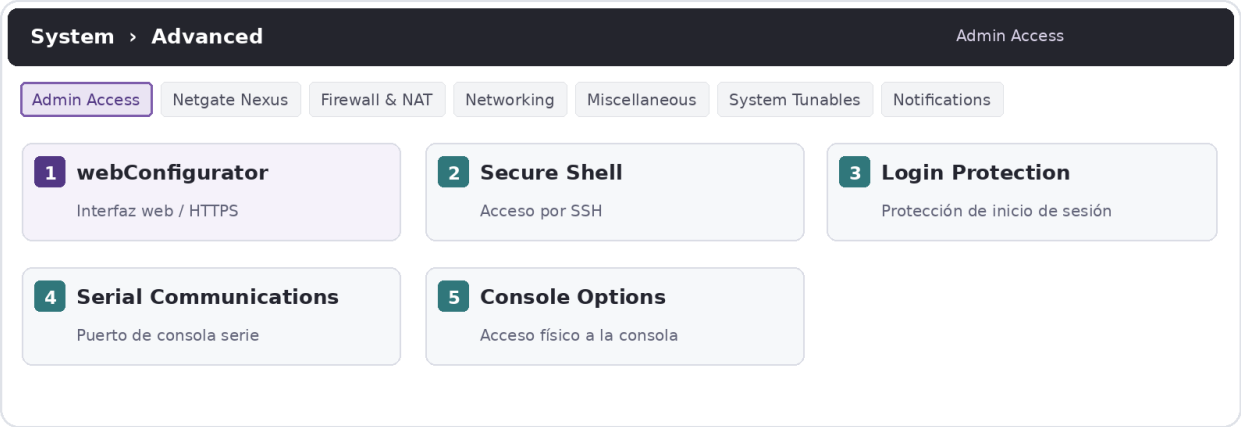


Figura 2.1. Organización de System → Advanced y sus cinco bloques de Admin Access. Esquema funcional, no captura de una instalación.

ADVERTENCIA IMPORTANTE Modificar el protocolo, el puerto o las reglas de acceso puede cerrar una sesión activa o impedir nuevas conexiones. Antes de aplicar cambios de acceso, mantener disponible un método alternativo de administración, preferiblemente la consola local, y guardar una copia de la configuración.

Qué permite hacer esta pantalla

Elegir cómo se accede a la interfaz web y qué certificado protege la conexión.

Habilitar SSH y determinar cómo autentican los usuarios autorizados.

Regular la respuesta frente a intentos repetidos de inicio de sesión fallidos.

Ajustar parámetros de consola serie y proteger el menú de consola.

2.1. Ubicación y pestañas relacionadas

Se accede desde el menú principal System → Advanced y, dentro de esta página, seleccionando la pestaña Admin Access. Las otras pestañas agrupan configuraciones independientes: no deben confundirse con campos de esta pantalla.

Pestaña	Ámbito
Admin Access	Acceso y mecanismos de administración. Es el contenido de este capítulo.
Netgate® Nexus	Funciones asociadas a Nexus, según disponibilidad y licencia.
Firewall & NAT	Parámetros avanzados del filtrado y de la traducción de direcciones.
Networking	Ajustes avanzados del funcionamiento de red.
Miscellaneous	Opciones generales adicionales del sistema.
System Tunables	Parámetros ajustables del sistema operativo.
Notifications	Mecanismos y preferencias de notificación.

2.2. webConfigurator: administración mediante navegador

webConfigurator es la interfaz gráfica de administración. Sus parámetros condicionan tanto el cifrado de la comunicación como la accesibilidad, la validación de las solicitudes y determinados comportamientos del navegador.

2.2.1. Protocol

Selecciona HTTP o HTTPS (SSL/TLS) como protocolo de comunicación entre el navegador y la interfaz del firewall. HTTP no cifra los datos intercambiados; HTTPS cifra la sesión utilizando TLS.

Para qué sirve. La elección de HTTPS protege credenciales, sesiones y cambios de configuración durante el transporte.

Precaución. HTTP no debe utilizarse para administrar el firewall a través de redes no confiables. HTTPS no sustituye a las reglas de control de acceso.

Cómo comprobarlo. Verificar que el navegador se conecta por HTTPS y que el certificado presentado corresponde al dispositivo previsto.

2.2.2. SSL/TLS Certificate

Permite escoger el certificado que presenta webConfigurator cuando funciona mediante HTTPS. El desplegable excluye certificados incompatibles con el servidor web o sus algoritmos.

Para qué sirve. Un certificado de confianza facilita autenticar el equipo y evita advertencias recurrentes en los navegadores administrados.

Precaución. No basta con cifrar: el administrador también debe asegurarse de que accede al firewall correcto. La gestión de certificados se realiza en el administrador de certificados.

Cómo comprobarlo. Abrir los detalles del certificado en el navegador y revisar identidad, validez, algoritmo y cadena de confianza.

2.2.3. TCP Port

Determina el puerto TCP en el que escucha la interfaz. Los puertos convencionales son 80 para HTTP y 443 para HTTPS; un valor personalizado sustituye al puerto habitual. El cambio se aplica al guardar.

Para qué sirve. Permite adaptar la interfaz a necesidades operativas o liberar un puerto para otros servicios cuando la arquitectura lo requiere.

Precaución. Cambiar el puerto no constituye una medida de seguridad suficiente: los servicios continúan siendo detectables si la red permite alcanzarlos. Verificar también las reglas del firewall.

Cómo comprobarlo. Después de guardar, abrir la dirección de administración con el protocolo y el puerto que correspondan.

2.2.4. Max Processes

Indica cuántos procesos de atención de solicitudes utiliza la interfaz web. La documentación de Netgate establece un valor predeterminado de dos.

Para qué sirve. Puede mejorar la capacidad de respuesta cuando varios administradores utilizan la interfaz simultáneamente.

Precaución. Incrementarlo consume recursos adicionales; no conviene elevarlo sin un problema que lo justifique.

Cómo comprobarlo. Observar si las páginas dejan de tardar o fallar en escenarios de acceso concurrente.

2.2.5. WebGUI redirect

La casilla «Disable webConfigurator redirect rule» controla la redirección automática que acepta solicitudes HTTP en el puerto 80 y dirige el navegador al puerto configurado para la interfaz. Por defecto, la redirección está habilitada.

Para qué sirve. Facilita que una solicitud HTTP termine en la interfaz HTTPS sin que el administrador tenga que escribir la dirección completa.

Precaución. Marcar «Disable…» desactiva la regla de redirección: no desactiva por sí mismo HTTPS. No debe interpretarse como una regla general de autorización de acceso.

Cómo comprobarlo. Tras aplicar un cambio, probar el comportamiento al iniciar una conexión HTTP y el acceso directo por HTTPS.

2.2.6. HSTS

La casilla «Disable HTTP Strict Transport Security» controla la emisión de la cabecera Strict-Transport-Security. Cuando HSTS está habilitado, el navegador recuerda que debe utilizar HTTPS para el nombre del firewall.

Para qué sirve. Reduce el riesgo de degradar accidentalmente la comunicación de HTTPS a HTTP en accesos posteriores.

Precaución. Si se desactiva HSTS, los navegadores que ya almacenaron la política pueden seguir forzando HTTPS hasta limpiar o agotar su información local.

Cómo comprobarlo. Comprobar que el navegador mantiene HTTPS en accesos siguientes al mismo nombre.

2.2.7. OCSP Must-Staple

La opción «Force OCSP Stapling in nginx» fuerza al servidor web a presentar una respuesta OCSP durante la negociación TLS cuando resulte necesario. Algunas características del certificado pueden activar este comportamiento automáticamente.

Para qué sirve. Contribuye a los mecanismos de comprobación de estado del certificado cuando la cadena y el ecosistema de validación son compatibles.

Precaución. Para utilizar el ajuste es necesaria la cadena completa de certificados; no se debe habilitar sin verificar su compatibilidad.

Cómo comprobarlo. Comprobar el certificado completo y el resultado de validación TLS con herramientas apropiadas.

2.2.8. WebGUI Login Autocomplete

«Enable webConfigurator login autocomplete» permite que el formulario de acceso admita sugerencias de autocompletado o guardado de credenciales por parte del navegador.

Para qué sirve. Aporta comodidad a determinados equipos de administración controlados.

Precaución. Muchos navegadores actuales no respetan estrictamente esta indicación; una política de seguridad debe gestionarse también desde el propio navegador o mediante administración centralizada.

Cómo comprobarlo. Probar el comportamiento en el navegador utilizado y revisar su política de contraseñas.

2.2.9. GUI login messages

La casilla «Lower syslog level for successful GUI login events» reduce la severidad de registro de inicios de sesión satisfactorios. En ciertos dispositivos, el nivel de emergencia puede activar una señal acústica de consola.

Para qué sirve. Reduce avisos innecesarios derivados de accesos normales, sin ocultar por ello la existencia del inicio de sesión.

Precaución. No debe confundirse con deshabilitar la auditoría de accesos. El sonido de consola también dispone de controles en Notifications.

Cómo comprobarlo. Consultar los registros correspondientes tras un inicio de sesión autorizado.

2.2.10. Roaming

«Allow GUI administrator client IP address to change during a login session» permite conservar la sesión del administrador cuando cambia su IP de origen. Normalmente la sesión está vinculada a esa dirección.

Para qué sirve. Es útil cuando un administrador cambia de red o utiliza conexiones cuya IP puede variar durante la sesión.

Precaución. Permitir cambios de IP reduce una restricción de sesión; solo conviene activarlo cuando exista una necesidad documentada.

Cómo comprobarlo. Comprobar que la sesión conserva la validez bajo un cambio de origen legítimo, en un entorno controlado.

2.2.11. Anti-lockout

«Disable webConfigurator anti-lockout rule» controla la regla automática que facilita el acceso administrativo desde LAN. Esta protección normalmente permite el acceso a la GUI y a SSH en el puerto correspondiente de LAN, aunque existan reglas de filtrado definidas por el administrador.

Para qué sirve. Evita que una modificación de reglas bloquee por error las vías de administración más inmediatas.

Precaución. Marcar «Disable…» elimina esta protección automática. Puede dejar el firewall inaccesible por red si las reglas manuales no contemplan el acceso administrativo.

Cómo comprobarlo. Antes de deshabilitarla, confirmar que existen reglas explícitas que autorizan el acceso desde las redes de gestión y que un segundo método de acceso funciona.

PROCEDIMIENTO SEGURO PARA ANTI-LOCKOUT Crear primero las reglas de permiso administrativo y comprobarlas; efectuar copia de seguridad; disponer de consola local; y solo después deshabilitar la regla automática si es necesario controlar los accesos con políticas propias. Si se pierde el acceso, la consola permite recuperar la configuración, según la versión y el hardware.

2.2.12. DNS Rebind Check

«Disable DNS Rebinding Checks» desactiva controles destinados a limitar ataques de DNS rebinding. Estos mecanismos intervienen cuando las respuestas DNS contienen direcciones privadas en contextos que podrían resultar inseguros.

Para qué sirve. Mantener la protección activa reduce la superficie de exposición de la interfaz y de la resolución de nombres.

Precaución. No desactivar globalmente como primera solución. Según el caso, es posible introducir excepciones por dominio de forma más limitada. Un cambio de esta opción puede requerir reiniciar el servicio de resolución o reenvío DNS.

Cómo comprobarlo. Cuando un nombre interno presente problemas, diagnosticar primero la respuesta DNS y si interviene DNS Resolver o DNS Forwarder.

2.2.13. Alternate Hostnames

Acepta nombres alternativos mediante los cuales se podrá acceder a la interfaz y que se considerarán válidos para las comprobaciones relacionadas con DNS Rebind y HTTP_REFERER. Los nombres se separan mediante espacios.

Para qué sirve. Permite conservar los controles defensivos cuando existen varios nombres legítimos para administrar el firewall.

Precaución. Introducir únicamente nombres previstos y administrados. No es una lista de direcciones IP de redes autorizadas ni sustituye reglas de firewall.

Cómo comprobarlo. Acceder desde los nombres autorizados y verificar que no se producen bloqueos inesperados.

2.2.14. Browser HTTP_REFERER enforcement

«Disable HTTP_REFERER enforcement check» desactiva la validación del encabezado HTTP_REFERER, utilizado para comprobar el origen de determinadas solicitudes a la interfaz.

Para qué sirve. La comprobación ayuda a rechazar intentos de enviar solicitudes administrativas desde páginas ajenas al firewall.

Precaución. Desactivar esta comprobación elimina una protección adicional. Una incidencia con scripts externos debe resolverse con análisis del flujo antes de reducir la seguridad.

Cómo comprobarlo. Verificar el funcionamiento de formularios normales y de integraciones autorizadas si las hubiera.

2.2.15. Browser tab text

«Display page name first in browser tab» cambia el orden de la información del título del navegador: nombre del equipo y página, o página y nombre del equipo.

Para qué sirve. Acelera la identificación de pestañas en equipos desde los que se administran varias funciones o varios firewalls.

Precaución. Es una preferencia visual sin efecto sobre permisos, tráfico o seguridad de red.

Cómo comprobarlo. Abrir varias páginas de la interfaz y observar el texto de las pestañas.

2.3. Secure Shell: acceso administrativo por SSH

SSH permite acceder a una terminal remota cifrada y realizar operaciones avanzadas. No equivale a la interfaz web: habilitarlo amplía los métodos de administración y exige controlar cuidadosamente autenticación, autorizaciones y exposición de red.

2.3.1. Secure Shell Server

La casilla «Enable Secure Shell» habilita el demonio SSH. Si es necesario, se generan claves de host y se inicia el servicio después de guardar.

Para qué sirve. Ofrece acceso por consola para diagnóstico y mantenimiento cuando la interfaz web no basta.

Precaución. Mantener deshabilitado si no se utiliza. No publicar el puerto SSH directamente en Internet por comodidad.

Cómo comprobarlo. Comprobar que el servicio escucha únicamente en las redes previstas y que un usuario autorizado puede iniciar sesión.

2.3.2. SSHd Key Only: modos de autenticación

Este selector determina si SSH admite contraseñas, claves públicas o ambas simultáneamente. Las claves públicas autorizadas deben asociarse previamente al usuario en User Manager.

Modo	Cómo funciona	Uso y consecuencia
Password or Public Key	Permite contraseña válida o clave pública autorizada.	Flexible, aunque permite intentos basados en contraseña.
Public Key Only	Exige una clave pública autorizada; no admite contraseña como mecanismo único.	Recomendable para restringir el acceso a administradores con claves gestionadas.
Require Both Password and Public Key	Exige simultáneamente una contraseña válida y una clave pública autorizada.	Añade dos comprobaciones diferentes; requiere preparar y custodiar ambos factores.

ANTES DE CAMBIAR EL MÉTODO SSH Instalar y comprobar primero las claves públicas autorizadas. Cambiar a Public Key Only o Require Both sin preparar los usuarios puede impedir cualquier inicio de sesión remoto.

2.3.3. Allow Agent Forwarding

«Enables ssh-agent forwarding support» autoriza la delegación del agente SSH al conectarse desde el firewall hacia otros equipos. La clave privada permanece en el equipo origen, pero el agente puede atender peticiones de autenticación desde el destino.

Para qué sirve. Puede facilitar tareas administrativas encadenadas sin copiar claves privadas al firewall.

Precaución. El reenvío del agente aumenta riesgos si se compromete un host intermedio. Suele ser preferible mantenerlo desactivado porque el firewall no debe actuar como servidor de salto general.

Cómo comprobarlo. En un entorno expresamente habilitado, verificar que los saltos autorizados funcionan sin copiar claves privadas.

2.3.4. SSH port

Establece el puerto TCP de escucha de SSH. Si se deja vacío, utiliza el puerto estándar 22.

Para qué sirve. Permite adaptarse a una política de puertos o evitar conflictos con otros servicios.

Precaución. Cambiar el puerto reduce parte del ruido de escaneo, pero no constituye una protección sólida frente a ataques dirigidos.

Cómo comprobarlo. Verificar conectividad al puerto definido y la existencia de la regla de acceso pertinente.

2.4. Login Protection: defensa frente a intentos repetidos

pfSense utiliza el servicio sshguard para acumular puntuaciones de intentos de autenticación fallidos o sospechosos procedentes de clientes. Cuando se supera el umbral configurado, el origen puede quedar temporalmente bloqueado. La protección es aplicable a accesos de la GUI y SSH.

2.4.1. Threshold

Establece la puntuación acumulada por encima de la cual se considera necesario bloquear el origen. No representa directamente un número exacto de contraseñas erróneas: diferentes eventos pueden sumar puntuaciones distintas. La documentación oficial indica una puntuación típica de 10 por intento y un umbral predeterminado de 30.

Ventaja: limita automatismos de fuerza bruta. Riesgo: un valor excesivamente bajo puede bloquear usuarios legítimos ante varios errores consecutivos.

2.4.2. Blocktime

Define, en segundos, el periodo de bloqueo inicial tras superar Threshold. La documentación oficial indica 120 segundos como valor predeterminado. Los bloqueos de reincidentes crecen multiplicativamente, por un factor de 1,5. El desbloqueo incorpora variabilidad, por lo que el tiempo real puede superar el valor indicado.

Ventaja: introduce esperas progresivas y dificulta repetir intentos masivos. Precaución: no confundir el plazo de bloqueo con la caducidad de las sesiones legítimas.

2.4.3. Detection time

Indica cuánto tiempo recuerda sshguard la puntuación de un posible atacante tras la última actividad antes de reiniciarla. La documentación oficial señala 1.800 segundos como configuración predeterminada.

Ventaja: permite correlacionar intentos separados en el tiempo. Precaución: un periodo demasiado corto puede pasar por alto ataques espaciados; uno demasiado largo puede aumentar bloqueos indeseados.

2.4.4. Pass list y Add address

Pass list contiene direcciones o redes excluidas del mecanismo de bloqueo de sshguard. El control Add address crea una entrada adicional en esa relación.

Ventaja: puede ser útil para sistemas de supervisión de confianza cuyas comprobaciones provoquen falsos positivos. Limitación: los orígenes incluidos dejan de estar cubiertos por esta defensa particular.

NO CONFUNDIR EXCEPCIONES Pass list no concede por sí sola acceso a la interfaz web ni al servidor SSH. Solo excluye la protección de intentos de inicio de sesión: siguen interviniendo las reglas de firewall, la escucha del servicio y la autenticación.

2.4.5. Lectura conjunta de los parámetros

Campo	Pregunta operativa
Threshold	¿Cuánta puntuación acumulada provoca bloqueo?
Blocktime	¿Durante cuánto tiempo se bloquea inicialmente?
Detection time	¿Durante cuánto tiempo se acumulan las faltas?
Pass list	¿Qué orígenes quedan fuera de esta protección?

2.5. Serial Communications: consola serie

2.5.1. Serial Speed

Selecciona la velocidad de comunicación de la consola serie. Es necesario que el equipo administrador y el puerto de consola utilicen valores compatibles. La referencia habitual de Netgate para hardware moderno es 115200 bps, aunque puede haber equipos o configuraciones heredadas con velocidades inferiores.

Ventaja: permite acceder al equipo incluso cuando la administración por red no está disponible. Es especialmente útil en dispositivos sin pantalla, siempre que exista consola serie operativa.

Comprobación: abrir un terminal serie compatible con el dispositivo, revisar que los caracteres se leen correctamente y confirmar que se presenta el menú de consola. Si aparecen símbolos extraños, comprobar velocidad y parámetros de comunicación.

Precaución: según el cambio y la plataforma, puede ser necesario reiniciar para aplicar opciones de consola. Una conexión física al dispositivo sigue estando sujeta a las políticas de seguridad de acceso al recinto.

2.6. Console Options: menú de consola

2.6.1. Console menu — Password protect the console menu

Habilita la solicitud de credenciales antes de utilizar el menú de consola. Utiliza cuentas de administración válidas, y la documentación oficial indica que el cambio requiere reiniciar para entrar en vigor.

Ventaja: reduce el riesgo de operaciones accidentales o no autorizadas sobre el menú local, especialmente en ubicaciones con acceso físico compartido.

Precaución: no sustituye a medidas físicas de protección. Una persona con control físico suficiente del dispositivo podría disponer de otras vías de recuperación o manipulación. Probar el procedimiento de acceso y recuperación antes de depender de él.

2.7. Procedimiento práctico: revisar y asegurar el acceso

El siguiente recorrido sirve para revisar la política administrativa de un firewall existente. No impone valores concretos de red ni presupone una topología.

Abrir System → Advanced → Admin Access desde una sesión de administración autorizada.

Hacer una copia completa de la configuración mediante Diagnostics → Backup & Restore y custodiarla de forma segura.

Confirmar que existe acceso alternativo a la consola si debe modificarse la escucha web, SSH o Anti-lockout.

Revisar Protocol y SSL/TLS Certificate; verificar que la identidad del certificado y el uso de HTTPS son adecuados.

Revisar el TCP Port y determinar si la red de administración y las reglas de firewall permiten el acceso previsto.

Mantener HSTS y las comprobaciones de DNS Rebind y HTTP_REFERER salvo que exista un motivo técnico específico para alterar su comportamiento.

Examinar Anti-lockout antes de establecer reglas restrictivas para la administración de LAN.

Habilitar SSH solo si es necesario; configurar las claves autorizadas y elegir el modo de autenticación antes de restringir contraseñas.

Revisar Threshold, Blocktime, Detection time y Pass list para evitar excepciones innecesarias.

Guardar cada modificación de riesgo por separado y verificar el acceso desde una segunda sesión antes de cerrar la anterior.

Confirmar el estado final en los registros y conservar la copia de seguridad correspondiente al cambio.

2.8. Comprobación y diagnóstico

Síntoma	Posibles causas	Primera comprobación
La GUI deja de responder tras guardar	Cambio de protocolo o TCP Port, redirección, regla de acceso, certificado o servicio web.	Probar URL y puerto correctos; comprobar conectividad y reglas; utilizar consola si el acceso web se pierde.
El navegador fuerza HTTPS aunque se haya desactivado HSTS	Política HSTS almacenada previamente en el navegador.	Comprobar el historial HSTS del navegador y su procedimiento de limpieza.

Síntoma	Posibles causas	Primera comprobación
SSH solicita autenticación, pero no acepta la credencial	Modo de claves cambiado sin cargar las autorizadas, o permisos insuficientes.	Revisar SSHd Key Only, usuario y Authorized Keys mediante una vía de acceso alternativa.
Se bloquea una estación administradora tras varios intentos	La puntuación de sshguard ha superado el Threshold.	Inspeccionar registros, esperar el desbloqueo o recuperar mediante consola según los procedimientos de administración.
El acceso mediante nombre falla, pero mediante IP funciona	Posible comprobación DNS Rebind, nombre alternativo no permitido o DNS incorrecto.	Revisar resolución, hostname y Alternate Hostnames antes de desactivar defensas.
No aparece el menú de consola serie de forma legible	Velocidad serie o parámetros de terminal incorrectos.	Contrastar la velocidad con la prevista para el equipo y la consola.
Tras reglas nuevas ya no se administra por LAN	Se eliminó Anti-lockout sin una regla administrativa válida.	Recuperar por consola y verificar las reglas de gestión antes de reintroducir la restricción.

2.9. Recomendaciones de seguridad

Utilizar HTTPS y verificar la identidad del certificado, no solo la presencia del candado del navegador.

Limitar la administración a redes de gestión autorizadas o a un acceso VPN protegido; no exponer la GUI directamente a Internet.

Mantener los controles HSTS, DNS Rebind y HTTP_REFERER salvo necesidad justificada y revisada.

Usar el principio de mínimo privilegio en las cuentas de administración y preferir autenticación SSH basada en claves cuando se habilite SSH.

Evitar Pass list extensas: cada excepción desactiva una capa de protección para esos orígenes.

Guardar una copia de seguridad antes de modificar el acceso y verificar la recuperación de consola.

Documentar las decisiones de configuración y realizar cambios que puedan bloquear el acceso en una ventana de mantenimiento adecuada.

2.10. Glosario rápido

Término	Significado
webConfigurator	Interfaz web de administración de pfSense Plus.
TLS	Protocolo criptográfico que protege la comunicación de HTTPS.
HSTS	Política de navegador que obliga a utilizar HTTPS para un nombre.
OCSP Stapling	Mecanismo de entrega de información de estado de un certificado TLS por el servidor.
DNS Rebinding	Ataque que intenta redirigir un nombre controlado por un atacante hacia direcciones internas.
HTTP_REFERER	Cabecera que puede indicar el origen de una petición web.
Anti-lockout	Regla administrativa automática destinada a evitar el bloqueo del acceso por LAN.
sshguard	Servicio que identifica y bloquea temporalmente orígenes con intentos de acceso sospechosos.
Agent Forwarding	Delegación del agente SSH para autenticarse a través de un host intermedio.

2.11. Referencias técnicas

Documentación oficial de Netgate, «Admin Access», pfSense Documentation:

https://docs.netgate.com/pfsense/en/latest/config/advanced-admin.html

Documentación oficial de Netgate, «Making Backups in the GUI»:

https://docs.netgate.com/pfsense/en/latest/backup/configuration.html

Documentación oficial de Netgate, «Console Menu Basics»:

https://docs.netgate.com/pfsense/en/latest/config/console-menu.html

Nota de versión. Los menús, las casillas y los valores predeterminados pueden cambiar entre versiones de pfSense Plus o según el hardware. Debe comprobarse la interfaz instalada antes de modificar parámetros críticos.

03 System → Advanced → Netgate Nexus

System → Advanced → Netgate® Nexus

Controlador de administración, interfaz web y API, comunicación entre instancias y registro centralizado.

Esta pantalla regula la puesta en marcha y el funcionamiento del controlador Netgate Nexus. Es importante distinguir la interfaz web clásica de pfSense Plus, la nueva interfaz Nexus y el canal utilizado para gestionar instancias remotas. Cada uno tiene una finalidad y un acceso propios.



Figura 3.1. Estructura de la pestaña Netgate Nexus. Recreación funcional sin direcciones, nombres, certificados ni valores de ninguna instalación.

IDEA PRINCIPAL Activar Netgate Nexus habilita un controlador y una nueva vía de administración, pero no publica automáticamente sus servicios ni sustituye por sí solo las reglas de firewall, la autenticación o una política de gestión segura.

Qué permite hacer esta pantalla

Habilitar o deshabilitar el controlador Netgate Nexus.

Seleccionar el certificado de protección HTTPS y los puertos de su interfaz y API.

Ajustar registros, direcciones de escucha, parámetros de conexión entre instancias y tiempo de sesión.

Consultar el estado del controlador y, cuando corresponda, registrar instancias para su administración centralizada.

3.1. Qué es Netgate Nexus y en qué se diferencia de webConfigurator

Netgate Nexus es una interfaz gráfica de configuración y una API para pfSense Plus. Su controlador puede utilizarse para administrar el propio firewall y, en las versiones y entornos admitidos, para gestionar múltiples instancias desde un punto central. La documentación oficial sitúa su disponibilidad en pfSense Plus 25.07 y posteriores; determinadas funciones de gestión multiinstancia pueden exigir versiones, plataformas o licencias específicas.

Concepto	Función y alcance
webConfigurator	Interfaz tradicional de pfSense Plus. Permanece separada de Nexus y utiliza sus propios ajustes de acceso.
Netgate Nexus Controller	Servicio que proporciona la interfaz Nexus, una API y capacidades de administración.

Concepto	Función y alcance
Nexus GUI / API	Vías para consultar y administrar funciones y, en su caso, varios equipos mediante herramientas gráficas o automatización.
Instancia	Instalación de pfSense Plus administrada como sistema individual; puede ser el equipo controlador o uno remoto.
Multi-Instance Management (MIM)	Administración coordinada de distintas instancias a través de un controlador.
VPN Nexus	Canal de comunicación entre controlador e instancias. Es distinto del acceso HTTPS a la GUI/API.

Ventaja operativa. En instalaciones con numerosos firewalls, el control centralizado facilita inventario, supervisión, tareas repetitivas y reducción de cambios manuales inconsistentes.

Matiz importante. Nexus no es una opción de balanceo WAN ni un sustituto genérico de las VPN de usuarios. La VPN propia del controlador sirve a su canal de gestión de instancias.

3.2. Organización de la pantalla

La pestaña se encuentra dentro de System → Advanced, junto a otras áreas de configuración avanzada. La página mostrada se divide en tres zonas: Netgate Nexus, Advanced Options e Instance Registration. Las opciones avanzadas se expanden o contraen mediante el control Show Advanced / Hide Advanced; ese botón modifica la vista de los campos, no enciende ni apaga el controlador.

Zona	Campos o elementos	Cuándo se utiliza
Netgate Nexus	Enable · TLS Certificate · Service Ports	Puesta en marcha y exposición controlada de la GUI y la API.
Advanced Options	Logging · Listening Address/Port · Advertised Addresses · JWT Session Expiry · Custom Options	Ajustes finos de diagnóstico, conexión remota y seguridad de sesión.
Instance Registration	Estado de registro y campos de vinculación, cuando están disponibles	Incorporación de instancias al sistema de administración.

3.3. Netgate Nexus: configuración principal

3.3.1. Enable — Enable Netgate Nexus Controller

Activa o desactiva el daemon del controlador Nexus. Tras guardar, el servicio puede ofrecer la GUI, la API y, cuando se ha configurado la gestión multiinstancia, los mecanismos de comunicación con otras instancias.

Para qué sirve. Permite poner en funcionamiento la administración Nexus tanto para el equipo local como para escenarios centralizados.

Qué conviene evitar. No interpretar «activado» como «accesible desde cualquier red». Las reglas de firewall siguen controlando el tráfico permitido y deben revisarse por separado.

Cómo comprobarlo. Guardar el cambio, regresar a la pestaña y revisar el área de estado del controlador. Verificar el acceso por HTTPS desde una red de administración autorizada.

3.3.2. TLS Certificate — Certificado TLS

Selecciona el certificado que presenta el controlador cuando actúa como servidor TLS. Puede ser un certificado autofirmado, uno importado de una entidad de confianza o uno administrado mediante ACME, cuando el sistema lo permita.

Para qué sirve. Cifra el acceso HTTPS y ayuda al administrador a comprobar la identidad del servidor.

Qué conviene evitar. No confundir cifrado con identidad verificada: si el certificado no coincide con el nombre utilizado o no es de confianza, el navegador puede mostrar una advertencia. Evitar certificados caducados o cadenas incompletas.

Cómo comprobarlo. Acceder a la GUI mediante HTTPS y revisar en el navegador el nombre del certificado, sus fechas, su cadena y la entidad que lo firma.

3.3.3. Service Ports — API HTTP Port

Define el puerto TCP en el que el controlador puede recibir solicitudes HTTP sin cifrar de navegadores o clientes API.

Para qué sirve. Tiene utilidad limitada en pruebas controladas o entornos de desarrollo aislados.

Qué conviene evitar. HTTP no cifra credenciales ni contenido. No debe exponerse a Internet ni utilizarse como vía ordinaria de administración.

Cómo comprobarlo. Comprobar qué puerto figura en la configuración, su posible conflicto con otros servicios y que las reglas de acceso no lo publiquen fuera del entorno expresamente autorizado.

3.3.4. Service Ports — API HTTPS Port

Especifica el puerto TCP de la interfaz/API de Nexus a través de una conexión cifrada con TLS. No debe confundirse con el puerto del webConfigurator tradicional.

Para qué sirve. Proporciona acceso protegido a la nueva interfaz y a clientes de automatización que utilicen HTTPS.

Qué conviene evitar. No abrir este puerto de forma indiscriminada en WAN; restringir el origen a redes de administración o clientes VPN autorizados. Modificarlo puede obligar a actualizar accesos y reglas existentes.

Cómo comprobarlo. Realizar una conexión HTTPS desde un host administrador permitido y confirmar que el servicio responde en el puerto configurado.

DIFERENCIA CRUCIAL ENTRE PUERTOS El API HTTPS Port es el puerto de la interfaz/API de Nexus. El Listening Port de Advanced Options corresponde a la comunicación VPN del controlador con instancias. Son servicios diferentes y no deben documentarse como si fueran el mismo puerto.

3.4. Advanced Options: configuración avanzada

Este bloque agrupa ajustes que normalmente no es necesario modificar en una instalación sencilla. Se utiliza para adaptar el comportamiento del servicio a políticas de seguridad, redes con varios caminos o necesidades de diagnóstico.

3.4.1. Logging — Level

Selecciona el umbral de detalle de los mensajes registrados por el daemon del controlador. Las categorías disponibles pueden variar según la versión del paquete.

Para qué sirve. Ayuda a conocer errores, advertencias y sucesos útiles para resolver incidencias.

Qué conviene evitar. Un nivel excesivamente detallado puede generar volumen de registros innecesario y facilitar que información operativa sensible aparezca en trazas.

Cómo comprobarlo. Aplicar el nivel adecuado, reproducir una incidencia cuando corresponda y revisar los registros de Nexus. Restaurar el nivel habitual después del diagnóstico.

3.4.2. Logging — Verbose

Casilla que incrementa el detalle de registro generado por el controlador.

Para qué sirve. Permite recopilar información adicional en casos difíciles de reproducir.

Qué conviene evitar. No dejarlo activado indefinidamente sin motivo; aumentar el nivel de detalle exige controlar almacenamiento, conservación y acceso a registros.

Cómo comprobarlo. Activarlo temporalmente en una ventana controlada, verificar la información obtenida y desactivarlo al terminar.

3.4.3. Listening Address

Indica la dirección local en la que el controlador escucha conexiones VPN entrantes de otras instancias. La opción Any hace que escuche en las direcciones disponibles.

Para qué sirve. Permite limitar el punto de recepción de conexiones de gestión cuando el sistema dispone de varias interfaces o direcciones.

Qué conviene evitar. Este ajuste no selecciona la dirección de escucha de la GUI HTTPS/API. Vincular la VPN a una dirección inaccesible puede impedir la unión de instancias.

Cómo comprobarlo. Confirmar que la dirección elegida existe y es alcanzable desde las instancias; comprobar en el estado del servicio cuál es el punto de escucha real.

3.4.4. Listening Port

Fija, cuando se desea, el puerto utilizado por la VPN entre el controlador y las instancias. Si no se establece uno manualmente, el controlador puede elegirlo automáticamente.

Para qué sirve. Ofrece control sobre la conectividad de gestión entre sitios y facilita reglas de filtrado específicas cuando la arquitectura lo requiere.

Qué conviene evitar. No confundirlo con API HTTP/HTTPS. En la documentación de Netgate, el alias interno _nexus_vpn_port_ refleja el puerto de VPN que el controlador utiliza, lo que simplifica determinadas reglas.

Cómo comprobarlo. Consultar el estado del controlador y verificar que el puerto VPN anunciado coincide con la configuración prevista y con las reglas de acceso correspondientes.

3.4.5. Advertised Addresses

Permite definir las direcciones IP o nombres FQDN, opcionalmente acompañados de un puerto, que el controlador anuncia a otras instancias. Admite varios valores separados por comas. Vacío, puede anunciar sus direcciones mediante autodetección.

Para qué sirve. Resulta útil cuando las instancias deben descubrir o alcanzar un controlador ubicado tras NAT, con varias WAN o con dirección externa cambiante.

Qué conviene evitar. Anunciar direcciones que no son accesibles para las instancias puede impedir la conectividad aunque el servicio se encuentre en ejecución. No copiar aquí una dirección de ejemplo sin comprobar antes la resolución y el camino real.

Cómo comprobarlo. Verificar resolución DNS, ruta y acceso desde una instancia autorizada hacia el nombre o dirección anunciados.

3.4.6. JWT Session Expiry

Determina durante cuánto tiempo son válidos los tokens JWT usados para mantener sesiones de acceso. La unidad indicada por la pantalla es el minuto.

Para qué sirve. Controla el equilibrio entre duración de las sesiones y necesidad de renovar la autenticación.

Qué conviene evitar. Periodos demasiado largos incrementan la ventana de exposición de un token comprometido; periodos muy breves pueden interrumpir flujos administrativos o automatizaciones que no renuevan sesiones adecuadamente.

Cómo comprobarlo. Iniciar sesión, comprobar el comportamiento de caducidad y validar los procedimientos de renovación utilizados por la GUI o los clientes API.

3.4.7. Custom Options

Campo de texto para directivas específicas del controlador, introducidas una por línea.

Para qué sirve. Permite aplicar determinados parámetros no cubiertos por los controles habituales en casos de soporte o ajuste especializado.

Qué conviene evitar. Netgate recomienda no utilizar este campo salvo indicación de sus desarrolladores o del centro de soporte técnico. Una línea incorrecta puede alterar el funcionamiento del servicio.

Cómo comprobarlo. Mantenerlo sin cambios cuando no exista un requerimiento documentado. Si soporte solicita una directiva, registrar su motivo y verificar los registros del servicio tras guardarla.

3.5. Instance Registration — registro de instancias

La zona Instance Registration permite completar el vínculo de una instalación pfSense Plus con un controlador Nexus para las funciones de administración multiinstancia. La información disponible depende del estado del servicio: mientras el controlador no esté funcionando, la pantalla puede limitarse a informar de que el registro todavía no está disponible.

El alta completa de una instancia es un proceso de dos direcciones: se recopilan datos de registro desde la instancia, se incorporan al controlador y luego se introduce en la instancia la información de activación emitida por el controlador. Las opciones concretas visibles pueden variar con la versión y el papel del equipo.

Elemento	Qué representa	Precaución
Registration Data	Información que identifica una instancia para solicitar su asociación al controlador.	Tratar el contenido de registro como información administrativa y no publicarlo.
Controller / Nexus GUI	Interfaz desde la que se registra la instancia y se obtiene la activación.	Limitar el acceso a administradores autorizados.
Activation Data	Información de activación que completa la relación con el controlador.	No publicar ni reutilizar material de activación sin control.
Estado del servicio	Indicación de si el controlador permite operar o consultar el registro.	La aparición de controles no prueba por sí sola que una instancia esté gestionada correctamente.

Diferencia importante. La posibilidad de activar una interfaz Nexus para el propio firewall no implica automáticamente disponer de todas las capacidades de gestión de una flota: deben comprobarse los requisitos de versión, plataforma y licencia vigentes.

3.6. Procedimiento práctico: habilitar Nexus para administrar el equipo local

Este procedimiento es una secuencia de verificación segura; no presupone direcciones, certificados, puertos ni reglas de una empresa concreta.

1. Comprobar que la plataforma y la versión de pfSense Plus admiten Netgate Nexus y que existe una copia reciente de la configuración.
2. Confirmar que se dispone de una vía alternativa de administración antes de cambiar puertos, reglas o servicios.
3. Abrir System → Advanced → Netgate Nexus.
4. Revisar el certificado TLS disponible y decidir qué puerto HTTPS corresponde a la política de acceso.
5. Marcar Enable y guardar con Save, sin modificar opciones avanzadas que no sean necesarias.
6. Verificar el estado de Nexus en la misma pestaña y consultar el enlace seguro mostrado cuando el servicio esté operativo.
7. Revisar las reglas del firewall para permitir exclusivamente clientes de administración autorizados; no publicar la GUI/API en Internet.
8. Abrir la GUI Nexus mediante HTTPS y autenticarse con una cuenta que disponga de permisos adecuados.
9. Confirmar que la interfaz permite consultar el dispositivo local; comprobar que el webConfigurator clásico sigue siendo accesible por su vía de administración prevista.

PRECAUCIÓN AL GUARDAR Los cambios de puertos, certificado o dirección de escucha pueden afectar inmediatamente a la disponibilidad del servicio. Antes de modificar estos ajustes conviene asegurar la recuperación mediante consola o una vía de gestión alternativa.

3.7. Procedimiento práctico: preparar un controlador para varias instancias

En gestión multiinstancia, no basta con que el panel de configuración se muestre. El controlador y los equipos administrados deben cumplir los requisitos técnicos y establecer correctamente su canal de gestión.

1. Determinar qué equipo asumirá el papel de controlador y comprobar compatibilidad y licencias aplicables.
2. Habilitar Nexus en el controlador y validar su acceso HTTPS desde la red de administración.
3. Definir cómo alcanzarán las instancias al controlador y revisar Listening Address, Listening Port y Advertised Addresses cuando sea necesario.
4. Permitir únicamente la conectividad VPN necesaria hacia el controlador. La documentación propone utilizar el alias interno _nexus_vpn_port_ para el puerto del servicio.
5. Habilitar Nexus en cada instancia compatible y obtener sus datos de registro desde su propia interfaz.
6. Registrar la instancia en la GUI del controlador y completar la activación en el equipo gestionado.

7. Verificar que la instancia aparece correctamente y que se permite su administración remota con el perfil de permisos adecuado.
8. Documentar las pruebas, las restricciones de acceso y el procedimiento para revocar una instancia cuando deje de estar autorizada.

Seguridad de red. Netgate indica que el controlador no crea por sí mismo todas las reglas externas necesarias para su GUI y para la conectividad VPN de instancias. El acceso de administración HTTPS debe quedar restringido a redes y usuarios autorizados.

3.8. Cómo comprobar que funciona

Prueba	Qué observar	Interpretación
Servicio	Estado del controlador tras guardar.	Activo no equivale necesariamente a accesible desde cualquier origen.
Acceso HTTPS	Respuesta de la GUI en el puerto correspondiente.	Verifica disponibilidad y conectividad del servicio web.
Certificado	Identidad, validez y cadena de confianza.	Permite detectar configuración TLS inadecuada.
Inicio de sesión	Autenticación de una cuenta autorizada.	Valida el mecanismo de acceso, no los permisos de todas las operaciones.
Firewall	Reglas y registros de tráfico hacia los servicios Nexus.	Confirma que el acceso está permitido solo desde orígenes previstos.
Comunicación MIM	Alcance del punto de escucha VPN y estado de instancias.	Distingue la disponibilidad de la GUI y la conexión entre equipos.
Registros	Errores o advertencias recientes del controlador.	Ayuda a acotar fallos sin cambiar parámetros a ciegas.

3.9. Incidencias habituales y cómo diagnosticarlas

Síntoma	Posible causa	Comprobación recomendable
Nexus no responde.	Servicio detenido, incompatibilidad, cambio de puerto o filtrado.	Revisar estado, versión, logs, puerto HTTPS y reglas.
El navegador muestra aviso TLS.	Certificado autofirmado, vencido, nombre no coincidente o cadena incorrecta.	Examinar el certificado; no aceptar avisos automáticamente.
Se accede a webConfigurator pero no a Nexus.	Son servicios y puertos independientes.	Verificar la URL/puerto de Nexus y su filtrado.
El usuario no puede iniciar sesión.	Problema de credenciales, cuenta o permisos.	Revisar User Manager y registros de autenticación.
Una instancia no conecta.	Puerto VPN, dirección anunciada, NAT, DNS o reglas.	Comprobar el canal MIM, no solo la GUI HTTPS.
El registro no está disponible.	El controlador aún no está ejecutándose o faltan requisitos.	Comprobar el estado del servicio y su compatibilidad.
Se generan demasiados registros.	Nivel Logging o Verbose excesivo.	Reducir detalle tras recopilar evidencias.
Las sesiones terminan demasiado pronto.	Caducidad JWT demasiado restrictiva o cliente sin renovación.	Revisar JWT Session Expiry y comportamiento de autenticación.

3.10. Recomendaciones de seguridad y operación

Utilizar HTTPS y verificar la identidad del servicio mediante un certificado apropiado.

Mantener la GUI/API de Nexus fuera de la exposición directa a Internet; acceder por red de gestión o VPN.

Aplicar mínimo privilegio a los administradores y revisar periódicamente sus autorizaciones.

Distinguir los puertos de la GUI/API de los utilizados por la VPN de instancias.

Registrar los cambios antes de activar la gestión multiinstancia y disponer de un método de reversión.

Utilizar registros detallados solo cuando exista una necesidad concreta de diagnóstico.

Proteger los datos de registro, activación y cualquier credencial utilizada por API o automatizaciones.

Comprobar los requisitos y las notas de versión antes de habilitar funciones dependientes del paquete Nexus.

3.11. Ejercicio de comprensión de la pantalla

Sin modificar la configuración, localizar visualmente los siguientes controles y responder las preguntas de verificación:

Localizar	Pregunta técnica
Enable	¿Es el control que pone en ejecución el servicio de Nexus?
TLS Certificate	¿Qué identidad y protección presentará la GUI/API HTTPS?
API HTTP / API HTTPS	¿Cuál es la vía cifrada y cuál debe evitarse para administración ordinaria?
Listening Address / Port	¿A qué servicio corresponden: GUI web o canal VPN entre instancias?
Advertised Addresses	¿Cómo conocen las instancias la dirección a la que pueden conectarse?
JWT Session Expiry	¿Qué caduca y qué consecuencia tiene su duración?
Instance Registration	¿Qué debe ocurrir para completar la vinculación de una instancia?

Resultado esperado: identificar los controles sin confundir el canal de administración HTTPS, la VPN de comunicación entre instancias y la activación del sistema multiinstancia.

3.12. Ideas esenciales

Nexus incorpora una interfaz y API propias para pfSense Plus; no es simplemente una pestaña más del webConfigurator.

Puede administrar el equipo local y, cuando se cumplen los requisitos, varias instancias.

El certificado TLS y los puertos HTTP/HTTPS protegen y delimitan el acceso a la GUI/API.

Listening Address y Listening Port pertenecen a la conectividad VPN de Nexus, no al servicio web HTTPS.

Las direcciones anunciadas, los tokens JWT y el registro de instancias cumplen funciones distintas.

Activar el controlador no elimina la obligación de configurar reglas de acceso y verificar la seguridad de la administración.

Referencias técnicas

Netgate. «Netgate Nexus Options in the pfSense Plus GUI». docs.netgate.com/pfsense/en/latest/nexus/options.html

Netgate. «Netgate Nexus Controller Setup». docs.netgate.com/pfsense/en/latest/nexus/setup.html

Netgate. «Instance Registration». docs.netgate.com/pfsense/en/latest/nexus/mim/registration.html

Netgate. «Netgate Nexus». docs.netgate.com/pfsense/en/latest/nexus/index.html

Netgate. «Netgate Nexus & Multi-Instance Management FAQ». www.netgate.com/support/frequently-asked-questions-nexus

Nota editorial: las figuras no muestran configuraciones operativas. Los nombres de opciones corresponden a la interfaz de pfSense Plus y pueden presentar pequeñas diferencias entre versiones o revisiones del paquete Nexus.

04 System → Advanced → Firewall & NAT

Procesamiento de paquetes, normalización, tabla de estados, tráfico VPN, políticas de filtrado y traducción de direcciones.

Esta pantalla reúne parámetros globales del motor de filtrado PF. A diferencia de una regla individual, muchos de sus ajustes afectan al comportamiento de numerosas conexiones al mismo tiempo. Por ello debe interpretarse como una sección de ajuste especializado y no como una lista de opciones que convenga activar indiscriminadamente.



Figura 4.1. Estructura funcional de Firewall & NAT, sin capturas ni valores de ninguna instalación.

Qué aprenderá el lector

Reconocer cada control de la pestaña y distinguir su ámbito (paquetes, VPN, estados, NAT o protocolos).

Comprender qué cambia al habilitarlo y qué riesgos introduce un cambio global.

Identificar síntomas típicos: fragmentación, túneles lentos, rutas asimétricas, servicios internos por nombre externo y tablas saturadas.

Planificar cambios reversibles y verificar resultados mediante registros, estados, gateways y capturas de paquetes.

> **ADVERTENCIA ESENCIAL** La opción Disable Firewall no equivale a desactivar solamente NAT: deja el equipo funcionando como enrutador sin filtrado PF. No debe emplearse como prueba rutinaria.

4.1. Ubicación, alcance y criterios antes de modificar

La ruta es System → Advanced → Firewall & NAT. La pestaña está situada junto a Admin Access, Netgate Nexus, Networking, Miscellaneous, System Tunables y Notifications. Sus opciones son globales y, cuando existen excepciones por regla o interfaz, estas deben evaluarse antes de modificar el ajuste general.

Área	Qué controla	Cuándo interesa revisarla
Packet Processing	Normalización de paquetes y capacidad de estados.	Cortes anómalos, fragmentos, alta concurrencia.
VPN Packet Processing	Fragmentos y ajuste MSS en determinados túneles.	Problemas de rendimiento o MTU en VPN.
Advanced Options	Motor PF, políticas de estado y comportamientos especiales.	Multi-WAN, IPsec, HA, filtrado L2, rutas.
Bogon Networks	Frecuencia de actualización de redes no asignadas o reservadas.	Mantenimiento de listas de bloqueo.
Network Address Translation	NAT64, NAT Reflection y TFTP proxy.	Acceso interno a servicios publicados o transición IPv6/IPv4.
State Timeouts	Caducidad de estados por protocolo y fase.	Sesiones ociosas, dispositivos especiales, depuración.

En pfSense, el firewall es de tipo stateful: una conexión permitida suele crear un estado y el tráfico de respuesta se contrasta con ese estado. El número de estados, su política de vinculación y su caducidad influyen tanto en la seguridad como en la continuidad de las comunicaciones.

4.2. Packet Processing — Procesamiento de paquetes

4.2.1. IP Do-Not-Fragment compatibility

Clear invalid DF bits instead of dropping the packets. Permite tratar determinados paquetes malformados o inconsistentes: paquetes fragmentados que mantienen marcado el indicador IPv4 «Don't Fragment» (DF).

UTILIDAD Puede restablecer interoperabilidad con implementaciones que generan este tráfico, como ciertos usos de NFS y VoIP.

PRECAUCIÓN No es un remedio genérico para problemas MTU. Conviene comprobar si existe un dispositivo que genera paquetes anómalos antes de debilitar la validación.

COMPROBACIÓN Correlacionar bloqueos, captura de paquetes y pruebas del servicio afectado antes y después del ajuste.

4.2.2. IP Random ID generation

Insert a stronger ID into IP header of packets passing through the filter. Sustituye el campo de identificación IPv4 de paquetes elegibles por valores menos predecibles. Se aplica a paquetes no fragmentados tras el posible reensamblado.

UTILIDAD Mitiga la predictibilidad de identificadores IP generados por determinados sistemas operativos.

PRECAUCIÓN Su efecto es acotado al campo IPv4 indicado; no sustituye cifrado, autenticación ni mecanismos de seguridad de las aplicaciones. Además, depende de que el scrub correspondiente esté operativo.

COMPROBACIÓN Verificar su efecto con una captura de paquetes controlada y comparando encabezados, si es necesario.

4.2.3. Firewall Optimization Options

Determina la estrategia de expiración de estados. El desplegable no cambia por sí mismo las reglas que permiten o bloquean paquetes; altera cuánto tiempo pueden conservarse estados ociosos según el tipo de tráfico.

Modo	Comportamiento	Ventaja y riesgo
Normal	Equilibrio predeterminado para la mayoría de entornos.	Punto de partida recomendado.
High Latency	Tolera mejor enlaces con alta latencia y retiene sesiones ociosas más tiempo.	Útil en conexiones satelitales; puede incrementar consumo de estados.
Aggressive	Caduca estados inactivos más pronto.	Puede liberar recursos; riesgo de cortar sesiones válidas.
Conservative	Retiene estados más tiempo para evitar cierres prematuros.	Útil en tráfico poco frecuente pero persistente; exige más memoria.

CASO PRÁCTICO Si una aplicación con sesiones UDP muy espaciadas pierde conectividad por caducidad, revisar estados y probar un ajuste localizado antes de pasar todo el firewall a Conservative.

4.2.4. Disable Firewall Scrub

Deshabilita la normalización de paquetes (scrub) del motor PF. Normalmente scrub participa en el tratamiento de fragmentos y encabezados.

UTILIDAD Puede ser una medida de compatibilidad excepcional en NFS o VoIP cuando se ha identificado la normalización como origen del problema.

PRECAUCIÓN Al desactivarlo también dejan de funcionar funciones que dependen de scrub, incluidas ciertas correcciones DF y la aleatorización de IP ID. No desactiva por sí mismo todos los mecanismos MSS.

COMPROBACIÓN Revisar capturas y registros del servicio afectado y confirmar que el cambio no perjudica a otros flujos.

4.2.5. Firewall Adaptive Timeouts

Al aumentar el uso de la tabla de estados, PF puede reducir progresivamente la duración de los estados para liberar capacidad. Esta función consta de dos umbrales, Adaptive Start y Adaptive End.

4.2.5.a. Adaptive Start

Umbral de ocupación de la tabla de estados a partir del cual empieza el acortamiento de los tiempos de expiración. La documentación oficial señala un cálculo automático predeterminado del 60 % del límite máximo de estados.

UTILIDAD Ofrece un mecanismo progresivo de contención si el número de conexiones crece.

PRECAUCIÓN Si se sitúa demasiado bajo, conexiones legítimas pueden expirar mucho antes de lo previsto.

COMPROBACIÓN Comprobar ocupación y evolución de la tabla de estados en el Dashboard y Diagnostics → States.

4.2.5.b. Adaptive End

Umbral teórico en el que el factor adaptativo llevaría los tiempos de estado a cero. La documentación define un valor automático del 120 % del máximo permitido; debe quedar por encima del límite efectivo de estados.

UTILIDAD Define cómo de intensa será la reducción progresiva de expiración.

PRECAUCIÓN No debe ajustarse para que la tabla alcance ese valor; se utiliza como referencia de escalado. Un ajuste incorrecto puede provocar purgas y desconexiones.

COMPROBACIÓN Correlacionar incidencias de sesiones con crecimiento de estados y valores configurados.

Relación conceptual: factor de tiempo ≈ (Adaptive End − estados actuales) / (Adaptive End − Adaptive Start). Por debajo del inicio se mantienen los tiempos normales; entre ambos umbrales se reducen progresivamente. No deben copiarse umbrales de otros equipos sin dimensionar la RAM.

4.2.6. Firewall Maximum States

Fija el máximo de entradas simultáneas en la tabla de estados del firewall. Si se deja sin definir, pfSense calcula un valor dependiente de recursos del sistema.

UTILIDAD Permite dimensionar el número de conexiones concurrentes en entornos de alta actividad.

PRECAUCIÓN Aumentarlo consume RAM y no resuelve automáticamente problemas de ancho de banda. La modificación del tamaño de tablas hash de estados requiere reinicio para surtir plenamente efecto.

COMPROBACIÓN Consultar el uso real y los avisos de agotamiento antes de alterar el límite.

4.2.7. Firewall Maximum Table Entries

Limita el número total de entradas en tablas de direcciones utilizadas por aliases y otras funciones, como protecciones frente a bloqueos de sesión o determinados paquetes.

UTILIDAD Permite cargar listas extensas sin fallos de compilación del conjunto de reglas.

PRECAUCIÓN Las actualizaciones de aliases pueden requerir que convivan temporalmente listas anteriores y nuevas. Un límite insuficiente puede impedir cargar reglas; un exceso consume memoria.

COMPROBACIÓN Revisar el estado de carga del filtro y los registros al actualizar listas grandes.

4.2.8. Firewall Maximum Fragment Entries

Establece cuántos fragmentos mantiene PF pendientes de reensamblado cuando scrub está activo.

UTILIDAD Permite adaptar entornos con tráfico fragmentado legítimo inusualmente frecuente.

PRECAUCIÓN Ampliarlo a ciegas incrementa consumo de recursos y puede enmascarar un problema de MTU o de origen del tráfico.

COMPROBACIÓN Buscar en registros mensajes relacionados con el límite de entradas de fragmentos y capturar tráfico si procede.

4.3. VPN Packet Processing — Tráfico de VPN

Esta sección incorpora parámetros de tratamiento para determinados flujos de IPsec y OpenVPN, además del servidor PPPoE. No debe interpretarse como un sustituto de las opciones específicas de cada túnel.

4.3.1. IP Do-Not-Fragment compatibility

Aplica al ámbito VPN el mismo tratamiento de bits DF inconsistentes descrito para el procesamiento general.

UTILIDAD Puede recuperar comunicación cuando la encapsulación encuentra paquetes anómalos con información DF incoherente.

PRECAUCIÓN No garantiza corregir un MTU excesivo ni problemas de Path MTU Discovery.

COMPROBACIÓN Probar transferencia a través del túnel y observar registros/capturas.

4.3.2. IP Fragment Reassemble

Reassemble IP Fragments until they form a complete packet. Retiene los fragmentos hasta obtener un datagrama completo antes de enviarlo a filtrado.

UTILIDAD Facilita que las reglas trabajen sobre paquetes completos y no sobre fragmentos aislados.

PRECAUCIÓN El almacenamiento temporal implica consumo de memoria y puede introducir latencia.

COMPROBACIÓN Comprobar si se reducen las incidencias de tráfico fragmentado sin deteriorar el rendimiento.

4.3.3. Enable Maximum MSS

Activa MSS clamping sobre tráfico TCP VPN compatible. MSS es el tamaño máximo de datos TCP dentro de un segmento y se negocia durante el establecimiento de la conexión.

UTILIDAD Puede corregir páginas incompletas, sesiones lentas o transferencias grandes que fallan debido a sobrecarga de encapsulación y problemas PMTUD.

PRECAUCIÓN No modifica genéricamente todos los paquetes UDP ni resuelve cualquier pérdida de VPN. En IPsec VTI el ajuste puede corresponder a la interfaz VTI asignada.

COMPROBACIÓN Comparar conexiones TCP de prueba de pequeño y gran tamaño, revisar PMTU y observar retransmisiones antes/después.

CUÁNDO USARLO Si ping o conexiones cortas funcionan por VPN pero ciertas páginas o archivos grandes fallan, investigar primero MTU/MSS, fragmentación y bloqueo de ICMP necesario para PMTUD.

4.4. Advanced Options — Comportamiento avanzado de PF

4.4.1. Disable Firewall — Disable all packet filtering

Apaga el filtrado PF y, como consecuencia, desactiva también NAT: el dispositivo pasa a una función de enrutamiento sin firewall PF.

UTILIDAD Solo tiene sentido en arquitecturas diseñadas expresamente para operar sin este filtrado.

PRECAUCIÓN RIESGO CRÍTICO: puede eliminar controles fundamentales y exponer redes. Para desactivar exclusivamente NAT debe configurarse Outbound NAT, no esta casilla.

COMPROBACIÓN Confirmar controles de seguridad externos y disponer de una vía local de recuperación antes de cualquier prueba excepcional.

4.4.2. Firewall State Policy

Define cómo se relaciona cada entrada de la tabla de estados con la interfaz por la que circulan los paquetes. Afecta a rutas asimétricas, VPN, Multi-WAN y escenarios de alta disponibilidad.

Política	Funcionamiento	Ventaja / compromiso
Interface Bound States	El estado queda asociado a la interfaz; tráfico equivalente por otra interfaz no coincide y puede descartarse.	Más estricto y predecible; reduce salidas imprevistas. Puede requerir ajustes específicos en VPN VTI y HA.

Política	Funcionamiento	Ventaja / compromiso
Floating States	El estado puede coincidir aunque el paquete recorra otra interfaz.	Más tolerante con rutas asimétricas o equipos HA diferentes; menor aislamiento por interfaz.

RECOMENDACIÓN Mantener el comportamiento estricto salvo una necesidad comprobada. La política puede sobreescribirse en reglas concretas; suele ser preferible a relajar todo el sistema.

4.4.3. Disable state-policy override for IPsec rules

Cuando está activo, evita que las reglas IPsec adopten automáticamente Floating States en situaciones que requerirían esa excepción.

UTILIDAD Permite controlar explícitamente cómo se vinculan los estados del tráfico IPsec, especialmente al evaluar una política global estricta.

PRECAUCIÓN Al desactivar la excepción automática podrían fallar flujos IPsec VTI según el modo de filtrado. La opción no tiene el mismo efecto en todos los modos de filtro IPsec.

COMPROBACIÓN Comprobar rutas y tráfico real de túneles IPsec, estados y reglas por interfaz antes de generalizar el ajuste.

4.4.4. Ethernet Filtering — Enable Ethernet Filtering

Activa reglas PF basadas en atributos de cabeceras Ethernet (capa 2). Al habilitarlo aparece la pestaña Ethernet en Firewall → Rules.

UTILIDAD Permite políticas de acceso L2 para tráfico que atraviesa interfaces compatibles, complementarias a las reglas L3.

PRECAUCIÓN No equivale a controlar todo el tráfico entre equipos de un mismo switch si ese tráfico no pasa por el firewall. Las reglas Ethernet no conservan estado por defecto y su política es de paso salvo reglas restrictivas.

COMPROBACIÓN Comprobar que aparece Firewall → Rules → Ethernet y verificar el orden de evaluación y las coincidencias de cada regla.

4.4.5. Static route filtering — Bypass firewall rules for traffic on the same interface

Hace que determinados paquetes que entran y salen por la misma interfaz puedan eludir comprobaciones PF cuando intervienen rutas estáticas.

UTILIDAD Puede solventar problemas de routing asimétrico entre varias redes accesibles mediante una interfaz.

PRECAUCIÓN Reduce la inspección del tráfico y puede abrir caminos no previstos. No utilizar solo porque una subred remota no responde: diagnosticar primero rutas y reglas.

COMPROBACIÓN Comparar trazas de tráfico, logs y estados antes de considerar esta excepción.

4.4.6. Disable Auto-added VPN rules

Desactiva reglas automáticas que pfSense agrega para posibilitar la negociación IPsec y requiere que el administrador cree las reglas necesarias.

UTILIDAD Aporta control explícito de los orígenes permitidos para iniciar servicios VPN.

PRECAUCIÓN Puede impedir nuevos túneles o reconexiones si no existe una política manual equivalente. No confundir con las reglas que autorizan el tráfico interior del túnel.

COMPROBACIÓN Revisar interfaces externas, puertos/protocolos de IPsec y negociación real del túnel tras el cambio.

4.4.7. Disable reply-to — Disable reply-to on WAN rules

Evita la inserción automática de reply-to en reglas de interfaces tipo WAN. Por defecto, reply-to facilita que una respuesta salga por la interfaz y gateway por los que entró la conexión.

UTILIDAD Puede ser necesario ante ciertos bridges, rutas estáticas o topologías WAN particulares.

PRECAUCIÓN En Multi-WAN, desactivarlo globalmente puede romper la simetría de flujos o modificar la salida de las respuestas. Valorar antes la opción por regla.

COMPROBACIÓN Comprobar retorno de tráfico desde cada enlace y capturar las rutas de ida y vuelta.

4.4.8. Disable Negate rules — Disable Negate rule on policy routing rules

Impide reglas automáticas de excepción destinadas a conservar rutas locales y VPN cuando otras reglas usan policy routing con gateways específicos.

UTILIDAD Permite al administrador construir excepciones completamente explícitas a una política de enrutamiento.

PRECAUCIÓN Sin excepciones manuales pueden enviarse destinos de VPN o redes directamente conectadas al gateway equivocado.

COMPROBACIÓN Probar tráfico entre redes internas y túneles, e inspeccionar reglas superiores sin gateway asignado.

4.4.9. Allow APIPA — Allow APIPA traffic

Retira el bloqueo especial predeterminado sobre tráfico IPv4 Link-Local/APIPA, reservado para comunicaciones locales de enlace, permitiendo que actúen reglas de usuario.

UTILIDAD Puede resultar necesario en interconexiones excepcionales de proveedores que utilizan direcciones Link-Local.

PRECAUCIÓN Ese rango no está diseñado para ser enrutado normalmente. Solo procede ante un requisito verificable, y no convierte APIPA en un esquema de direccionamiento empresarial.

COMPROBACIÓN Confirmar requisito del proveedor, interfaz afectada y reglas de filtrado explícitas.

4.4.10. Aliases Hostnames Resolve Interval

Determina cada cuánto tiempo el servicio filterdns vuelve a resolver los nombres DNS de aliases de tipo host.

UTILIDAD Reduce el retraso para reflejar cambios DNS en reglas basadas en hostnames.

PRECAUCIÓN Intervalos muy cortos multiplican consultas DNS y cambios de tablas; demasiado largos pueden dejar direcciones caducadas durante más tiempo.

COMPROBACIÓN Verificar resolución DNS real, actualización del alias y coincidencia del tráfico con las reglas.

4.4.11. Check certificate of aliases URLs

Verifica certificados TLS HTTPS durante la descarga de listas de aliases obtenidas mediante URL.

UTILIDAD Reduce el riesgo de aceptar datos desde servidores con identidad TLS no verificada.

PRECAUCIÓN Deshabilitarlo para resolver rápidamente un certificado inválido debilita la autenticidad de las fuentes. Es preferible instalar una cadena de confianza válida.

COMPROBACIÓN Comprobar descarga correcta de listas y errores de certificados en registros.

4.5. Bogon Networks — Actualización de listas

4.5.1. Update Frequency

Establece la periodicidad de actualización de la lista de redes sin asignación pública habitual o reservadas por las autoridades de direccionamiento, distintas de las privadas RFC 1918.

UTILIDAD Mantiene actualizados los conjuntos de direcciones que pueden bloquearse mediante la opción de redes bogon de interfaces.

PRECAUCIÓN Una lista desactualizada puede interpretar incorrectamente bloques reasignados. Bogon no es sinónimo de dirección maliciosa y tampoco sustituye otras políticas antisuplantación.

COMPROBACIÓN Inspeccionar la última actualización y comprobar que las interfaces están usando las listas según su finalidad.

4.6. Network Address Translation — Traducción de direcciones

4.6.1. NAT64 Prefix Override

La opción Allow overriding the NAT64 prefix used in rules and services permite definir un prefijo NAT64 alternativo cuando la versión instalada la ofrece. NAT64 permite que determinados clientes IPv6 se comuniquen con servicios IPv4 mediante traducción. Su uso debe coordinarse con DNS64 y, cuando corresponda, PREF64.

UTILIDAD Ofrece margen de adaptación en escenarios especializados de interoperabilidad IPv6/IPv4 con requisitos definidos.

PRECAUCIÓN CRÍTICA La propia interfaz advierte que sobrescribir el prefijo puede incumplir RFC y romper NAT64. También desactiva reglas predeterminadas que bloquean traducciones a determinadas direcciones IPv4 no globales. No habilitar sin diseño y pruebas específicas.

COMPROBACIÓN Validar alcance IPv6→IPv4, resolución DNS64 y destinos permitidos en un laboratorio aislado antes de producción.

4.6.2. NAT Reflection mode for port forwards

NAT Reflection (también llamado hairpin NAT en determinados casos) intenta que un cliente interno alcance un servicio interno utilizando su dirección externa publicada, cuando existe un port forward correspondiente. No añade, por sí solo, el port forward original.

Modo	Cómo funciona	Cuándo usarlo / limitaciones
Disabled	No crea reflexión global. Una regla concreta puede sobrescribir el valor si la versión lo admite.	Recomendado cuando se usa Split DNS o no se necesita acceso interno mediante dirección externa.
Pure NAT	Utiliza reglas NAT de PF para redirigir al servidor real.	Mejor escalabilidad; necesita inferir correctamente interfaz y gateway; en misma subred puede necesitar NAT de salida adicional.
NAT + Proxy	Un proceso auxiliar acepta la conexión y crea otra hacia el servidor.	Útil si no se conoce correctamente el camino al cargar reglas. Más sobrecarga; límites documentados para rangos y cantidad de puertos.

COMPATIBILIDAD DE PROTOCOLOS NAT + Proxy está documentado para TCP y no admite UDP. Para reflexión de puertos UDP se debe estudiar Pure NAT o una solución de DNS dividido. Comprobar además los límites de puertos y las condiciones del modo elegido antes de aplicarlo.

RECOMENDACIÓN Para servicios internos accesibles por nombre, preferir Split DNS: devolver desde el DNS interno la dirección interna del servidor y evitar el bucle a través del firewall. Además, el servidor puede ver la dirección original del cliente.

4.6.3. Reflection Timeout

Controla el tiempo límite de conexiones atendidas por el componente de NAT Reflection en modo NAT + Proxy; se expresa en segundos.

UTILIDAD Ayuda a evitar conexiones auxiliares ociosas durante periodos indefinidos.

PRECAUCIÓN No tiene el mismo alcance en Pure NAT; no confundir con los temporizadores globales de estados PF.

COMPROBACIÓN Probar sesiones de distinta duración en servicios que utilicen efectivamente NAT + Proxy.

4.6.4. Enable NAT Reflection for 1:1 NAT

Crea reglas de reflexión adicionales para que redes internas puedan acceder a destinos mapeados mediante NAT uno a uno por su dirección externa.

UTILIDAD Permite homogeneizar una URL o dirección publicada entre clientes externos e internos.

PRECAUCIÓN Solo cubre el componente de entrada; puede ser insuficiente si cliente y servidor comparten subred o si la ruta no regresa por el firewall.

COMPROBACIÓN Validar que el cliente recibe respuesta del servicio esperado y que no existe asimetría de retorno.

4.6.5. Enable automatic outbound NAT for Reflection

Crea reglas NAT de salida auxiliares para que, cuando cliente y servidor están en la misma subred, las respuestas regresen por el firewall.

UTILIDAD Puede completar el hairpin de Pure NAT y 1:1 NAT Reflection sin tener que definir todas las reglas manualmente en interfaces asignadas.

PRECAUCIÓN Oculta al servidor la IP original del cliente al sustituir su origen; puede afectar registros de auditoría. En interfaces no asignadas podrían requerirse reglas manuales.

COMPROBACIÓN Comprobar flujo completo, registro del servidor y NAT aplicado con captura de paquetes.

4.6.6. TFTP Proxy

Permite seleccionar las interfaces en las que se ejecuta el auxiliar de TFTP para clientes que acceden a servidores TFTP externos.

UTILIDAD Ayuda a protocolos TFTP que negocian transferencias a través de puertos dinámicos y se ven afectados por NAT.

PRECAUCIÓN No habilitar en interfaces que no necesitan TFTP; el selector de interfaces no debe confundirse con un permiso universal de firewall.

COMPROBACIÓN Verificar transferencia real de un archivo y revisar registros si falla la sesión.

4.7. State Timeouts — Caducidad de estados

Los siguientes campos expresan segundos, pero no deben rellenarse copiando números de otro sistema. En ausencia de un requisito concreto conviene dejar el campo sin definir para que rija el algoritmo de optimización seleccionado. Los tiempos dependen de fases del protocolo y no son límites universales para cada aplicación.

4.7.1. TCP

Campo	Qué representa	Síntoma si se reduce demasiado
TCP First	Primer paquete de una conexión TCP.	Pérdida de intentos que tardan en recibir respuesta.
TCP Opening	Conexión en establecimiento, antes de una respuesta.	Fallos en inicios de sesión o servicios lentos.
TCP Established	Conexión TCP establecida.	Cortes en sesiones persistentes poco activas.
TCP Closing	Una de las partes ha enviado FIN.	Cierres irregulares y retransmisiones.
TCP FIN Wait	Ambos extremos han enviado FIN y completan el cierre.	Desaparición temprana de los últimos segmentos.
TCP Closed	Conexión reiniciada o marcada como cerrada.	Eliminar demasiado pronto los rastros del cierre.
TCP Tsdiff	Tolerancia temporal de diferencias de marcas TCP.	Problemas en validación de marcas temporales TCP.

4.7.2. SCTP

SCTP es un protocolo de transporte orientado a asociaciones, usado en determinadas plataformas de telecomunicaciones. Algunas versiones muestran temporizadores específicos de SCTP. Su disponibilidad y significado deben comprobarse en la ayuda y documentación de la versión instalada.

Campo	Alcance práctico
SCTP First	Estado inicial del primer intercambio SCTP.
SCTP Opening	Fase de establecimiento de la asociación.
SCTP Established	Asociación SCTP operativa.
SCTP Closing	Cierre de la asociación.
SCTP Closed	Estado final/cerrado tras la terminación.

PRECAUCIÓN Si no se administran aplicaciones SCTP específicas, no modificar estos tiempos. La asociación y sus flujos multihoming requieren diagnóstico especializado.

4.7.3. UDP

Campo	Qué representa	Impacto a vigilar
UDP First	Primer datagrama observado.	Solicitudes iniciales que no reciben respuesta.
UDP Single	Existe tráfico inicial, pero no respuesta del extremo remoto.	Estados unidireccionales que expiran pronto.
UDP Multiple	Se observa tráfico en ambas direcciones.	Cortes en aplicaciones UDP de intercambios esporádicos.

4.7.4. ICMP

Campo	Qué representa
ICMP First	Primer intercambio ICMP que crea el estado.
ICMP Error	Tiempo aplicable a respuestas de error ICMP asociadas.

4.7.5. Other

Campo	Qué representa
Other First	Primer paquete de protocolos no incluidos en categorías anteriores.
Other Single	Tráfico sin respuesta observado para otros protocolos.
Other Multiple	Tráfico bidireccional de otros protocolos.

REGLA DE ORO Modificar un timeout solo cuando se ha identificado la aplicación, el patrón de inactividad y la fase precisa que causa el corte. Si existe un control por regla, valore esa intervención menos invasiva.

4.8. Procedimientos prácticos de diagnóstico

4.8.1. Cuando el firewall parece saturado

1. Consultar en el Dashboard el consumo de CPU, memoria y tabla de estados; no confundir una carga puntual con agotamiento sostenido.
2. Abrir Diagnostics → States y estudiar protocolos, orígenes y destinos con mayor número de estados.
3. Revisar registros y paquetes instalados que pueden multiplicar tablas de aliases; distinguir estado de conexión frente a entrada de tabla de alias.
4. Correlacionar los picos con horas de servicio y aplicaciones.
5. Cambiar umbrales solo si se demuestra que el límite es insuficiente para el hardware y la carga esperada.

4.8.2. Una VPN conecta, pero determinados archivos fallan

1. Probar una transferencia pequeña y otra de mayor tamaño para comparar el patrón.
2. Revisar MTU, PMTUD, DF y posibles retransmisiones en los extremos.
3. Comprobar si la encapsulación requiere MSS clamping y si la opción corresponde al túnel o a una interfaz VTI.
4. Cambiar un único parámetro por vez y repetir las pruebas.
5. Registrar la mejora o revertir el ajuste si no existe efecto reproducible.

4.8.3. El servicio publicado funciona desde Internet, no desde LAN

1. Comprobar la resolución DNS del nombre del servicio desde una red interna.
2. Si el nombre devuelve la dirección externa, valorar primero un Host Override o Split DNS.
3. Si se necesita reflexión NAT, confirmar el modo elegido y la existencia del port forward.
4. Si cliente y servidor comparten subred, revisar la necesidad de NAT de salida auxiliar.
5. Validar respuestas, registros del servidor y que la sesión no depende de un cambio accidental de rutas.

4.8.4. Multi-WAN con respuestas por enlace inesperado

1. Comprobar la política de routing aplicada por las reglas de la interfaz de entrada.
2. Verificar reply-to y los gateways asociados; evitar deshabilitarlo globalmente como primera medida.
3. Comprobar excepciones para destinos locales y VPN (negate rules o reglas manuales sin gateway).
4. Revisar la política Interface Bound/Floating States y la tabla de estados.
5. Usar capturas de paquetes desde ambas interfaces para confirmar el camino real del flujo.

4.8.5. Una nueva lista de aliases provoca errores de filtrado

1. Revisar validez TLS de la fuente si el alias se descarga por HTTPS.
2. Comprobar resolución DNS y formato/contenido del alias.
3. Inspeccionar límite Firewall Maximum Table Entries y mensajes de recarga de reglas.
4. Verificar el resultado en Status → Filter Reload y registros del sistema.
5. Restaurar la versión de lista anterior si el conjunto de reglas no carga correctamente.

4.9. Lista de verificación antes de guardar

Existe una copia reciente y accesible de la configuración.

Se dispone de acceso alternativo a la administración, preferiblemente consola local u otra vía segura.

Se ha identificado una incidencia medible y el parámetro que podría resolverla.

Se ha evaluado si una excepción por regla o interfaz evita un cambio global.

El efecto previsto sobre VPN, NAT, rutas y usuarios está documentado.

Existe un procedimiento de reversión y una ventana de mantenimiento cuando sea necesario.

Las pruebas posteriores incluyen servicio, DNS, rutas, estados y registros según el cambio.

> **NOTA OPERATIVA** Guardar un parámetro global puede afectar conexiones existentes o futuras; algunos cambios requieren reinicio para que la estructura interna entre plenamente en vigor. Realizar pruebas en un entorno autorizado y con retorno planificado.

4.10. Glosario de la pantalla

Término	Definición operativa
PF	Motor de filtrado de paquetes en el que se apoyan firewall y NAT.
State / estado	Registro que representa una conexión o intercambio conocido por el firewall.
Scrub	Normalización de paquetes y determinadas operaciones sobre fragmentos/encabezados.
DF	Indicador IPv4 «Don’t Fragment» para evitar fragmentación en ruta.
MTU	Tamaño máximo del paquete que soporta un enlace sin fragmentarse.
MSS	Tamaño máximo de datos TCP dentro de un segmento.
reply-to	Mecanismo de PF que fuerza el camino de retorno de conexiones entrantes.
NAT Reflection	Acceso desde redes internas a un servicio interno a través de su dirección externa.
Split DNS	Respuestas DNS distintas para el mismo nombre según el cliente sea interno o externo.
Bogon	Bloque IP reservado o no asignado para el uso previsto en Internet.

4.11. Conclusiones

Firewall & NAT es una pantalla de ajustes globales con impacto directo sobre la seguridad, el encaminamiento y la persistencia de conexiones. La estrategia más fiable consiste en conservar valores automáticos cuando funcionan, investigar la causa real de las incidencias y limitar las excepciones a los flujos que las necesitan.

En particular, la política de estados, los mecanismos de reensamblado y scrub, reply-to y las opciones de NAT Reflection deben revisarse con especial rigor cuando existen VPN, varias WAN o servidores publicados.

Fuentes técnicas y notas de versión

Referencia principal: Netgate, “Firewall & NAT”, https://docs.netgate.com/pfsense/en/latest/config/advanced-firewall-nat.html

Referencias complementarias: “NAT Reflection”, https://docs.netgate.com/pfsense/en/latest/nat/reflection.html; “Ethernet (Layer 2) Rules”, https://docs.netgate.com/pfsense/en/latest/firewall/ethernet-rules.html; “Troubleshooting Firewall Rules”, https://docs.netgate.com/pfsense/en/latest/troubleshooting/firewall.html

Los nombres de los controles y las opciones avanzadas pueden variar con la versión. NAT64 Prefix Override y los temporizadores SCTP solo deben ajustarse cuando estén disponibles y su efecto esté documentado para la instalación administrada.

05 System → Advanced → Networking

DHCP, direccionamiento IPv6, comportamiento de interfaces, optimizaciones de hardware y conectividad PPPoE.

Esta pantalla agrupa parámetros globales que influyen en cómo el firewall obtiene y entrega configuración de red, procesa IPv6 y utiliza los controladores de las interfaces. Muchos ajustes funcionan a nivel del sistema: pueden afectar a más de una interfaz o servicio.

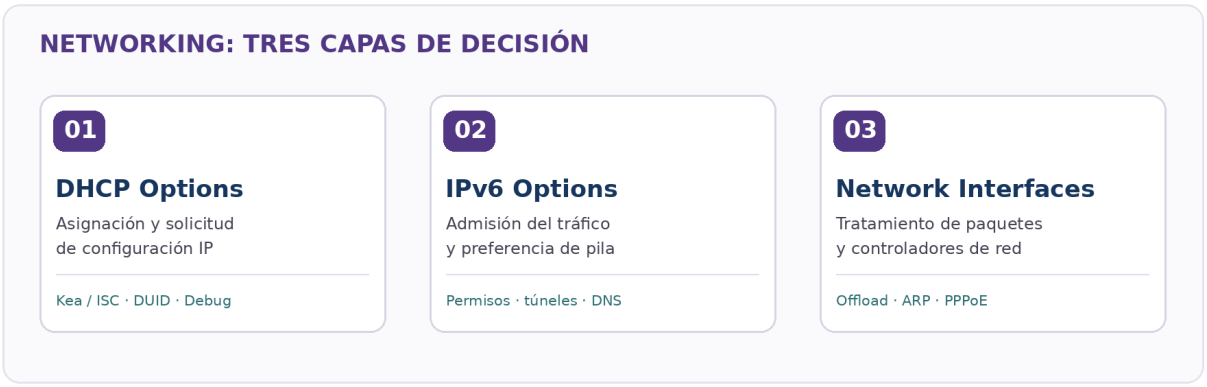


Figura 5.1. Mapa funcional de Networking; representación conceptual sin información de ninguna instalación.

Qué aprenderá el lector

Diferenciar la selección del servidor DHCP de los ajustes del cliente DHCPv6 y de los anuncios de enrutador (RA).

Interpretar las casillas de IPv6 sin confundir permitir tráfico con activar o desactivar toda la pila IPv6.

Comprender cuándo una función de offloading es útil, cuándo causa fallos y cómo diagnosticarla.

Aplicar los cambios de forma controlada, preservando el acceso administrativo y minimizando interrupciones.

CRITERIO PROFESIONAL Antes de modificar una opción global, documente el estado anterior, disponga de acceso alternativo y guarde una copia de configuración. No cambie varios parámetros a la vez.

5.1. Localización y visión general

Ruta de navegación: System → Advanced → Networking. Las pestañas vecinas incluyen Admin Access, Netgate Nexus, Firewall & NAT, Miscellaneous, System Tunables y Notifications. Este capítulo se limita a los controles visibles en Networking.

Grupo visible	Qué determina	Cuándo consultarlo
DHCP Options	Motor servidor DHCP, herramientas de depuración y DUID del cliente DHCPv6.	Cambios de backend, incidencias IPv6, prefijos del proveedor.
IPv6 Options	Reglas globales sobre IPv6, túneles, preferencia de protocolos y DNS local.	IPv6 no funciona, resolución por nombre errática, coexistencia IPv4/IPv6.
Network Interfaces	Descarga de tareas a NIC, soporte ALTQ, ARP, estados y PPPoE.	Tráfico que falla en una VM, rendimiento, cortes tras cambios de WAN.

Las denominaciones se mantienen en inglés tal como aparecen en la interfaz. Su presencia y posición pueden variar entre versiones de pfSense Plus; las explicaciones relacionan los controles con la documentación técnica de Netgate.

5.2. DHCP Options — Opciones de DHCP

El primer grupo mezcla ajustes del servidor DHCP (entrega de direcciones a equipos clientes) con parámetros del cliente DHCPv6 del propio firewall (obtención de dirección o prefijo de un proveedor). Son funciones diferentes y no deben confundirse.

5.2.1. Server Backend — Motor servidor DHCP

Permite escoger qué implementación presta el servicio DHCP a los clientes de la red. La selección repercute en DHCPv4 y DHCPv6 según las capacidades y ajustes de la edición instalada.

Opción	Qué significa	Criterio de administración
Kea DHCP	Motor moderno mantenido por ISC; evolución principal del servicio DHCP.	Opción recomendada para nuevas configuraciones, previa revisión de funciones utilizadas.
ISC DHCP (Deprecated)	Motor heredado cuyo ciclo de mantenimiento finalizó.	Mantener solo si una dependencia exige su uso y existe un plan de migración.
Ignore Deprecation Warning	Oculta el aviso de obsolescencia del backend ISC.	No elimina vulnerabilidades ni prolonga el soporte del producto.

QUÉ HACE Cambiar Kea/ISC modifica el servicio que responde a las solicitudes DHCP de los clientes.

VENTAJA Facilita la transición a una implementación moderna y permite conservar temporalmente el legado cuando sea imprescindible.

PRECAUCIÓN No conmutar en producción sin inventario de reservas, opciones DHCP, registro DNS y HA. Pueden existir diferencias de configuración y disponibilidad durante la migración.

COMPROBACIÓN Revisar estado del servidor, concesiones activas, DNS interno y registros; obtener o renovar una concesión en una estación de pruebas.

CRITERIO PROFESIONAL Kea dispone actualmente de integración para registrar nombres de clientes en DNS Resolver, pero las funciones disponibles han evolucionado entre versiones. No deben asumirse limitaciones documentadas para versiones antiguas como si fuesen permanentes.

5.2.2. RADVD Debug — Depuración de anuncios IPv6

QUÉ HACE Al habilitar “Log all radvd log levels”, radvd registra mensajes más detallados sobre los Router Advertisements (RA) que facilitan la autoconfiguración IPv6.

VENTAJA Ayuda a averiguar por qué los clientes no reciben correctamente información de su red IPv6.

PRECAUCIÓN Incrementa la cantidad de registros; no constituye una solución automática al fallo ni activa por sí misma RA.

COMPROBACIÓN Revisar registros de enrutamiento, comparar anuncios antes y después y desactivar el detalle extra al terminar el diagnóstico.

5.2.3. DHCP6 Debug — Depuración del cliente DHCPv6

QUÉ HACE Inicia el cliente DHCPv6 del firewall en modo de depuración para mostrar información adicional de negociaciones y respuestas.

VENTAJA Permite investigar fallos de obtención de dirección IPv6 o delegación de prefijos del proveedor.

PRECAUCIÓN El mayor volumen de mensajes debe mantenerse solo mientras se reproduce el problema.

COMPROBACIÓN Contrastar eventos del cliente DHCPv6 con el estado de la interfaz y con los registros; registrar el momento del fallo.

5.2.4. Do not allow PD/Address release

QUÉ HACE Impide que dhcp6c envíe al proveedor una liberación de la dirección o del prefijo IPv6 al cerrar la sesión.

VENTAJA Puede evitar que ciertos proveedores liberen inmediatamente un prefijo que se desea conservar tras reinicios o reconexiones.

PRECAUCIÓN No asegura que el operador entregue siempre el mismo prefijo: intervienen su política de concesiones y la duración de los arrendamientos.

COMPROBACIÓN Tras una reconexión controlada, verificar prefijo delegado, rutas y conectividad de clientes IPv6.

5.2.5. DHCP6 DUID — Identificador del cliente DHCPv6

El DUID (DHCP Unique Identifier) identifica al solicitante en intercambios DHCPv6. No es una dirección IP ni debe tratarse como una contraseña. En la mayoría de instalaciones debe mantenerse la generación automática; conviene fijarlo solo cuando existe una razón operativa, como conservar identidad ante reinstalaciones o requisitos del operador.

Formato	Cómo se construye	Cuándo puede ser relevante
Raw DUID	Valor completo del identificador tal como se conserva en fichero o registro.	Reutilizar exactamente un identificador previamente asignado.
DUID-LLT	Tipo de enlace, dirección de enlace y tiempo de generación.	Identificador creado a partir de enlace físico y momento.
DUID-EN	Número de empresa y un identificador definido por el fabricante.	Ambientes en que el proveedor exige un DUID de empresa.
DUID-LL	Identificador basado en la dirección del enlace.	Identidad estable basada en el dispositivo de red.
DUID-UUID	Identificador universal único del sistema.	Cuando se emplea un UUID para identificar al cliente.

Raw DUID y botón Copy DUID

Al seleccionar Raw DUID aparece un campo para consignar el identificador. Copy DUID copia al campo el valor detectado por el sistema. El botón facilita conservar la identidad existente, especialmente si el servicio cambia de soporte o se recrea la configuración.

La modificación puede requerir reinicio o reconfiguración de las interfaces WAN para que el cliente vuelva a negociar utilizando el nuevo identificador. Si /var reside en RAM, guardar un DUID estable puede evitar cambios no deseados entre arranques.

COMPROBACIÓN Antes de cambiar nada, verificar en los registros qué identificador utiliza el cliente; después comprobar si la negociación y la delegación IPv6 son coherentes. No publicar el DUID de producción en capturas o anexos.

5.3. IPv6 Options — Comportamiento de IPv6

5.3.1. Allow IPv6

QUÉ HACE Al estar marcada, permite que las reglas configuradas y automáticas puedan procesar tráfico IPv6. Al desmarcarla se impone un bloqueo global del tráfico IPv6 que atraviesa el filtro.

VENTAJA Es un control central para decidir si el firewall transporta IPv6.

PRECAUCIÓN No desactiva todas las funciones IPv6 internas ni borra su configuración; tampoco permite automáticamente todos los paquetes IPv6 cuando está marcada.

COMPROBACIÓN Comprobar reglas IPv6, gateways y tráfico de prueba; no evaluar solo la presencia de una dirección IPv6 en una interfaz.

5.3.2. IPv6 over IPv4 Tunneling

QUÉ HACE Habilita la redirección de tráfico IPv6 encapsulado en IPv4 mediante el protocolo IP número 41 hacia el extremo interno de túnel previsto por la configuración.

VENTAJA Permite escenarios de transporte IPv6 sobre una infraestructura IPv4 cuando existe un terminador del túnel detrás del firewall.

PRECAUCIÓN No es una VPN cifrada ni debe confundirse con NAT convencional. Debe existir una regla de WAN que permita el protocolo 41 cuando se requiera.

COMPROBACIÓN Inspeccionar la entrada del protocolo 41, la configuración del extremo del túnel y la conectividad IPv6 resultante.

5.3.3. Prefer IPv4 over IPv6

QUÉ HACE Hace que el propio firewall priorice IPv4 cuando un nombre de destino dispone tanto de registro IPv4 como IPv6.

VENTAJA Puede facilitar actualizaciones o consultas externas del propio firewall cuando IPv6 está parcialmente operativo.

PRECAUCIÓN No modifica la preferencia de los ordenadores, teléfonos ni demás clientes que están detrás del firewall; tampoco repara una ruta IPv6 rota.

COMPROBACIÓN Probar desde pfSense resolución DNS y conectividad saliente por cada familia de direcciones.

5.3.4. IPv6 DNS entry

QUÉ HACE Al marcar “Do not generate local IPv6 DNS entries for LAN interfaces”, evita crear registros locales IPv6 del propio firewall en determinadas interfaces LAN.

VENTAJA Puede prevenir que la administración por nombre resuelva a una dirección IPv6 dinámica o temporalmente ausente.

PRECAUCIÓN Reduce la disponibilidad de resolución local del firewall por IPv6; no elimina registros externos ni cambia la configuración DNS de los clientes.

COMPROBACIÓN Comprobar registros resueltos para el nombre del firewall y repetir la prueba después de una pérdida o renovación de prefijo.

CRITERIO PROFESIONAL No confundir “Prefer IPv4 over IPv6” (elección del protocolo por el firewall) con “IPv6 DNS entry” (creación de registros de nombre del firewall). Una opción modifica preferencias de conexión; la otra, entradas DNS locales.

5.4. Network Interfaces — Interfaces de red

Estas opciones afectan al modo en que el sistema operativo y las tarjetas de red intercambian y procesan paquetes. Una casilla que comienza por “Disable” realiza lo contrario de una función de activación: al marcarla se desactiva la aceleración o característica indicada.

5.4.1. Hardware Checksum Offloading

QUÉ HACE Al marcar “Disable hardware checksum offload” se impide descargar en la tarjeta de red el cálculo o la validación de checksums.

VENTAJA Puede evitar errores de paquetes, pérdida de rendimiento o comunicaciones anómalas en determinados controladores físicos y adaptadores virtualizados.

PRECAUCIÓN Cuando el hardware funciona correctamente, el offloading puede ahorrar CPU. Desactivarlo indiscriminadamente no mejora por definición el rendimiento.

COMPROBACIÓN Reproducir el fallo, capturar tráfico en ambos extremos y evaluar contadores de errores. Aplicar el ajuste y reiniciar o reconfigurar la interfaz según proceda.

NOTA DE DIAGNÓSTICO Con checksum offload activo, una captura tomada antes del procesamiento por hardware puede mostrar sumas incorrectas o vacías sin que exista corrupción real en la red.

5.4.2. Hardware TCP Segmentation Offloading (TSO)

QUÉ HACE Al marcar “Disable hardware TCP segmentation offload”, la NIC deja de realizar la segmentación TCP que normalmente podría delegarle el sistema operativo.

VENTAJA Evita una fuente de incompatibilidades y carga adicional en equipos que encaminan tráfico ajeno, en lugar de actuar como un host final.

PRECAUCIÓN En firewalls y routers Netgate aconseja mantener TSO desactivado; cambiar la casilla a ciegas puede causar degradación o problemas con IPv6.

COMPROBACIÓN Medir el funcionamiento de TCP y el rendimiento real, revisar registros y conservar la opción de desactivación cuando sea la configuración recomendada.

5.4.3. Hardware Large Receive Offloading (LRO)

QUÉ HACE Al marcar “Disable hardware large receive offload”, la NIC no agrupa paquetes recibidos antes de entregarlos al sistema operativo.

VENTAJA Evita demoras y reprocesamiento que pueden perjudicar al encaminamiento cuando los paquetes deben seguir hacia otra interfaz.

PRECAUCIÓN Aunque LRO puede beneficiar a servidores que consumen tráfico local, normalmente resulta inadecuado para un firewall o router.

COMPROBACIÓN Evaluar latencia, caudal y estabilidad del tráfico reenviado antes y después, con pruebas comparables.

Función	Operación de hardware	Por qué debe vigilarse en firewall
Checksum	Calcula/verifica checksums.	Controladores defectuosos pueden ocasionar descartes o errores aparentes.
TSO	Divide segmentos TCP grandes.	Puede interferir con tráfico encaminado o reducir rendimiento.
LRO	Agrupa paquetes recibidos.	Puede retrasar reenvío y exigir segmentación posterior.

5.4.4. Virtual NIC ALTQ support

QUÉ HACE Activa soporte de ALTQ en adaptadores virtuales como vtnet y hn para ciertos mecanismos de gestión de colas y limitación del tráfico.

VENTAJA Permite utilizar funciones de traffic shaping que dependen de ALTQ en esos controladores.

PRECAUCIÓN Puede deshabilitar multiqueue y reducir la capacidad máxima de procesamiento. El cambio requiere reiniciar el firewall.

COMPROBACIÓN Comprobar que las colas previstas funcionan y comparar latencia y rendimiento antes y después, sin sacrificar capacidad sin necesidad.

5.4.5. ARP Handling — Suppress ARP messages

QUÉ HACE Silencia registros originados cuando la asociación entre una dirección IP y una MAC cambia en la red local.

VENTAJA Reduce ruido en registros de entornos donde estos cambios son esperables y están justificados.

PRECAUCIÓN Puede ocultar señales de conflicto IP, cambios de equipo no planificados o comportamientos anómalos; normalmente interesa conservar los avisos.

COMPROBACIÓN Antes de silenciar, identificar el motivo de los cambios ARP y correlacionarlos con switches y endpoints.

5.4.6. Reset All States

QUÉ HACE Al marcar “Reset all states if WAN IP Address changes”, borra toda la tabla de estados cuando cambia la dirección IP de la conexión WAN, en vez de eliminar solo los estados vinculados a la antigua IP.

VENTAJA Puede ayudar en escenarios específicos de cambios frecuentes de dirección donde quedan estados obsoletos.

PRECAUCIÓN Interrumpe todas las sesiones registradas, incluso las no relacionadas directamente con la WAN afectada. No suele ser necesario habilitarlo de forma general.

COMPROBACIÓN Comparar desconexiones, cambios de dirección y ocupación de estados; planificar cualquier prueba por su impacto en usuarios.

5.4.7. Use if_pppoe kernel module for PPPoE client

QUÉ HACE Al activar esta opción, pfSense utiliza el controlador PPPoE del kernel if_pppoe en lugar del mecanismo heredado basado en mpd5 para las interfaces PPPoE afectadas.

VENTAJA Puede ofrecer una implementación más eficiente del enlace PPPoE.

PRECAUCIÓN No admite necesariamente prestaciones antiguas como MLPPP; los dos backends PPPoE no pueden usarse simultáneamente. Cambiarlo interrumpe la conectividad de las conexiones PPPoE afectadas.

COMPROBACIÓN Realizar la operación en ventana de mantenimiento, confirmar renegociación PPPoE y comprobar gateway, DNS y navegación después del cambio.

CAMBIO POTENCIALMENTE DISRUPTIVO Nunca cambie el backend PPPoE desde una única sesión remota sin acceso alternativo. La caída temporal de la WAN puede dejar sin posibilidad de revertir el ajuste.

5.5. Procedimientos prácticos de diagnóstico

Caso A. Los clientes dejan de obtener dirección tras migrar DHCP

1. Anotar el backend previo y las funciones utilizadas: reservas, opciones especiales, HA y registro DNS.
2. Comprobar que el servicio del nuevo backend está activo y que la configuración de cada interfaz ha quedado aplicada.
3. Revisar registros DHCP y conceder/renovar una concesión desde un único cliente de pruebas.
4. Confirmar que el cliente obtiene los parámetros esperados y que la resolución de nombres funciona.
5. Si hay incidencias, restaurar el estado anterior siguiendo el procedimiento de reversión documentado.

Objetivo: aislar si el problema afecta al backend, al alcance DHCP de una interfaz o a servicios dependientes como DNS.

Caso B. El firewall obtiene IPv4, pero no recibe prefijo IPv6

1. Comprobar la configuración IPv6 de la WAN y el estado del cliente DHCPv6.
2. Habilitar temporalmente DHCP6 Debug y revisar los mensajes de solicitud, respuesta o fallo.
3. Verificar si existe delegación de prefijo y si las interfaces internas pueden utilizarlo.
4. Valorar “Do not allow PD/Address release” solamente si se ha identificado ese comportamiento específico del proveedor.
5. Desactivar la depuración tras documentar las evidencias y verificar conectividad de clientes.

Objetivo: diferenciar un problema de negociación DHCPv6 de un bloqueo por reglas IPv6 o una ausencia de Router Advertisements.

Caso C. pfSense virtualizado presenta cortes o errores de red

1. Confirmar el tipo de adaptador de red virtual y revisar contadores de errores.
2. Comprobar el estado de las opciones Checksum Offloading, TSO y LRO.
3. Si el entorno es compatible con la recomendación de Netgate para VirtIO, verificar “Disable hardware checksum offload”.
4. Aplicar una sola modificación y, si corresponde, reiniciar el firewall en una ventana controlada.
5. Repetir pruebas de tráfico, revisar logs y comparar resultados con los obtenidos antes del cambio.

Objetivo: investigar incompatibilidades de NIC y offloading antes de concluir que el problema es una regla de firewall.

Caso D. Caen conexiones después de un cambio de WAN

1. Comprobar el evento de cambio de dirección y los estados asociados.
2. Determinar si los cortes afectan únicamente a la WAN que cambió o a todas las sesiones.
3. Revisar la opción Reset All States y el comportamiento de gateways y rutas.
4. Evitar activar un borrado global de estados sin necesidad, especialmente con VPN y sesiones empresariales activas.

Objetivo: entender las consecuencias de limpiar estados y evitar intervenciones que amplíen una interrupción localizada.

5.6. Matriz de riesgos y cambios

Cambio o control	Impacto potencial	Cómo proceder
Kea ↔ ISC	Pérdida temporal de DHCP, cambios de comportamiento en DNS/HA.	Copia, inventario de funciones, prueba cliente y reversión.
DUID / DHCPv6	Renegociación de identidad y posible variación de prefijos.	Confirmar requisito del proveedor y guardar situación anterior.

Cambio o control	Impacto potencial	Cómo proceder
Allow IPv6	Bloqueo global del tráfico IPv6 si se desmarca.	Revisar reglas y rutas IPv6 antes de modificar.
Checksum / TSO / LRO	Variación de rendimiento; posible necesidad de reconfigurar o reiniciar.	Modificar de uno en uno, medir y revertir si empeora.
Virtual NIC ALTQ	Reinicio y posible pérdida de capacidad multiqueue.	Validar necesidad de ALTQ y realizar pruebas comparativas.
Reset All States	Corte generalizado de sesiones cuando cambie la WAN.	Habilitar solo tras diagnóstico claro.
if_pppoe	Interrupción de la conexión WAN PPPoE.	Mantenimiento con acceso alternativo.

5.7. Lista de comprobación del administrador

¿Se ha identificado la versión exacta de pfSense Plus y las funciones disponibles?

¿Existe una copia reciente de la configuración y acceso alternativo?

¿Se conoce qué casilla activa o desactiva una función por su redacción exacta?

¿Se ha documentado el problema que motiva el cambio?

¿Se han planificado pruebas de conectividad, DHCP, DNS, IPv6 y VPN, cuando apliquen?

¿Se ha definido cómo revertir el cambio y cuándo hacerlo?

¿Se han desactivado los modos de depuración que ya no son necesarios?

5.8. Glosario esencial

Concepto	Significado práctico
DHCP backend	Programa que gestiona concesiones y parámetros de red para clientes.
DHCPv6 DUID	Identificador persistente del cliente en negociaciones DHCPv6.
Prefix Delegation (PD)	Delegación de un prefijo IPv6 que puede utilizarse en redes internas.
RADVD / RA	Servicio y mensajes de anuncio de routers para autoconfiguración IPv6.
Offloading	Delegación de tareas de procesamiento de paquetes a la tarjeta de red.
TSO / LRO	Segmentación TCP de salida / agrupación de paquetes de entrada mediante hardware.
ALTQ	Infraestructura de colas utilizada por determinados mecanismos de control de tráfico.
ARP	Protocolo que relaciona direcciones IPv4 con direcciones de enlace en una LAN.
State table	Conjunto de conexiones reconocidas y seguidas por el firewall.
PPPoE	Encapsulación de sesiones PPP sobre Ethernet, usada en ciertos accesos WAN.

5.9. Referencias técnicas

Netgate Documentation. “Networking — Advanced Configuration Options”.
https://docs.netgate.com/pfsense/en/latest/config/advanced-networking.html

Netgate Documentation. “DHCP” y “Kea Settings Tab”.
https://docs.netgate.com/pfsense/en/latest/services/dhcp/ |
https://docs.netgate.com/pfsense/en/latest/services/dhcp/kea-settings.html

Netgate Documentation. “Virtualizing with Proxmox VE” y “Hardware Tuning and Troubleshooting”.
https://docs.netgate.com/pfsense/en/latest/recipes/virtualize-proxmox-ve.html |
https://docs.netgate.com/pfsense/en/latest/hardware/tune.html

Las notas corresponden a las funciones documentadas en esta pantalla; las opciones exactas pueden evolucionar con las versiones de pfSense Plus.

06 System → Advanced → Miscellaneous

Conectividad saliente, balanceo, ahorro energético, hardware criptográfico, estados, pasarelas, memoria y almacenamiento.

La pestaña Miscellaneous agrupa ajustes globales que no pertenecen a una única interfaz o servicio. Algunos modifican la resiliencia del sistema y otros su consumo de recursos. La mayoría deben conservarse en su estado habitual salvo que exista una necesidad de administración, rendimiento o diagnóstico.



Figura 6.1. Mapa conceptual de Miscellaneous; esquema sin direcciones, nombres ni parámetros de ninguna instalación.

Qué aprenderá el lector

Configurar el uso de un proxy para las conexiones salientes del propio firewall.

Comprender el efecto de las conexiones persistentes (sticky) en Multi-WAN.

Distinguir funciones de ahorro de energía, aceleración criptográfica y sensores de temperatura.

Controlar las sesiones durante fallos y recuperaciones de gateways sin causar cortes innecesarios.

Evaluar el uso de discos RAM, la memoria de PHP y el tratamiento de registros.

CRITERIO DE ADMINISTRACIÓN Los nombres de controles reproducen los rótulos técnicos de la interfaz. No se publican valores configurados, direcciones de gestión, credenciales ni detalles de topología; los ejemplos se describen sin identificadores concretos.

6.1. Localización y estructura de la pantalla

Ruta: System → Advanced → Miscellaneous. La página reúne secciones independientes, de forma que Save guarda los ajustes aplicables según el comportamiento de cada opción. Algunas requieren reiniciar el equipo o interrumpen sesiones activas. Conviene obtener una copia de configuración y disponer de acceso alternativo antes de intervenir.

Área visible	Propósito principal	Riesgo operativo
Proxy Support	Acceso del firewall a Internet mediante proxy	Actualizaciones y paquetes inaccesibles
Load Balancing	Persistencia de rutas en conexiones Multi-WAN	Sesiones cortadas o mal distribuidas
Power Savings - PowerD	Cambios de frecuencia del procesador	Latencia o ahorro energético insuficiente
Cryptographic & Thermal Hardware	Aceleración de VPN y monitorización térmica	Incompatibilidad de hardware
Schedules / Gateway Monitoring	Estados ante horarios y fallos de gateways	Cortes y salida por enlaces no previstos

Área visible	Propósito principal	Riesgo operativo
PHP / RAM Disk / Hardware / Feedback	Recursos, disco e identificación	Consumo de RAM, pérdida de registros

6.2. Proxy Support — Proxy de salida

Estos campos se aplican a las conexiones salientes que realiza el propio pfSense Plus, por ejemplo al consultar repositorios o descargar paquetes. No convierten el firewall en un servidor proxy para todos los usuarios de la LAN. Para el tráfico de clientes se necesitan otras funciones y políticas de red.

6.2.1. Proxy URL

QUÉ HACE Identifica el servidor proxy por nombre DNS o dirección de red para las conexiones salientes compatibles del sistema.

VENTAJA Permite que el firewall alcance servicios externos cuando la red corporativa obliga a utilizar proxy.

PRECAUCIÓN No confundir el campo con la dirección de la administración web ni añadir rutas de páginas en lugar de la identidad del proxy.

COMPROBACIÓN Probar desde el firewall una función que necesite Internet, como consultar actualizaciones o repositorios, y revisar registros de conexión.

6.2.2. Proxy Port

QUÉ HACE Selecciona el puerto TCP en el que escucha el servidor proxy. La documentación cita puertos habituales, pero el correcto lo define el administrador del proxy.

VENTAJA Permite adaptar el firewall a un servicio proxy que escucha en un puerto no estándar.

PRECAUCIÓN Un puerto equivocado puede impedir el acceso a servicios de mantenimiento incluso cuando el proxy responde por otros medios.

COMPROBACIÓN Revisar la combinación servidor/puerto, conectividad y posibles restricciones de cortafuegos intermedios.

6.2.3. Proxy Username

QUÉ HACE Usuario para autenticarse ante el proxy cuando el servidor exige identidad.

VENTAJA Facilita operar en redes con políticas de acceso autenticado.

PRECAUCIÓN Evitar credenciales de privilegio excesivo o asociadas a personas; usar, cuando proceda, una cuenta de servicio controlada.

COMPROBACIÓN Comprobar que la consulta de paquetes funciona sin errores de autenticación.

6.2.4. Proxy Password / Confirm

QUÉ HACE Contraseña del usuario de proxy y su confirmación para evitar errores de escritura.

VENTAJA Impide que un fallo tipográfico inutilice la autenticación saliente.

PRECAUCIÓN No reproducir credenciales en documentación, capturas, tickets ni registros. Respetar las políticas de custodia de secretos.

COMPROBACIÓN Guardar y realizar una operación de red controlada; si falla, revisar autenticación en origen y en el servidor proxy.

EJEMPLO PRÁCTICO Si un firewall no puede consultar las actualizaciones mientras las estaciones autorizadas sí pueden navegar, comprobar si el equipo necesita configurar un proxy de salida. Una prueba desde el firewall discrimina un problema de proxy de un problema de DNS o gateway.

6.3. Load Balancing — Persistencia entre gateways

En un grupo de gateways configurado para repartir conexiones, varias conexiones sucesivas pueden salir por WAN diferentes. Algunas aplicaciones necesitan mantener una procedencia externa consistente durante una sesión. Sticky connections intenta conservar la asociación de un origen con un gateway mientras exista una referencia de estado.

6.3.1. Use sticky connections

QUÉ HACE Vincula las conexiones de un mismo origen con el gateway elegido, en lugar de distribuir cada nueva conexión de forma independiente mientras la asociación siga vigente.

VENTAJA Reduce problemas en servicios que esperan que varias conexiones relacionadas compartan la misma salida pública.

PRECAUCIÓN Puede disminuir la eficiencia del reparto: un único cliente con mucho tráfico puede concentrar carga en un enlace. No suma los anchos de banda como si fueran una única línea.

COMPROBACIÓN Probar una aplicación con varias conexiones y verificar en los estados y en el tráfico WAN que mantiene una salida coherente.

6.3.2. Source tracking timeout

QUÉ HACE Define cuánto tiempo, en segundos, se mantiene la asociación del origen una vez que dejan de existir los estados que la sustentaban. El comportamiento predeterminado elimina la asociación cuando expiran los estados.

VENTAJA Evita que un usuario salte prematuramente a otra WAN entre varias conexiones separadas por períodos de inactividad.

PRECAUCIÓN Un tiempo demasiado alto prolonga asociaciones poco convenientes durante cambios de carga o disponibilidad.

COMPROBACIÓN Medir el comportamiento de una aplicación que pierde sesión en Multi-WAN y ajustar solo si se confirma relación con la persistencia.

DIFERENCIA CLAVE Sticky connections no sustituye una regla de policy routing ni configura por sí sola los grupos de gateways. Tampoco garantiza continuidad de una sesión TCP cuya IP pública de salida cambia durante una caída.

6.4. Power Savings - PowerD — Gestión de energía

6.4.1. Enable PowerD

QUÉ HACE Activa el servicio powerd para regular dinámicamente la frecuencia del procesador según la carga y el estado de alimentación cuando el hardware lo permite.

VENTAJA Puede reducir consumo eléctrico y disipación térmica con poca actividad.

PRECAUCIÓN El efecto real depende del hardware, del soporte del procesador y de otros mecanismos de energía. Algunos equipos no obtienen ahorros medibles.

COMPROBACIÓN Observar frecuencia de CPU, carga, temperatura, latencia y consumo si se dispone de medición fiable.

6.4.2. Modos disponibles en AC, Battery y Unknown Power

AC Power define la política con alimentación de red; Battery Power la aplica si el sistema identifica funcionamiento con batería; Unknown Power se utiliza cuando la fuente no puede determinarse. La detección varía según equipo y controladores.

Modo	Funcionamiento	Cuándo valorarlo
Maximum	Mantiene la mayor frecuencia o rendimiento disponible.	Pruebas de latencia o necesidad de respuesta máxima.
Minimum	Favorece la frecuencia más baja para reducir consumo.	Entornos muy poco exigentes, siempre con pruebas.
Adaptive	Aumenta rendimiento al crecer la carga y lo reduce cuando se encuentra inactivo.	Equilibrio entre respuesta y ahorro energético.
Hiadaptive	Reacciona antes al aumento de carga y tarda más en reducir frecuencia.	Cuando la interactividad y la baja latencia tienen prioridad.

Las opciones AC Power, Battery Power y Unknown Power presentan las mismas modalidades. Elegir Hiadaptive o Maximum no crea capacidades de CPU inexistentes; únicamente modifica cómo se aprovechan las disponibles. La documentación también describe Speed Shift en plataformas compatibles: si aparece esa característica, su interacción con PowerD debe revisarse antes de activar ambos mecanismos.

COMPROBACIÓN Tras cambiar PowerD, comparar condiciones semejantes de carga y tráfico. Un menor porcentaje de frecuencia no equivale necesariamente a menor consumo o mejor temperatura.

6.5. Cryptographic & Thermal Hardware

6.5.1. IPsec-MB — Aceleración criptográfica

QUÉ HACE Activa IPsec Multi-Buffer para utilizar rutinas optimizadas mediante instrucciones SIMD de CPU en cifrados compatibles. La opción puede acelerar flujos de IPsec, OpenVPN DCO o WireGuard cuando los algoritmos y la plataforma lo permiten.

VENTAJA Puede elevar el rendimiento de túneles y reducir carga de CPU durante cifrado intensivo.

PRECAUCIÓN No asegura una mejora en todos los equipos ni en cualquier cifrado. Puede competir con aceleradores dedicados y requiere reinicio para su aplicación según la interfaz.

COMPROBACIÓN Medir rendimiento del túnel y carga de CPU antes/después, usando tráfico comparable y revisando los registros del subsistema criptográfico.

6.5.2. Cryptographic Hardware

QUÉ HACE Selecciona módulos de aceleración compatibles con el equipo. En la interfaz estudiada aparecen None y SafeXcel and BSD Crypto Device (safexcel, cryptodev); otras plataformas pueden mostrar controladores distintos.

VENTAJA Permite aprovechar chips criptográficos dedicados cuando la arquitectura los soporta.

PRECAUCIÓN No seleccionar módulos por analogía con otros equipos. Cambiar módulos puede requerir reinicio y no implica que todos los protocolos los vayan a usar.

COMPROBACIÓN Confirmar detección del acelerador en el sistema y comparar el coste de CPU y la velocidad real de VPN.

6.5.3. Thermal Sensors

QUÉ HACE Escoge el controlador para leer la temperatura de CPU o placa: None/ACPI, Intel Core o AMD K8/K10/K11, según compatibilidad.

VENTAJA Aporta observabilidad sobre calentamiento y ayuda a correlacionar carga, ventilación y funcionamiento.

PRECAUCIÓN Elegir un controlador no compatible puede no mostrar datos. La temperatura del núcleo no equivale necesariamente a la del interior del equipo.

COMPROBACIÓN Consultar las lecturas mediante el widget térmico si existe o herramientas de diagnóstico; comprobar coherencia con la carga.

MATIZ DE VERSIÓN Las opciones de aceleración y sensores varían según procesador, hardware y edición. La lista anterior reproduce únicamente las opciones de esta pantalla; no debe generalizarse a cualquier dispositivo.

6.6. Schedules — Comportamiento al vencer un horario

6.6.1. Do not kill connections when schedule expires

QUÉ HACE Si se marca, al expirar un horario de una regla no se eliminan automáticamente las sesiones ya establecidas; se impide lo nuevo según la evaluación posterior de las reglas, pero las sesiones existentes pueden continuar.

VENTAJA Evita interrumpir bruscamente operaciones iniciadas dentro de una franja autorizada.

PRECAUCIÓN En redes con horarios estrictos de seguridad, permitir que persistan sesiones contradice el corte inmediato esperado.

COMPROBACIÓN Abrir una conexión de prueba durante el horario, mantenerla tras la expiración y comprobar si la sesión continúa como prescribe la política.

6.7. Gateway Monitoring — Fallo y recuperación de enlaces

Estas opciones modifican cómo se eliminan estados cuando un gateway falla o se recupera. Un estado representa el seguimiento de una comunicación por el firewall. Borrarlo obliga normalmente a la aplicación a establecer una nueva conexión; esto puede facilitar que use otro camino, pero también puede interrumpir llamadas, VPN y sesiones en curso.

6.7.1. State Killing on Gateway Recovery

Se aplica al comportamiento de recuperación cuando el gateway predeterminado es un grupo de failover. La selección determina qué estados de gateways de menor prioridad se limpian al volver el gateway preferente.

Opción de la pantalla	Qué provoca	Implicación
Don’t kill states from the firewall itself	No fuerza el borrado de estados propios del firewall por esta política.	Menos interrupciones; ciertas conexiones pueden continuar por la WAN de respaldo.
Kill all states for lower-priority gateways	Elimina todos los estados que usan gateways de prioridad inferior.	Regreso más agresivo a la WAN prioritaria, con cortes de sesiones.
Only kill policy routing states for lower-priority gateways	Limita el borrado a estados creados con enrutamiento por política.	Cambio más selectivo; reduce el impacto en estados ajenos a policy routing.
Only kill states with the same address family as the gateway group	Filtra el borrado por familia IPv4 o IPv6 del grupo.	Evita afectar indiscriminadamente comunicaciones de otra familia.

6.7.2. Don’t kill policy routing states for lower-priority gateways

QUÉ HACE Al marcar esta casilla, evita el comportamiento global que elimina estados de policy routing por gateways de prioridad inferior cuando vuelve el principal. Los grupos pueden tener ajustes específicos que modifiquen ese comportamiento.

VENTAJA Reduce interrupciones de sesiones que funcionan por el enlace de respaldo.

PRECAUCIÓN Pueden mantenerse comunicaciones existentes por una WAN secundaria hasta que finalicen o sean reiniciadas.

COMPROBACIÓN Forzar en un entorno de pruebas la recuperación de un gateway y observar la salida de conexiones existentes y nuevas.

6.7.3. State Killing on Gateway Failure

Modo	Qué sucede	Precaución
Do not kill states on gateway failure	No realiza limpieza automática de estados por esta causa.	Algunas aplicaciones esperan a que caduquen sus sesiones.
Kill states for all gateways which are down	Intenta limpiar estados asociados a gateways caídos cuyo estado contiene información de gateway (policy routing o reply-to).	No necesariamente alcanza estados originados por simple cambio del gateway predeterminado.
Flush all states on gateway failure	Vacía la tabla de estados completa cuando se dispara la condición de fallo.	Muy disruptivo: puede cortar conexiones ajenas al enlace afectado.

La política puede estar condicionada por la monitorización habilitada y por overrides configurados en gateways. Las respuestas no deben asumirse idénticas ante la pérdida de cable, la caída del monitor y un cambio de rutas.

6.7.4. Skip rules when gateway is down

QUÉ HACE Si se marca “Do not create rules when gateway is down”, la regla de policy routing cuyo gateway está caído se omite; de lo contrario, pfSense puede crearla sin ese gateway y dejar que el tráfico use el gateway por defecto.

VENTAJA Permite evitar que determinados tráficos utilicen rutas alternativas al enlace previsto.

PRECAUCIÓN Al desaparecer la regla, otra regla inferior podría permitir una salida inesperada. Añadir una regla posterior de bloqueo/rechazo para el mismo tráfico si se necesita prohibición absoluta.

COMPROBACIÓN Simular caída del gateway y verificar qué regla toma el tráfico, qué salida utiliza y qué muestran logs/estados.

6.7.5. Static routes — Rutas al destino de monitorización

QUÉ HACE La casilla “Do not add static routes for gateway monitor IP addresses” impide que pfSense añada automáticamente rutas específicas hacia las direcciones de monitorización de gateways.

VENTAJA Útil cuando la organización mantiene esas rutas de forma explícita y controlada.

PRECAUCIÓN Sin rutas adecuadas, el monitor puede medir por una WAN distinta y generar diagnósticos falsos o conmutaciones indebidas.

COMPROBACIÓN Revisar tabla de rutas y efectuar comprobaciones de alcance por la interfaz prevista antes y después del cambio.

POLÍTICA PROFESIONAL En Multi-WAN no hay una política universal: conservar estados minimiza cortes, y borrarlos acelera la creación de nuevas conexiones por el enlace operativo. Es una elección de continuidad, seguridad y comportamiento de aplicaciones.

6.8. PHP Settings — Memory Limit

6.8.1. Memory Limit

QUÉ HACE Establece el máximo de memoria que puede consumir un proceso PHP, utilizado por componentes de la interfaz y ciertas tareas del sistema. Si se deja vacío, rige el valor calculado por el equipo y la versión.

VENTAJA Puede resolver operaciones de administración muy voluminosas que superan el límite ordinario.

PRECAUCIÓN Aumentarlo sin diagnosticar errores puede empeorar presión de memoria o esconder una ejecución defectuosa. No equivale a ampliar toda la RAM del dispositivo.

COMPROBACIÓN Buscar el error concreto, medir memoria disponible y repetir la operación problemática después de un ajuste conservador.

6.9. RAM Disk Settings — Uso de memoria como disco

Las rutas /tmp y /var reciben datos transitorios o de escritura frecuente. Los RAM disks trasladan parte de ese trabajo desde el almacenamiento persistente a memoria. La ventaja es reducir escrituras, especialmente en medios flash limitados; el coste es consumir RAM y asumir pérdida de datos no guardados ante apagados inesperados.

6.9.1. Use RAM Disks

QUÉ HACE Habilita un sistema de archivos en memoria para /tmp y /var. El cambio obliga a reiniciar y afecta a los contenidos existentes de esos directorios.

VENTAJA Disminuye escrituras de la base del sistema sobre el almacenamiento persistente.

PRECAUCIÓN Riesgo de pérdida de información volátil, incompatibilidades con paquetes y falta de RAM. La configuración no debe activarse por costumbre en todos los equipos.

COMPROBACIÓN Antes de aplicar, revisar uso real de /tmp y /var, espacio de RAM y paquetes instalados; después del reinicio revisar servicios, logs y concesiones DHCP.

6.9.2. /tmp RAM Disk

QUÉ HACE Determina el espacio máximo disponible en memoria para archivos temporales en /tmp, expresado en MiB. La interfaz establece un mínimo técnico.

VENTAJA Evita que operaciones temporales tengan que escribir permanentemente al disco.

PRECAUCIÓN Un tamaño demasiado pequeño puede impedir instalaciones, descompresión o actualizaciones que usan /tmp.

COMPROBACIÓN Comparar tamaño asignado, ocupación normal y picos al instalar o actualizar paquetes.

6.9.3. /var RAM Disk

QUÉ HACE Establece el espacio reservado en memoria para /var, donde pueden residir registros, bases de datos transitorias y otros datos de servicios.

VENTAJA Reduce acceso a almacenamiento para archivos de actividad frecuente.

PRECAUCIÓN /var puede crecer mucho más de lo previsto según paquetes y registros; un agotamiento del espacio causa fallos de servicios.

COMPROBACIÓN Monitorizar ocupación en operación ordinaria y durante incidencias; verificar la retención de datos y los servicios tras reinicios.

6.9.4. Periodic RAM Disk Data Backups

Permite elegir cada cuántas horas se guardan en disco ciertas categorías de datos volátiles, para intentar recuperarlos después de un arranque. Menor intervalo significa menos exposición a pérdida de datos, pero mayor actividad de escritura.

Categoría	Qué conserva	Por qué importa
RRD Data	Series estadísticas utilizadas en gráficas históricas.	Mantener continuidad de tendencias después de reinicios.
DHCP Leases	Información de concesiones de direcciones de clientes.	Reducir inconsistencias tras reiniciar el servicio o el firewall.
Log Directory	Archivos de registro del sistema que se almacenan en el directorio correspondiente.	Preservar información de diagnóstico y auditoría.
Captive Portal Data	Datos utilizados por el portal cautivo.	Conservar información necesaria para el funcionamiento del portal.

ADVERTENCIA DE DATOS La copia periódica no garantiza conservar lo producido desde la última ejecución. Para entornos que necesitan trazabilidad, enviar logs a un servidor syslog remoto y comprobar que se reciben de forma continua.

6.10. Hardware Settings — Hard disk standby time

6.10.1. Hard disk standby time

QUÉ HACE Permite que un disco mecánico entre en reposo tras un periodo de inactividad. “Always on” mantiene la unidad activa; las opciones temporizadas representan minutos.

VENTAJA En discos magnéticos puede reducir consumo y ruido cuando existen períodos de inactividad.

PRECAUCIÓN No se recomienda aplicar la función a memorias CF, SSD o medios flash. En discos con escritura frecuente puede aumentar latencia y ciclos de arranque/parada.

COMPROBACIÓN Comprobar el tipo de almacenamiento y, si se habilita, revisar tiempo de respuesta y fiabilidad en acceso después del reposo.

6.11. Installation Feedback — Netgate Device ID

6.11.1. Do NOT send Netgate Device ID with user agent

QUÉ HACE Al marcarlo, se omite el identificador Netgate Device ID del encabezado User-Agent en las solicitudes a Netgate contempladas por esta funcionalidad.

VENTAJA Permite limitar la transmisión de ese identificador en las peticiones afectadas.

PRECAUCIÓN No elimina necesariamente todas las comunicaciones con Netgate ni equivale a anonimato completo; algunos servicios podrían necesitar identificación para soporte o licencias.

COMPROBACIÓN Examinar política de servicios y revisar el comportamiento de las funciones de actualización, soporte y comunicación aplicables.

6.12. Procedimientos prácticos

Caso A. Una aplicación pierde la sesión cuando hay balanceo

Confirmar que el sistema realmente utiliza un grupo de gateways con balanceo; no confundir balanceo con failover.

Revisar si la aplicación abre conexiones paralelas que deben salir por la misma WAN.

Verificar estados y el gateway empleado por cada conexión.

Valorar Use sticky connections y, si el problema persiste tras inactividad, Source tracking timeout.

Repetir la prueba y registrar impacto sobre el reparto de carga.

Caso B. La WAN principal vuelve y se interrumpe una llamada

Comprobar eventos de monitorización y momento exacto de recuperación del gateway.

Revisar la política de State Killing on Gateway Recovery y si existen reglas policy routing.

Diferenciar sesiones generadas por el firewall y por los clientes.

Seleccionar la política menos disruptiva compatible con los objetivos de retorno a WAN principal.

Reproducir con una llamada de prueba o sesión persistente, monitorizando los estados.

Caso C. Una regla de salida específica pasa por otra WAN

Identificar la regla que asigna el gateway y verificar que el destino de monitorización está disponible.

Comprobar si la regla se conserva sin gateway al marcarse éste como caído.

Si la política exige que nunca se use otro enlace, considerar Skip rules when gateway is down.

Añadir una regla posterior de bloqueo que impida coincidencias con reglas inferiores no deseadas.

Probar la indisponibilidad del gateway y comprobar la ruta efectiva mediante tráfico de ensayo.

Caso D. El firewall tiene errores tras activar discos RAM

Consultar ocupación de /tmp y /var y la RAM disponible.

Revisar registros de falta de espacio e identificar paquetes que escriben datos en esos directorios.

Evaluar ampliación responsable de tamaños o desactivación de RAM disks cuando corresponda.

Revisar intervalos de respaldos periódicos y recepción de syslog remoto.

Programar un reinicio controlado y comprobar que vuelven a funcionar servicios, DHCP y registros.

Caso E. Rendimiento de VPN inferior a lo esperado

Medir primero velocidad, CPU y latencia del túnel con una carga estable.

Confirmar algoritmos cifrados utilizados y disponibilidad de IPsec-MB o hardware criptográfico.

Cambiar exclusivamente la opción compatible y aplicar reinicio si se requiere.

Repetir medición en condiciones equivalentes.

Conservar únicamente las mejoras contrastadas y documentar la reversión.

6.13. Lista de comprobación antes de guardar

Comprobación	Motivo
¿Existe copia de seguridad de la configuración?	Permite recuperar opciones si el nuevo comportamiento no es aceptable.
¿Está identificado el propósito del cambio?	Evita activar opciones globales sin hipótesis técnica.
¿Se ha valorado el impacto en sesiones y gateways?	Previene interrupciones innecesarias en usuarios y VPN.

Comprobación	Motivo
¿Hay acceso administrativo alternativo?	Reduce el riesgo de quedar sin gestión durante un problema.
¿Se sabe si requiere reinicio?	Permite programar ventanas de mantenimiento.
¿Está definido cómo comprobar y revertir?	Facilita confirmar resultados sin improvisar.

6.14. Ideas esenciales

El proxy es para conexiones salientes del propio pfSense; no es un servidor proxy de LAN.

Sticky connections favorece estabilidad de sesiones, no aumenta por sí solo la capacidad de una conexión.

PowerD y aceleración criptográfica dependen del soporte real del hardware.

Borrar estados agiliza nuevas rutas, pero interrumpe comunicaciones establecidas.

Los RAM disks reducen escrituras y requieren dimensionamiento, respaldo y evaluación de pérdida de datos.

La privacidad de los identificadores de telemetría debe evaluarse por servicio, no como garantía absoluta.

Referencias técnicas

Netgate · Miscellaneous — https://docs.netgate.com/pfsense/en/latest/config/advanced-misc.html

Netgate · Gateway Settings — https://docs.netgate.com/pfsense/en/latest/routing/gateway-configure.html

Netgate · Cryptographic Accelerators — https://docs.netgate.com/pfsense/en/latest/hardware/cryptographic-accelerators.html

Netgate · Contact with Netgate Servers — https://docs.netgate.com/pfsense/en/latest/general/netgate-servers.html

Los rótulos se corresponden con las opciones presentes en la pantalla estudiada. La disponibilidad de funciones puede variar por versión y plataforma; la documentación oficial prevalece para confirmar compatibilidades.

07 System → Advanced → System Tunables

Parámetros internos de FreeBSD, procesamiento de red, seguridad, protocolos, puentes, VPN y alta disponibilidad.

Esta sección permite consultar y mantener parámetros del sistema mediante identificadores sysctl (OID). Su utilidad no radica en aumentar indiscriminadamente el rendimiento, sino en resolver necesidades concretas sin comprometer la estabilidad del firewall.



Figura 7.1. Relación entre interfaz de administración, parámetros del núcleo, posibles efectos y proceso de validación.

Qué aprenderá el lector

Interpretar las columnas de System Tunables y distinguir parámetros en ejecución de parámetros de arranque.

Conocer la finalidad y el riesgo de cada uno de los identificadores de la pantalla.

Relacionar OID concretos con conectividad, criptografía, TCP/IP, IPv6, bridges y alta disponibilidad.

Consultar valores y descripciones desde la consola sin modificar la configuración.

Aplicar un procedimiento de cambio reversible y documentado.

REGLA GENERAL: No existe un conjunto universal de valores «mejores». Los valores adecuados dependen de la versión, del hardware, de los controladores y del tráfico. En la mayoría de los casos se deben conservar los ajustes proporcionados por pfSense Plus.

7.1. Dónde está y qué muestra

Ruta: System → Advanced → System Tunables. La vista contiene una tabla de parámetros del sistema. Habitualmente cada fila identifica un OID, una descripción, su valor vigente o configurado y acciones de edición. Las opciones visibles pueden variar entre versiones y plataformas.

Elemento	Qué representa	Uso en la práctica
Tunable / OID	Identificador jerárquico del subsistema FreeBSD.	Determina exactamente qué propiedad se consulta o configura.
Description	Breve descripción informativa del parámetro.	Aporta contexto, pero puede ser insuficiente para elegir un cambio seguro.
Value	Valor asociado a ese OID en la configuración o en el sistema.	Su significado y rango dependen del parámetro; no existe una unidad común.
Edit / Add	Control para editar una fila existente o crear un OID.	Debe utilizarse sólo tras verificar disponibilidad, sintaxis y efecto.
Save	Guarda la definición configurada en la interfaz.	No implica que todos los cambios se apliquen instantáneamente.

Tres familias que conviene diferenciar

Familia	Comportamiento	Dónde se gestiona
Runtime tunable	Permite cambios con el sistema arrancado, si el OID es modificable.	System Tunables, cuando pfSense admite su gestión.
Loader tunable	Se establece antes de arrancar el núcleo; puede quedar sólo de lectura después.	Archivo loader.conf.local y reinicio; no es el mecanismo de la tabla.
Read-only	Expone información o estadísticas; no acepta modificación directa.	Consulta mediante sysctl, sin alterar valor.

Guardar una fila no garantiza que el núcleo acepte cualquier valor: la interfaz no puede validar las particularidades de todos los OID. Si el cambio requiere reinicio, debe identificarse antes de programar la intervención.

7.2. Cómo se administran los parámetros

7.2.1. Consultar sin modificar

Desde Diagnostics → Command Prompt o una consola autorizada se pueden obtener las propiedades disponibles. Los comandos siguientes realizan consultas, no cambios:

```
sysctl -a   — muestra los OID visibles y sus valores.
sysctl -d kern.ipc.maxsockbuf   — solicita la descripción de ese OID, si está disponible.
sysctl kern.ipc.maxsockbuf   — consulta el valor actual de ese parámetro.
sysctl net.inet.ip.intr_queue_drops   — consulta un contador útil durante el diagnóstico de colas IP, si existe.
```

7.2.2. Editar un parámetro persistente

Comprobar la documentación correspondiente a la misma versión de pfSense Plus y FreeBSD.

Guardar una copia reciente de la configuración en Diagnostics → Backup & Restore.

Registrar el OID, su descripción y el valor anterior en un registro de cambios.

Abrir la fila con Edit y modificar únicamente el campo necesario.

Guardar, comprobar si el cambio se aplicó y determinar si requiere reinicio.

Verificar conectividad, recursos, registros y comportamiento del servicio afectado.

Revertir el cambio si aparecen resultados no previstos.

PRECAUCIÓN DE ACCESO: Si un OID afecta al filtrado, bridging, TCP/IP o alta disponibilidad, es recomendable disponer de acceso de consola alternativo y una ventana de mantenimiento. No intervenir en sistemas críticos únicamente desde una sesión remota susceptible de perderse.

7.3. Consola, núcleo y aceleración criptográfica

Los siguientes OID se relacionan con la consola, el núcleo de FreeBSD y la aceleración criptográfica. Los identificadores IPsec-MB sólo tienen efecto si el módulo y la plataforma los admiten. [2]

hw.syscons.kbd_reboot

QUÉ HACE Control heredado relacionado con el reinicio mediante teclado en la consola syscons.

CUÁNDO INTERESA Sólo tiene interés en consolas compatibles y cuando existe una política sobre acciones locales.

PRECAUCIÓN Baja · Dependiente de plataforma; no asumir que actúa sobre todas las consolas.

kern.corefile

QUÉ HACE Define el patrón de nombre y ubicación de archivos core generados tras fallos de procesos.

CUÁNDO INTERESA Es útil para diagnósticos avanzados bajo indicación de soporte.

PRECAUCIÓN Alta · Los core pueden contener datos sensibles y ocupar disco.

kern.crypto.iimb.arch

QUÉ HACE Selecciona la arquitectura SIMD que utiliza IPsec-MB; en automático prioriza la compatible con la CPU.

CUÁNDO INTERESA Comparar comportamiento criptográfico en diagnóstico o desarrollo.

PRECAUCIÓN Alta · Compatibilidad ligada a arquitectura; no forzar instrucciones inexistentes.

kern.crypto.iimb.enable_aescbc

QUÉ HACE Habilita que IPsec-MB atienda operaciones AES-CBC en plataformas compatibles.

CUÁNDO INTERESA Ajustar coexistencia con otros aceleradores cuando corresponda.

PRECAUCIÓN Alta · Puede cambiar el rendimiento de algoritmos VPN.

kern.crypto.iimb.enable_multiq

QUÉ HACE Distribuye trabajos criptográficos de IPsec-MB por varias colas.

CUÁNDO INTERESA Optimizar paralelismo en cargas compatibles.

PRECAUCIÓN Alta · Efecto dependiente de núcleos, tráfico y versión.

kern.crypto.iimb.max_jobs

QUÉ HACE Limita el tamaño de los lotes de trabajos procesados por IPsec-MB.

CUÁNDO INTERESA Equilibrar procesamiento por lotes y latencia.

PRECAUCIÓN Alta · Un lote mayor no implica necesariamente más rendimiento.

kern.crypto.iimb.prefetch

QUÉ HACE Gestiona la precarga de claves para trabajos de IPsec-MB.

CUÁNDO INTERESA Ajuste de microoptimización o pruebas de rendimiento.

PRECAUCIÓN Alta · No modificar sin mediciones específicas.

kern.crypto.iimb.use_task

QUÉ HACE Controla si se usa una cola de tareas separada para callbacks de trabajos criptográficos.

CUÁNDO INTERESA Puede ser relevante en equipos de alto rendimiento.

PRECAUCIÓN Alta · Verificar estabilidad, latencia y rendimiento VPN.

kern.ipc.maxsockbuf

QUÉ HACE Establece el límite de memoria reservable en búferes de sockets.

CUÁNDO INTERESA Investigar aplicaciones limitadas por tamaño de búfer, con evidencia.

PRECAUCIÓN Alta · Una reserva excesiva puede aumentar la presión de memoria.

kern.random.harvest.mask

QUÉ HACE Máscara de fuentes empleadas para reunir entropía del sistema.

CUÁNDO INTERESA Sólo depuración especializada del subsistema aleatorio.

PRECAUCIÓN Crítica · Modificar la recolección de entropía sin justificación puede ser inseguro.

kern.randompid

QUÉ HACE Modifica la aleatorización de los identificadores de procesos (PID).

CUÁNDO INTERESA Ajuste interno de endurecimiento o compatibilidad.

PRECAUCIÓN Alta · No confundir con control de permisos ni seguridad completa.

kern.shutdown.secure_halt

QUÉ HACE Controla el comportamiento de apagado seguro del sistema, según implementación.

CUÁNDO INTERESA Tratamiento de parada ordenada de la plataforma.

PRECAUCIÓN Alta · No equivale a borrado seguro de datos.

7.4. Alta disponibilidad, ICMP y procesamiento IPv4

Estas opciones afectan a mensajes de control de red, manejo de paquetes IPv4 y, en algunos casos, a conmutaciones CARP. Deben evaluarse mediante métricas antes de intervenir.

net.inet.carp.senderr_demotion_factor

QUÉ HACE Regula cómo influyen los errores de envío sobre la degradación de prioridad CARP.

CUÁNDO INTERESA Diagnosticar conmutaciones inesperadas en alta disponibilidad.

PRECAUCIÓN Crítica · Puede afectar a cuál nodo asume el servicio.

net.inet.icmp.icmplim

QUÉ HACE Limita la emisión de determinados mensajes ICMP por segundo.

CUÁNDO INTERESA Controlar respuestas y rate limiting ante tráfico intenso.

PRECAUCIÓN Alta · Un límite inadecuado altera trazas y diagnóstico.

net.inet.icmp.reply_from_interface

QUÉ HACE Determina la selección de interfaz de origen para ciertas respuestas ICMP sobre tráfico no local.

CUÁNDO INTERESA Analizar ICMP en equipos con varias interfaces.

PRECAUCIÓN Alta · Puede cambiar la dirección origen vista por otros sistemas.

net.inet.ip.intr_queue_maxlen

QUÉ HACE Define el tamaño máximo de la cola de entrada de procesamiento IP.

CUÁNDO INTERESA Investigar descartes de cola bajo cargas elevadas.

PRECAUCIÓN Alta · Aumentar el tamaño consume recursos y no elimina todas las causas de pérdida.

net.inet.ip.portrange.first

QUÉ HACE Define el inicio de un rango de puertos de origen gestionado por la pila IPv4.

CUÁNDO INTERESA Compatibilidad con aplicaciones especiales que usan puertos locales.

PRECAUCIÓN Alta · Modificar la asignación de puertos puede generar conflictos.

net.inet.ip.process_options

QUÉ HACE Controla el procesamiento de opciones del encabezado IPv4, como rutas fuente o marcas de tiempo.

CUÁNDO INTERESA Pruebas de compatibilidad con tráfico IPv4 poco habitual.

PRECAUCIÓN Alta · Las opciones IP pueden introducir implicaciones de seguridad.

net.inet.ip.random_id

QUÉ HACE Controla la aleatorización del campo de identificación IPv4 en los paquetes que corresponda.

CUÁNDO INTERESA Mitigar predictibilidad del identificador en determinados flujos.

PRECAUCIÓN Alta · Puede interactuar con fragmentación y otros mecanismos de red.

net.inet.ip.redirect

QUÉ HACE Controla el envío de mensajes ICMP Redirect IPv4.

CUÁNDO INTERESA Revisar recomendaciones de rutas desde el propio firewall a otros equipos.

PRECAUCIÓN Alta · El envío de redirects puede inducir cambios de ruta no deseados.

net.inet.raw.maxdgram

QUÉ HACE Fija el tamaño máximo de datagramas enviados desde sockets IP raw.

CUÁNDO INTERESA Compatibilidad con programas especializados de red.

PRECAUCIÓN Alta · Afecta a herramientas que emplean sockets raw.

net.inet.raw.recvspace

QUÉ HACE Establece el espacio de recepción para sockets raw IPv4.

CUÁNDO INTERESA Diagnóstico de pérdidas en herramientas específicas.

PRECAUCIÓN Alta · Requiere medir memoria y tráfico.

7.5. Comportamiento TCP y UDP

Los parámetros de TCP y UDP influyen en el comportamiento de la pila del propio sistema. No sustituyen las reglas de firewall ni garantizan mejoras universales.

net.inet.tcp.blackhole

QUÉ HACE Regula la respuesta TCP ante paquetes hacia puertos sin servicio, incluida la omisión de RST en ciertos modos.

CUÁNDO INTERESA Reducir respuestas indeseadas en determinadas políticas de seguridad.

PRECAUCIÓN Alta · Puede dificultar diagnóstico de puertos y aplicaciones.

net.inet.tcp.delayed_ack

QUÉ HACE Controla el retraso de ACK para intentar combinarlos con el envío de datos.

CUÁNDO INTERESA Analizar compatibilidad, eficiencia y latencia de sesiones TCP.

PRECAUCIÓN Alta · No existe un valor óptimo universal.

net.inet.tcp.drop_synfin

QUÉ HACE Controla si se descartan segmentos TCP con SYN y FIN simultáneos.

CUÁNDO INTERESA Endurecimiento frente a combinaciones TCP inusuales.

PRECAUCIÓN Alta · Puede afectar a pruebas especializadas o tráfico atípico.

net.inet.tcp.log_debug

QUÉ HACE Habilita información de depuración de errores por segmentos TCP entrantes.

CUÁNDO INTERESA Recoger más evidencia durante una incidencia acotada.

PRECAUCIÓN Media · Más registros pueden elevar ruido y consumo de almacenamiento.

net.inet.tcp.recvspace

QUÉ HACE Define el tamaño inicial del búfer de recepción de TCP.

CUÁNDO INTERESA Analizar rendimiento de conexiones TCP en escenarios medidos.

PRECAUCIÓN Alta · Modificaciones genéricas pueden empeorar las cargas.

net.inet.tcp.sendspace

QUÉ HACE Define el tamaño inicial del búfer de envío de TCP.

CUÁNDO INTERESA Tareas muy concretas de ajuste de la pila TCP.

PRECAUCIÓN Alta · Combinar con medición de latencia y memoria.

net.inet.tcp.syncookies

QUÉ HACE Controla el uso de SYN cookies para sobrecarga de la caché de conexiones entrantes.

CUÁNDO INTERESA Resiliencia ante acumulación de intentos de conexión TCP.

PRECAUCIÓN Alta · Debe evaluarse con la configuración y versión del kernel.

net.inet.tcp.tso

QUÉ HACE Controla el mecanismo TCP Segmentation Offload en la pila.

CUÁNDO INTERESA Resolver problemas vinculados con TSO y ciertos drivers.

PRECAUCIÓN Alta · Su efecto puede coexistir con ajustes de Networking y de arranque.

net.inet.udp.blackhole

QUÉ HACE Modifica el envío de avisos ICMP Port Unreachable ante UDP no atendido.

CUÁNDO INTERESA Adaptar respuesta del sistema ante datagramas no solicitados.

PRECAUCIÓN Alta · Puede complicar pruebas de conectividad UDP.

net.inet.udp.checksum

QUÉ HACE Controla el cálculo de comprobaciones de integridad UDP en el contexto del kernel.

CUÁNDO INTERESA Sólo ajustes extraordinarios de compatibilidad o depuración.

PRECAUCIÓN Crítica · Desactivar verificaciones de integridad es potencialmente peligroso.

net.inet.udp.maxdgram

QUÉ HACE Define el tamaño máximo de datagrama UDP de salida permitido en el subsistema correspondiente.

CUÁNDO INTERESA Compatibilidad con aplicaciones que generan datagramas grandes.

PRECAUCIÓN Alta · No elimina por sí solo límites de MTU ni problemas de fragmentación.

MATIZ TÉCNICO: El valor de un parámetro TCP/UDP del núcleo no debe confundirse con el comportamiento de reglas stateful de pf, NAT o el tráfico que atraviesa el firewall. Confirmar primero si el OID afecta al tráfico reenviado, al propio firewall o a ambos.

7.6. IPv6 e IPsec

Los cambios en selección de direcciones, router advertisements y asociaciones de seguridad pueden repercutir en conectividad IPv6 e IPsec.

net.inet6.ip6.prefer_tempaddr

QUÉ HACE Decide la preferencia de direcciones IPv6 temporales como origen, cuando existen.

CUÁNDO INTERESA Evaluar privacidad y selección de origen IPv6.

PRECAUCIÓN Media · Puede alterar flujos salientes y diagnósticos basados en origen.

net.inet6.ip6.redirect

QUÉ HACE Controla el envío de mensajes de redirección ICMPv6 en los supuestos pertinentes.

CUÁNDO INTERESA Analizar comportamientos de enrutamiento IPv6.

PRECAUCIÓN Alta · Puede influir en rutas percibidas por los clientes.

net.inet6.ip6.rfc6204w3

QUÉ HACE Afecta a aceptar anuncios RA de routers IPv6 cuando el equipo también reenvía paquetes.

CUÁNDO INTERESA Compatibilidad con entornos IPv6 de proveedor y delegación.

PRECAUCIÓN Alta · Puede modificar el aprendizaje de ruta predeterminada.

net.inet6.ip6.use_tempaddr

QUÉ HACE Controla la creación de direcciones IPv6 temporales cuando la autoconfiguración lo permite.

CUÁNDO INTERESA Política de privacidad y comportamiento de direcciones locales.

PRECAUCIÓN Media · No confundir crear direcciones con priorizarlas.

net.key.preferred_oldsa

QUÉ HACE Parámetro interno de política de asociaciones de seguridad (SA) en la pila IPsec.

CUÁNDO INTERESA Sólo soporte especializado ante problemas de selección de SA.

PRECAUCIÓN Crítica · Verificar semántica exacta en kernel y versión concretos.

7.7. Bridges, interfaces y sincronización de estados

En entornos bridge y HA, la coherencia entre filtrado, interfaces y sincronización de estados tiene prioridad sobre cualquier ajuste de rendimiento. [3][4]

net.link.bridge.member_ifaddrs

QUÉ HACE Control heredado relacionado con direcciones de capa 3 en interfaces miembros de bridge.

CUÁNDO INTERESA Compatibilidad histórica con diseños de puentes.

PRECAUCIÓN Alta · Está marcado como obsoleto; evitar diseñar soluciones nuevas sobre él.

net.link.bridge.pfil_bridge

QUÉ HACE Define si las reglas del firewall se aplican sobre la interfaz bridge.

CUÁNDO INTERESA Elegir un único punto de filtrado al administrar puentes.

PRECAUCIÓN Crítica · Dejar las rutas de filtrado incoherentes puede pasar o bloquear tráfico inesperado.

net.link.bridge.pfil_member

QUÉ HACE Define si el filtrado se aplica sobre las interfaces miembro de un bridge.

CUÁNDO INTERESA Controlar el tráfico por puerto físico/miembro.

PRECAUCIÓN Crítica · Cambiarlo exige revisar reglas de todos los miembros.

net.link.bridge.pfil_onlyip

QUÉ HACE Controla el tratamiento de tramas no IP al utilizar filtros en puentes.

CUÁNDO INTERESA Compatibilidad con protocolos Ethernet distintos de IPv4/IPv6.

PRECAUCIÓN Alta · Puede alterar el paso de tramas imprescindibles para otros equipos.

net.link.tap.user_open

QUÉ HACE Comportamiento heredado de creación de dispositivos TAP por usuarios.

CUÁNDO INTERESA Compatibilidad de aplicaciones que solicitan interfaces virtuales.

PRECAUCIÓN Alta · Depende de permisos del dispositivo y del sistema FreeBSD.

net.link.vlan.mtag_pcp

QUÉ HACE Conserva información de prioridad PCP de VLAN al transportar paquetes por la pila de red.

CUÁNDO INTERESA Análisis de prioridad 802.1Q y tratamiento de tráfico etiquetado.

PRECAUCIÓN Alta · No equivale por sí mismo a configurar una política completa de QoS.

net.pfsync.carp_demotion_factor

QUÉ HACE Factor que relaciona incidencias de pfsync con la degradación CARP.

CUÁNDO INTERESA Investigar estado HA, sincronización de sesiones y conmutaciones.

PRECAUCIÓN Crítica · Cambios pueden modificar la elección del nodo principal.

PUNTO CRÍTICO EN BRIDGES: Según Netgate, al menos uno de los mecanismos de filtrado en miembros o en la interfaz bridge debe permanecer habilitado cuando se espera aplicar reglas de firewall sobre el puente. Un cambio simultáneo puede provocar un resultado inseguro o pérdida de acceso. [3]

7.8. Sockets raw, colas de enrutamiento y disco

La mayoría de estos ajustes se reservan para diagnóstico medido de aplicaciones especializadas o de E/S.

net.raw.recvspace

QUÉ HACE Espacio de recepción en sockets raw del subsistema correspondiente.

CUÁNDO INTERESA Ajustes puntuales para procesos con sockets especializados.

PRECAUCIÓN Alta · Medir uso de memoria y comportamiento de las aplicaciones.

net.raw.sendspace

QUÉ HACE Espacio de envío en sockets raw del subsistema correspondiente.

CUÁNDO INTERESA Pruebas de rendimiento o compatibilidad muy concretas.

PRECAUCIÓN Alta · No mejora automáticamente el rendimiento general.

net.route.netisr_maxqlen

QUÉ HACE Límite de cola de despacho de eventos o mensajes de enrutamiento.

CUÁNDO INTERESA Analizar presión en colas del subsistema de rutas.

PRECAUCIÓN Alta · Requiere contadores y evidencia de saturación.

vfs.read_max

QUÉ HACE Controla la lectura anticipada máxima en agrupaciones de bloques del sistema de archivos.

CUÁNDO INTERESA Investigar patrones de E/S secuencial, cuando proceda.

PRECAUCIÓN Alta · Puede incrementar memoria/E/S sin beneficio bajo otras cargas.

7.9. Procedimientos de diagnóstico guiado

Caso A. Una interfaz bridge pasa tráfico sin coincidir con las reglas esperadas

Documentar qué interfaces forman el bridge y dónde están aplicadas las reglas.

Leer net.link.bridge.pfil_member y net.link.bridge.pfil_bridge mediante sysctl, sin alterar sus valores.

Confirmar si el filtrado se espera en miembros o en la interfaz lógica; verificar que al menos uno participa.

Revisar reglas de Firewall → Rules, registros y pruebas de tráfico en ambos sentidos.

Si se requiere un cambio, hacerlo en ventana controlada y verificar acceso administrativo de inmediato.

Caso B. Descenso de rendimiento con tráfico IP intenso

Registrar los síntomas: pérdida, latencia, uso de CPU, buffers y throughput.

Consultar el contador de descartes de cola IP y el tamaño máximo configurado.

Contrastar si las pérdidas corresponden a cola IP, NIC, ancho de banda o estados del firewall.

Ajustar únicamente si existe evidencia; después medir otra vez y comparar contra el escenario inicial.

Caso C. VPN con rendimiento criptográfico inferior al esperado

Comprobar el algoritmo utilizado, el modo VPN, el soporte de CPU y la carga de la máquina.

Verificar si IPsec-MB está habilitado y si el conjunto de OID kern.crypto.iimb.* está presente.

No forzar arquitecturas SIMD ni lotes de trabajo sin una prueba comparativa reproducible.

Registrar throughput, latencia, CPU y errores antes y después de cualquier variación.

Caso D. HA con cambios inesperados entre nodo primario y secundario

Comprobar Status → CARP y los registros de pfsync, interfaces y conectividad de sincronización.

Consultar el estado de degradación CARP y sus factores relacionados.

Resolver primero pérdidas de enlace, problemas de sincronización o bucles de capa 2.

Modificar factores de democión sólo con justificación contrastada; no usarlos para ocultar averías.

7.10. Política de cambios y reversión

Situación	Acción correcta	Evitar
Cambio de rendimiento	Medir antes y después, sobre un síntoma reproducible.	Alterar varios OID al mismo tiempo.
Núcleo / criptografía	Confirmar soporte exacto de versión, CPU y módulo.	Copiar valores de otra plataforma.
Filtrado de bridges	Verificar punto de filtrado y acceso de consola.	Deshabilitar a ciegas filtrado en todas las interfaces.
Alta disponibilidad	Validar CARP, pfsync y ambas unidades.	Desactivar protecciones que alertan de fallos reales.
Valores de arranque	Distinguir sysctl runtime de loader.conf.local.	Introducir valores de arranque en la pestaña equivocada.
Error tras aplicar	Restaurar el OID anterior, reiniciar si procede y comprobar.	Continuar con cambios sin aislar la causa.

Lista de comprobación

¿Se ha identificado el motivo concreto para cambiar el OID?

¿Está verificada su existencia y su documentación en esta versión?

¿Se dispone de copia de configuración y acceso alternativo?

¿Se ha registrado el valor previo fuera de este libro?

¿Está claro si el ajuste es inmediato, al reinicio o de sólo lectura?

¿Se han definido indicadores medibles de éxito o reversión?

¿Han pasado las pruebas de seguridad, conectividad y recuperación?

7.11. Glosario esencial

Término	Definición	Por qué importa
OID	Identificador de objeto del árbol de configuración del kernel.	Evita confundir nombres similares de subsistemas.
sysctl	Mecanismo FreeBSD para consultar o configurar parámetros del núcleo.	Permite observar el estado real del sistema.
Runtime	Parámetro cambiable durante la ejecución, cuando está permitido.	No todos necesitan reinicio.
Loader	Parámetro que se define antes del arranque del kernel.	No se gestiona como sysctl ordinario en esta pestaña.
CARP / pfsync	Conmutación de direcciones virtuales y sincronización de estados, respectivamente.	Esencial para continuidad en clusters.
Bridge / pfil	Conmutación de capa 2 y puntos de enganche del filtrado.	Determina dónde se evalúan reglas.
IPsec-MB	Mecanismo de aceleración criptográfica en plataformas compatibles.	Influye en determinados algoritmos VPN.
TSO	Delegación de segmentación TCP en el hardware o pila de red.	Puede influir en rendimiento y compatibilidad.

7.12. Ideas clave

System Tunables no es una pantalla de optimización automática: permite intervenir en mecanismos de bajo nivel.

Los nombres de OID se mantienen estables dentro del contexto descrito, pero los valores y el soporte pueden cambiar entre versiones.

Los ajustes de puentes, IPsec, criptografía y alta disponibilidad exigen medidas de seguridad y verificación adicionales.

La mejor práctica habitual consiste en conservar los valores suministrados por pfSense Plus salvo que exista una causa técnica verificable.

Referencias técnicas

[1] Netgate — System Tunables

[2] Netgate — Cryptographic Accelerators: IPsec-MB

[3] Netgate — Bridging and Firewall Rules

[4] Netgate — Troubleshooting High Availability

[5] Netgate — Hardware Tuning and Troubleshooting

[6] FreeBSD — Boot Process / sysctl

08 System → Advanced → Notifications

Alertas del sistema, avisos sobre certificados y notificaciones remotas mediante correo, Telegram, Pushover y Slack.

Las notificaciones facilitan que un administrador conozca determinadas situaciones relevantes sin depender exclusivamente de revisar el panel de control. Esta pantalla permite elegir canales de entrega y afinar cuándo se emiten algunos avisos. Su valor está en combinar configuración, verificación y una gestión responsable de los destinatarios.



Figura 8.1. Relación entre los eventos detectados por pfSense Plus y los canales de notificación configurados.

Qué aprenderá el lector

Localizar las opciones de notificación de pfSense Plus e identificar su ámbito de actuación.

Comprender cada parámetro de caducidad de certificados y su política de avisos.

Configurar el envío por SMTP diferenciando TLS implícito y STARTTLS.

Conocer las credenciales y destinos necesarios para Telegram, Pushover y Slack.

Entender las prioridades de Pushover, incluidos avisos persistentes de emergencia.

Comprobar que los cambios guardados y los mensajes de prueba funcionan de extremo a extremo.

Diagnosticar fallos frecuentes sin exponer contraseñas, tokens o datos de una instalación.

PRINCIPIO DE FUNCIONAMIENTO Que un canal esté configurado no significa que exista garantía de recepción: influyen DNS, conectividad, certificados TLS, permisos de las API, políticas del proveedor y configuración del destinatario. Las notificaciones complementan, no sustituyen, una monitorización integral.

8.1. Acceso a la pantalla y alcance

Ruta de administración: System → Advanced → Notifications. Esta pestaña se encuentra dentro de Advanced y agrupa las secciones General Settings, E-Mail, Sounds, Telegram, Pushover y Slack.

Además de los avisos en la interfaz gráfica (icono de notificaciones en la barra superior), el sistema puede emitir señales locales por hardware compatible y mensajes remotos mediante servicios configurados. La presencia de un método no implica que todo tipo de evento se envíe por él: depende de si el sistema o el paquete genera una notificación y de su configuración.

Método	Dónde se consulta	Qué aporta
Avisos de GUI	Interfaz de pfSense Plus	Consulta local de eventos y errores
Sonidos	Consola física o serial compatible	Señales locales de ciertos eventos
SMTP	Bandeja de correo designada	Mensajes archivables y distribuidos a varios responsables
Telegram	Chat o canal autorizado	Notificación rápida en aplicaciones cliente
Pushover	Dispositivos de usuarios autorizados	Prioridad, sonido y reintentos de emergencia

Método	Dónde se consulta	Qué aporta
Slack	Canal de un espacio de trabajo	Colaboración y visibilidad de avisos

8.2. General Settings: caducidad de certificados

Los certificados digitales permiten identificar servicios y establecer conexiones seguras. Si una autoridad de certificación o un certificado vence, puede provocar errores de confianza, imposibilidad de conexión o interrupciones de servicios. Por eso es útil avisar con antelación.

Certificate Expiration

QUÉ HACE Activa una comprobación diaria de las fechas de caducidad de las autoridades de certificación y certificados almacenados; genera avisos de los vencidos o próximos al vencimiento.

UTILIDAD Permite programar renovaciones o sustituciones antes de que afecten a usuarios y VPN.

PRECAUCIÓN La alerta no renueva el certificado por sí sola. Debe existir un proceso de renovación y comprobación posterior.

Ignore Revoked

QUÉ HACE Impide avisos de caducidad para certificados que constan como revocados al menos una vez en una lista de revocación (CRL).

UTILIDAD Evita notificaciones poco útiles de certificados que ya no deberían emplearse.

PRECAUCIÓN No significa que deba ignorarse la seguridad de la revocación: sólo modifica determinados avisos de vencimiento.

Certificate Expiration Threshold

QUÉ HACE Establece el límite máximo, en días, para considerar que un certificado se acerca a su vencimiento. El valor predeterminado documentado es 27 días. El sistema utiliza el menor entre dicho límite y un tercio del período de vida del certificado menos un día.

UTILIDAD Ajusta la antelación máxima, evitando generar avisos demasiado pronto para certificados de vida corta.

PRECAUCIÓN Si la renovación depende de terceros o de procedimientos lentos, verificar si el margen efectivo permite completar el cambio.

PUNTO TÉCNICO Certificate Expiration Threshold no es un número fijo de días garantizados para todos los certificados. El aviso puede activarse con menos antelación debido a la fórmula que limita su aplicación.

8.3. E-Mail: notificaciones por SMTP

El correo es un canal habitual para centralizar incidencias y disponer de una trazabilidad accesible. pfSense Plus establece una conexión SMTP hacia un servidor capaz de aceptar el envío, ya sea mediante autenticación o mediante permisos de retransmisión explícitos.

Disable SMTP

QUÉ HACE Al marcarla, deshabilita las notificaciones SMTP ordinarias, conservando los campos de configuración.

UTILIDAD Permite silenciar el canal sin eliminar los datos necesarios para algunos paquetes que puedan utilizar la configuración de correo.

PRECAUCIÓN Deshabilitar el envío en pfSense no equivale a retirar credenciales almacenadas; revisar su ciclo de vida.

E-Mail server

QUÉ HACE Indica el nombre DNS completo o la dirección del servidor SMTP utilizado para el envío.

UTILIDAD Define el servidor de salida empleado por las notificaciones.

PRECAUCIÓN Debe resolver y ser alcanzable desde el propio firewall. Utilizar el nombre que corresponda al certificado TLS cuando se valide.

SMTP Port of E-Mail server

QUÉ HACE Define el puerto TCP del servicio SMTP. Los puertos habituales son 25, 587 y 465; cada servicio puede exigir un modo de conexión distinto.

UTILIDAD Permite adaptar el cliente al servidor o al proveedor utilizado.

PRECAUCIÓN El puerto 587 suele emplearse para Submission con STARTTLS; el 465, para TLS implícito; el 25 a menudo se reserva para relé o transporte y puede estar bloqueado por el proveedor de acceso.

Connection timeout to E-Mail server

QUÉ HACE Determina los segundos máximos de espera para establecer conexión con el servidor. El valor predeterminado documentado es 20 segundos.

UTILIDAD Evita que el intento quede pendiente indefinidamente si el servidor no responde.

PRECAUCIÓN Aumentar la espera puede ayudar en enlaces lentos, pero no soluciona un servidor inaccesible ni errores de TLS.

Secure SMTP Connection

QUÉ HACE Si se marca, el cliente intenta establecer TLS directamente desde el comienzo de la conexión (SSL/TLS implícito).

UTILIDAD Protege las comunicaciones cuando el servidor utiliza este modo.

PRECAUCIÓN No se debe marcar para un servicio que exige primero SMTP en texto claro y luego STARTTLS, como ocurre normalmente en el puerto 587. Cuando no se marca, pfSense puede negociar STARTTLS automáticamente en 25/587 si hay autenticación.

Validate SSL/TLS

QUÉ HACE Valida el certificado del servidor SMTP frente a las autoridades de confianza conocidas por el firewall.

UTILIDAD Confirma la identidad del servidor remoto y ayuda a prevenir conexiones con destinos suplantados.

PRECAUCIÓN Desactivar la validación puede mantener el cifrado, pero impide verificar de forma fiable el servidor. Corregir certificados o confianza es preferible a deshabilitarla.

From e-mail address

QUÉ HACE Dirección declarada como remitente (cabecera From) de los mensajes de notificación.

UTILIDAD Facilita identificar el origen y cumplir políticas del servidor de correo.

PRECAUCIÓN El proveedor puede exigir que el remitente exista o coincida con la identidad autenticada.

Notification E-Mail address

QUÉ HACE Dirección o direcciones destinatarias a las que pfSense enviará los avisos; admite varias separadas por comas.

UTILIDAD Permite distribuir notificaciones entre responsables o buzones de operaciones.

PRECAUCIÓN Limitar la lista a destinatarios autorizados y evitar difundir datos de infraestructura innecesariamente.

Notification E-Mail auth username (optional)

QUÉ HACE Nombre de usuario usado para autenticarse en SMTP cuando el servidor la requiere.

UTILIDAD Identifica la cuenta remitente ante el servidor.

PRECAUCIÓN No todos los proveedores utilizan el mismo formato de usuario; seguir su política de autenticación.

Notification E-Mail auth password / Confirm

QUÉ HACE Contraseña o credencial de aplicación utilizada para autenticarse; el campo Confirm comprueba que ambas entradas coincidan.

UTILIDAD Permite enviar mediante servidores que exigen autenticación.

PRECAUCIÓN Preferir credenciales específicas de servicio y no reutilizar contraseñas administrativas; no incluirlas en capturas o documentos.

Notification E-Mail auth mechanism

QUÉ HACE Selecciona el mecanismo de autenticación ofrecido por la pantalla: PLAIN o LOGIN.

UTILIDAD Permite adaptarse a las capacidades del servidor SMTP.

PRECAUCIÓN PLAIN y LOGIN no son mecanismos de cifrado: emplear un canal TLS adecuado. Si el proveedor requiere OAuth, esta pantalla puede no satisfacer ese requisito por sí sola.

Test SMTP Settings

QUÉ HACE Ordena enviar una notificación de prueba utilizando los últimos ajustes guardados.

UTILIDAD Verifica conectividad, autenticación, negociación TLS y entrega inicial del correo.

PRECAUCIÓN Puede realizar la prueba aunque Disable SMTP esté marcado. Guardar primero: los valores sin guardar no serán los empleados en la prueba.

8.3.1. Cómo elegir el modo de seguridad SMTP

Situación del servidor	Ajuste relevante	Comprobación
TLS implícito, normalmente puerto 465	Secure SMTP Connection: activado	El servidor acepta TLS desde el inicio y su certificado valida
Submission con STARTTLS, normalmente puerto 587	Secure SMTP Connection: desactivado	El servidor permite STARTTLS y la autenticación configurada
Relé interno de correo, normalmente puerto 25	Depende de las políticas del relé	Verificar acceso, requisitos TLS y permisos de retransmisión

SEGURIDAD No debe confundirse «sin marcar Secure SMTP Connection» con «correo siempre sin cifrar». En los puertos con negociación STARTTLS, el cliente puede establecer TLS después del saludo inicial, de acuerdo con el mecanismo y la configuración documentados por Netgate.

8.4. Sounds: señales locales

Console Bell

QUÉ HACE Activa una señal de campana en consolas conectadas, incluidas terminales seriales, para determinados mensajes de emergencia como ciertos registros de acceso a la GUI.

UTILIDAD Ofrece un aviso adicional en equipos o terminales atendidos localmente.

PRECAUCIÓN El sonido depende de que el hardware y la consola lo soporten; no equivale a una alerta remota.

Startup/Shutdown Sound

QUÉ HACE La casilla «Disable the startup/shutdown beep» evita los pitidos que el firewall puede emitir al terminar el arranque o comenzar el apagado.

UTILIDAD Permite adaptar el comportamiento acústico a salas técnicas o dispositivos sin altavoz.

PRECAUCIÓN En plataformas sin altavoz esta función puede no tener efecto.

8.5. Telegram: avisos mediante un bot

Telegram permite recibir mensajes en un chat privado o canal autorizado. pfSense no utiliza una cuenta personal de Telegram directamente: necesita un bot con su token de API y un destino donde el bot tenga capacidad para publicar.

Enable Telegram

QUÉ HACE Habilita el envío ordinario de notificaciones mediante la API de Telegram.

UTILIDAD Ofrece avisos relativamente inmediatos en móvil o escritorio.

PRECAUCIÓN No sustituye una monitorización crítica con garantías contractuales de entrega.

API Key

QUÉ HACE Token del bot que autoriza las solicitudes del firewall frente a Telegram.

UTILIDAD Identifica la integración y permite enviar avisos mediante el bot configurado.

PRECAUCIÓN Es una credencial secreta: limitar el acceso, revocarla si se expone y evitar mostrarla en capturas, registros o repositorios.

Chat ID

QUÉ HACE Identificador numérico del chat privado o identificador público de canal en formato @nombre donde se envían los mensajes.

UTILIDAD Permite dirigir cada notificación al espacio autorizado.

PRECAUCIÓN El bot debe tener los permisos y acceso necesarios; un ID correcto no basta si no puede escribir en el destino.

Test Telegram Settings

QUÉ HACE Envía un mensaje de prueba con la última configuración guardada, incluso si el envío ordinario está deshabilitado.

UTILIDAD Permite validar token, destinatario, conexión hacia la API y recepción.

PRECAUCIÓN Guardar antes de probar y comprobar el resultado en el chat de destino.

8.5.1. Procedimiento de configuración

1. Crear un bot mediante el procedimiento oficial de Telegram y custodiar su token.
2. Preparar el chat o canal de destino e incorporar el bot cuando sea necesario.
3. Introducir API Key y Chat ID en la sección correspondiente.
4. Activar Enable Telegram si se desean notificaciones automáticas.
5. Guardar los cambios y ejecutar Test Telegram Settings.
6. Confirmar la recepción y documentar quién administra el bot y quién recibe avisos.

8.6. Pushover: avisos con prioridad y reintentos

Pushover es una plataforma de notificaciones para aplicaciones y usuarios. pfSense puede utilizarla para enviar avisos con distintos niveles de prioridad y sonidos. Destaca la posibilidad de repetir avisos de emergencia hasta su reconocimiento dentro del límite de tiempo configurado.

Enable Pushover

QUÉ HACE Habilita el envío ordinario de avisos a través de Pushover.

UTILIDAD Permite separar las alertas de infraestructura de otros mensajes de uso diario.

PRECAUCIÓN El servicio remoto y el dispositivo del usuario deben estar operativos.

API Key

QUÉ HACE Token de aplicación registrado en Pushover.

UTILIDAD Autoriza a pfSense a utilizar la aplicación creada para la integración.

PRECAUCIÓN No compartir el token ni incluirlo en documentación.

User Key

QUÉ HACE Clave que identifica la cuenta usuaria que recibirá los mensajes.

UTILIDAD Determina el destinatario final autorizado por Pushover.

PRECAUCIÓN No confundir esta clave con la API Key de la aplicación.

Notification Sound

QUÉ HACE Selecciona el sonido asociado al mensaje, según las opciones disponibles en Pushover.

UTILIDAD Permite reconocer avisos de infraestructura sin consultar de inmediato la pantalla.

PRECAUCIÓN El comportamiento final puede depender del sistema operativo, las preferencias y el estado del dispositivo.

En la interfaz descrita aparecen estas opciones de sonido: Device Default, Pushover, Bike, Bugle, Cash Register, Classical, Cosmic, Falling, Gamelan, Incoming, Intermission, Magic, Mechanical, Piano Bar, Siren, Space Alarm, Tug Boat, Alien (long), Climb (long), Persistent (long), Echo (long), Up Down (long), Vibrate only y None (silent).

Message Priority

QUÉ HACE Fija la categoría de importancia del mensaje: Lowest, Low, Normal, High o Emergency.

UTILIDAD Permite adaptar la intensidad de la alerta a la relevancia operativa.

PRECAUCIÓN Elegir High o Emergency de forma indiscriminada causa fatiga de alertas y puede interferir con periodos de descanso.

Prioridad	Comportamiento descrito	Uso orientativo
Lowest	Sin sonido ni vibración; puede aumentar el contador.	Avisos puramente informativos.
Low	Sin sonido ni vibración; visualización según dispositivo.	Eventos de baja urgencia.
Normal	Notificación conforme a la configuración habitual del usuario.	Incidencias habituales.
High	Sonido y vibración destacados; puede superar silencios programados.	Eventos que requieren atención rápida.
Emergency	Reintenta notificaciones hasta confirmación o caducidad.	Incidencias críticas que requieren reconocimiento.

Emergency Priority Notification Retry Interval

QUÉ HACE Indica cada cuántos segundos Pushover repetirá un mensaje Emergency pendiente de reconocimiento. La API exige al menos 30 segundos y documenta 60 segundos como valor predeterminado.

UTILIDAD Define la persistencia temporal del recordatorio.

PRECAUCIÓN Intervalos demasiado breves generan reiteraciones; deben alinearse con el plan de guardias.

Emergency Priority Notification Expiration

QUÉ HACE Define durante cuántos segundos se mantienen los reintentos hasta reconocimiento o vencimiento. Pushover fija un máximo de 10.800 segundos (3 horas) y documenta 300 segundos como valor predeterminado.

UTILIDAD Evita que una alerta siga repitiéndose indefinidamente.

PRECAUCIÓN Cuando finaliza la ventana de reintentos, la incidencia puede continuar; utilizar monitorización y escalado complementarios.

Test Pushover Settings

QUÉ HACE Envía un mensaje de prueba con la última configuración guardada, aunque esté desactivado el servicio normal de notificaciones.

UTILIDAD Permite verificar credenciales, cuenta y recepción.

PRECAUCIÓN Guardar antes de probar; si se utiliza prioridad Emergency, comprobar cómo se reconoce la alerta desde el cliente.

8.7. Slack: avisos en canales de equipo

Slack concentra comunicaciones de un equipo en canales. Esta integración permite publicar avisos de pfSense en un canal accesible a personal autorizado, conservando el contexto de conversación y facilitando la coordinación ante incidencias.

Enable Slack

QUÉ HACE Activa el envío ordinario de notificaciones mediante la API de Slack.

UTILIDAD Centraliza la comunicación de eventos de red en el entorno de colaboración.

PRECAUCIÓN No es una alternativa al registro de eventos ni a sistemas de monitorización: es un canal de distribución.

API Key

QUÉ HACE Credencial de integración que pfSense utiliza para autenticarse ante Slack.

UTILIDAD Permite que el firewall publique avisos con los permisos concedidos a la integración.

PRECAUCIÓN La denominación mostrada puede referirse al token exigido por la implementación. Revisar el tipo de token y permisos que exige Slack en el momento de configurarlo.

Slack Channel

QUÉ HACE Nombre del canal de Slack al que se enviarán los avisos.

UTILIDAD Permite separar mensajes operativos de las conversaciones generales.

PRECAUCIÓN Verificar que la aplicación tenga acceso y permisos de publicación en ese canal.

Test Slack Settings

QUÉ HACE Envía una notificación de prueba utilizando los ajustes guardados, aunque el envío ordinario esté deshabilitado.

UTILIDAD Comprueba que la API recibe la solicitud y el mensaje llega al canal.

PRECAUCIÓN Guardar primero; una respuesta favorable no garantiza que el canal sea leído y atendido.

8.8. Guardar, probar y validar

Las pruebas de correo y de los canales de mensajería usan los últimos valores guardados, no necesariamente los que aparecen en campos todavía sin guardar. Esto es especialmente importante cuando se reemplazan contraseñas, tokens o destinatarios.

1. Comprobar fecha, hora, zona horaria, DNS y salida a Internet del propio firewall.
2. Preparar la cuenta de servicio o integración con permisos limitados.
3. Cumplimentar las opciones del canal deseado y revisar la validación TLS o los permisos API.
4. Pulsar Save y esperar la confirmación de guardado.
5. Ejecutar el botón Test correspondiente; puede funcionar aunque el canal esté deshabilitado para el uso ordinario.
6. Confirmar la llegada al destino previsto y revisar los registros relacionados si no llega.
7. Documentar responsable, destinatarios, política de rotación de credenciales y procedimiento de contingencia.

PRUEBA DE EXTREMO A EXTREMO Que el botón de prueba haya sido pulsado no demuestra por sí solo que el aviso haya llegado. Verifique que el destinatario recibió el mensaje correcto, que no terminó en spam y que los permisos o ajustes de notificaciones no lo ocultaron.

8.9. Ejercicios de administración y diagnóstico

Ejercicio 1 · Activar avisos de certificados

1. Abrir General Settings y activar Certificate Expiration.
2. Revisar el umbral considerando el tiempo habitual de renovación.
3. Determinar si deben excluirse los certificados revocados.
4. Guardar y comprobar que existen destinatarios operativos para los avisos.

Comprobación: la política queda guardada; las notificaciones de vencimiento se verificarán cuando corresponda a la revisión diaria. No es necesario provocar la caducidad de un certificado productivo.

Ejercicio 2 · Comprobar un fallo de correo

Situación: el botón de prueba SMTP no entrega ningún mensaje.

1. Validar resolución DNS del servidor SMTP desde el propio firewall.
2. Comprobar acceso al puerto TCP definido y posibles bloqueos del proveedor.
3. Confirmar la correspondencia entre puerto, TLS implícito y STARTTLS.
4. Revisar certificado, remitente, autenticación y política del proveedor.
5. Guardar de nuevo y repetir la prueba; inspeccionar los registros apropiados.

Interpretación: conectar al servidor no significa que éste acepte el mensaje ni que lo entregue al destinatario.

Ejercicio 3 · Telegram recibe pruebas, pero no alertas habituales

Una prueba correcta demuestra que el token, el destino y la conectividad funcionan en ese instante. Compruebe después que Enable Telegram esté activado, que los eventos esperados generen una notificación en pfSense y que los permisos del canal o chat no hayan cambiado.

Ejercicio 4 · Reducir ruido en Pushover

Revisar Message Priority y evitar que los avisos informativos se envíen como Emergency. Ajustar los reintentos a los procedimientos de atención de incidencias y distinguir los eventos que justifican interrumpir al personal de guardia.

Ejercicio 5 · Slack autentica, pero no publica

Validar el token actualmente guardado, los permisos de la integración, la pertenencia de la aplicación al canal y el nombre del destino. Volver a probar después de guardar. No pegar claves ni respuestas completas con credenciales en tickets o capturas.

8.10. Diagnóstico rápido por síntomas

Síntoma	Causas que conviene comprobar	Acción recomendada
No llega el correo	DNS, puerto, bloqueo SMTP, TLS, autenticación, spam.	Probar conectividad, revisar registros y confirmar el buzón.
Error de certificado SMTP	Cadena de confianza, nombre DNS o certificado vencido.	Corregir certificado/CA antes de relajar la validación.
Telegram no entrega	Token revocado, chat incorrecto, bot sin permisos.	Validar bot, destino y conectividad con la API.
Pushover repite avisos	Se emplea Emergency sin reconocimiento.	Comprobar confirmación, retry, expire y prioridad.
Slack rechaza el envío	Token, permisos API o canal sin acceso.	Revisar integración y autorizaciones en Slack.
La prueba usa datos antiguos	Se modificaron campos sin guardar.	Guardar y lanzar de nuevo Test.
No se reciben ciertos eventos	No todos los mensajes generan notificación; canal deshabilitado.	Revisar origen del evento y método habilitado.

8.11. Recomendaciones profesionales

Mantener más de un mecanismo de observación para eventos críticos. Las notificaciones no son un sustituto de los registros ni de un sistema de supervisión.

Utilizar cuentas o integraciones de servicio y aplicar el principio de mínimo privilegio.

Preferir SMTP cifrado y validar certificados de servidores remotos.

Custodiar tokens, claves de bot y contraseñas; rotarlos al cambiar los responsables o detectar exposición.

Definir destinatarios según necesidad operativa y evitar canales públicos para información sensible.

Priorizar los avisos: reservas de máxima urgencia para sucesos que realmente requieran respuesta.

Comprobar las notificaciones después de cambios de proveedores, credenciales, DNS, certificados o reglas de salida.

Incluir la revisión de caducidad de certificados en el calendario de mantenimiento.

8.12. Glosario y referencias

Término	Significado
SMTP	Protocolo utilizado para transferir correo entre sistemas.
STARTTLS	Negociación que eleva a TLS una conexión iniciada en texto claro.
TLS implícito	Conexión cifrada desde el inicio del diálogo con el servidor.
CA / CRL	Autoridad de certificación / lista de certificados revocados.
API Key / Token	Credencial que autoriza solicitudes a una API.
Chat ID / Channel	Identificador del destino de un mensaje en una plataforma.
Emergency	Prioridad de Pushover con reintentos y confirmación del destinatario.

Fuentes técnicas consultadas:

Netgate Documentation — Notifications: https://docs.netgate.com/pfsense/en/latest/config/advanced-notifications.html

Netgate Documentation — Changing Credentials and Keys: https://docs.netgate.com/pfsense/en/latest/recipes/changing-credentials.html

Telegram — Bots: https://core.telegram.org/bots

Pushover — API: https://pushover.net/api

Slack — API: https://api.slack.com/

El comportamiento exacto de algunas integraciones de terceros depende de su servicio, sus permisos y las políticas vigentes. Las etiquetas y el alcance de este capítulo corresponden a las opciones de pfSense Plus descritas en esta sección de administración.

09 System → Boot Environments

Administración de entornos de arranque ZFS: conservación de estados recuperables, activación, pruebas, recuperación y limpieza.

Una actualización puede introducir mejoras, pero también incompatibilidades de hardware, paquetes o configuración. Los Boot Environments aportan un mecanismo local de recuperación que permite seleccionar un entorno anterior del sistema y arrancar desde él cuando resulta necesario.



Figura 9.1. Ciclo de administración de entornos de arranque. Esquema conceptual sin datos de instalación.

Qué aprenderá el lector

Distinguir un entorno de arranque ZFS de una copia de seguridad externa.

Interpretar todas las columnas de la pantalla y los indicadores de entorno activo y próximo arranque.

Conocer las funciones de los iconos de estrella, edición, clonación, historial, arranque temporal y borrado.

Crear entornos manualmente, activar uno de forma persistente o probarlo durante un único arranque.

Aplicar procedimientos seguros antes de actualizar y durante una recuperación.

Administrar el consumo de espacio sin perder el último entorno conocido como válido.

ALCANCE La funcionalidad documentada requiere pfSense Plus compatible y una instalación sobre ZFS. La existencia de la opción en el menú indica soporte para esta gestión; una instalación UFS no dispone de la misma funcionalidad.

9.1. Concepto y ventajas de Boot Environments

Un Boot Environment (BE) es un entorno de arranque del sistema basado en instantáneas y clones ZFS. Una instantánea conserva una vista de un punto concreto del sistema de archivos y un clon permite disponer de un entorno utilizable en lectura y escritura. Gracias a ello, el firewall puede mantener estados anteriores desde los que volver a arrancar.

Su interés principal es reducir el riesgo operativo de cambios significativos: si una actualización provoca un problema, puede elegirse un entorno anterior y recuperar su estado sin tener que realizar una reinstalación completa. En versiones modernas de pfSense Plus, este mecanismo también participa en las actualizaciones automáticas y su verificación de arranque.

Concepto	Qué significa	Alcance
Entorno actual	Entorno desde el que se ha iniciado el firewall.	Es el sistema en ejecución en ese momento.
Entorno predeterminado	Entorno seleccionado para los próximos arranques normales.	Puede ser distinto del actual.
Instantánea ZFS	Vista de los datos en un punto temporal.	Su consumo crece según cambian los datos.
Clon ZFS	Entorno derivado de una instantánea.	Permite arrancar y trabajar con ese estado.

Concepto	Qué significa	Alcance
Rollback de arranque	Volver a ejecutar un entorno anterior.	No sustituye una copia externa ni protege frente a la pérdida del disco.

ADVERTENCIA FUNDAMENTAL **Un entorno de arranque se almacena en el propio dispositivo. Una avería del almacenamiento, un borrado accidental o un daño grave pueden afectar a todos los entornos. Antes de cambios importantes, exporte también una copia de la configuración y consérvela fuera del firewall.**

9.2. Acceso a la pantalla y requisitos

Ruta de la interfaz web: System → Boot Environments. Esta sección se encuentra directamente bajo System; no pertenece al submenú Advanced.

Los entornos de arranque ZFS se documentan para pfSense Plus 22.05 y posteriores. Es imprescindible que la instalación utilice ZFS; una instalación sobre UFS no puede habilitar esta función marcando una casilla: requiere reinstalar sobre ZFS. El sistema utiliza hardware compatible de 64 bits.

La pantalla muestra una tabla con los entornos existentes, una marca de estado al comienzo de las filas, acciones por entorno y los controles generales Delete, Quick Create y Create. La etiqueta «Version» que aparece en algunas interfaces se corresponde conceptualmente con «Base Version» en la documentación de Netgate.

9.3. Campos de la tabla principal

Casilla de selección

QUÉ MUESTRA / HACE Marca uno o varios entornos para ejecutar operaciones de conjunto, especialmente su eliminación. La casilla de la cabecera permite seleccionar las entradas elegibles.

UTILIDAD Ahorra tiempo cuando se revisan varios entornos antiguos.

PRECAUCIÓN La selección no ejecuta por sí sola una acción; el borrado se confirma posteriormente. El entorno en ejecución no puede eliminarse.

Indicador de estado (icono junto al nombre)

QUÉ MUESTRA / HACE Una marca de verificación rellena identifica el entorno desde el que ha arrancado el firewall. Una marca de verificación contorneada puede identificar el que se utilizará en el siguiente arranque, si difiere del actual.

UTILIDAD Evita confundir el entorno ejecutándose con el que está preparado para arrancar.

PRECAUCIÓN No deduzca el arranque predeterminado únicamente por el nombre o la versión; revise también la estrella y el Dashboard.

Name

QUÉ MUESTRA / HACE Nombre interno del entorno. Los creados automáticamente durante actualizaciones pueden llevar un prefijo y una marca temporal; los creados manualmente reciben el nombre escogido por el administrador.

UTILIDAD Permite identificar la finalidad de cada entorno y localizar una referencia estable en procedimientos de recuperación.

PRECAUCIÓN Un nombre descriptivo ayuda, pero no prueba que el entorno haya sido comprobado. Registrar su propósito en Description.

Version / Base Version

QUÉ MUESTRA / HACE Versión del software pfSense Plus que contiene el entorno correspondiente.

UTILIDAD Facilita reconocer desde qué versión puede recuperarse el firewall.

PRECAUCIÓN El número por sí solo no garantiza compatibilidad de configuraciones posteriores ni una recuperación completa de servicios externos.

Created

QUÉ MUESTRA / HACE Fecha y hora de creación del entorno.

UTILIDAD Permite relacionarlo con un cambio, mantenimiento o actualización.

PRECAUCIÓN La fecha de creación no equivale a la fecha del último uso.

Last Booted

QUÉ MUESTRA / HACE Última fecha y hora en que ese entorno se utilizó para iniciar el firewall.

UTILIDAD Ayuda a saber si un entorno fue arrancado alguna vez y a reconstruir una secuencia de pruebas.

PRECAUCIÓN Un campo vacío o antiguo no demuestra que un entorno sea inválido: sólo informa del historial de arranque.

Space

QUÉ MUESTRA / HACE Espacio de disco atribuido al entorno por ZFS. Depende de las diferencias entre instantáneas, clones y datos conservados.

UTILIDAD Permite localizar entornos cuyo mantenimiento consume almacenamiento.

PRECAUCIÓN No interpretar la cifra como una partición independiente ni sumar los tamaños de forma ingenua; ZFS comparte bloques y su consumo puede variar.

Description

QUÉ MUESTRA / HACE Anotación ampliada que documenta el contenido o propósito del entorno.

UTILIDAD Permite distinguir entornos de recuperación, cambios planificados y pruebas.

PRECAUCIÓN Evitar nombres de organizaciones, credenciales, direcciones internas u otros detalles que no deban incluirse en registros compartidos.

Actions

QUÉ MUESTRA / HACE Conjunto de iconos para seleccionar el próximo arranque, editar, clonar, consultar el historial, arrancar de manera temporal y eliminar.

UTILIDAD Centraliza las operaciones sin acudir a la línea de comandos.

PRECAUCIÓN La activación y el arranque temporal no tienen el mismo efecto; cada operación debe interpretarse antes de pulsarla.

9.4. Significado de los iconos de Actions

Icono o control	Acción	Consecuencia práctica
★ Estrella rellena	Muestra el entorno elegido para el próximo arranque normal.	Es una señal de selección, no un botón para reiniciar.
☆ Estrella vacía	Activar el entorno de forma persistente.	Se convertirá en predeterminado para arranques posteriores.
Lápiz	Edit.	Permite cambiar Name y Description.
Dos hojas / clon	Clone.	Abre la creación tomando el entorno indicado como origen.
Historial / ramas	Configuration History.	Abre las versiones de configuración guardadas dentro de ese entorno.
▶️ Reproducir	Arrancar temporalmente y reiniciar.	Prueba ese entorno una vez; después rige el predeterminado.
Papelera	Eliminar.	Libera almacenamiento asociado cuando ZFS pueda recuperarlo.

Icono o control	Acción	Consecuencia práctica
DIFERENCIA DECISIVA	**La estrella vacía prepara un entorno para futuros arranques normales (selección persistente). El botón de reproducción selecciona un entorno para un solo arranque y solicita reiniciar inmediatamente. No conviene confundir «elegir el próximo arranque» con «reiniciar ahora».**	

9.5. Botones generales de la parte inferior

Delete

QUÉ MUESTRA / HACE Elimina las entradas seleccionadas mediante las casillas de la tabla, tras una confirmación.

UTILIDAD Facilita la limpieza de entornos antiguos y la recuperación de espacio.

PRECAUCIÓN No borrar el único entorno anterior cuya recuperación ya se haya validado. No se puede borrar el entorno que está ejecutándose.

Quick Create

QUÉ MUESTRA / HACE Clona inmediatamente el entorno predeterminado y asigna automáticamente un nombre basado en el momento de creación.

UTILIDAD Crea con rapidez una referencia recuperable antes de una intervención.

PRECAUCIÓN Se clona el predeterminado, que no necesariamente coincide con el que está ejecutándose si existen selecciones temporales o pendientes.

Create

QUÉ MUESTRA / HACE Abre un formulario para configurar Name, Clone From y Description, y guardarlos con Save.

UTILIDAD Permite crear una referencia con una finalidad documentada y decidir su origen.

PRECAUCIÓN El nombre sólo admite caracteres alfanuméricos y guion bajo. No utilizar espacios, acentos ni símbolos especiales en Name.

9.5.1. Campos del formulario Create / Clone

Campo	Descripción	Recomendación
Name	Identificador del nuevo entorno; acepta letras, números y guion bajo.	Nombre breve, significativo y sin datos sensibles.
Clone From	Entorno existente que se usará como fuente.	Confirmar el origen: actual o predeterminado no siempre coinciden.
Description	Texto libre para describir el propósito.	Describir el cambio o la fase operativa sin revelar detalles privados.
Save	Confirma la creación del entorno.	Comprobar después que aparece en la tabla.

9.6. Procedimiento práctico: crear un punto recuperable

Objetivo: disponer de un entorno anterior conocido como válido antes de ejecutar una modificación importante. El procedimiento no realiza ninguna intervención por sí solo hasta que el administrador lo ejecute en la interfaz.

1. Comprobar en el Dashboard que el firewall funciona normalmente y qué Boot Environment aparece como actual y próximo.
2. Descargar una copia de configuración desde Diagnostics → Backup & Restore y guardarla fuera del dispositivo.
3. Entrar en System → Boot Environments y revisar la existencia de espacio libre suficiente.
4. Utilizar Create para indicar un nombre y una descripción; seleccionar conscientemente Clone From. También puede usarse Quick Create si se necesita un clon rápido del predeterminado.
5. Guardar y comprobar que el nuevo entorno aparece en la lista con el origen esperado.

6. Conservar anotada la finalidad del entorno y la forma de recuperarlo; no cambiar el entorno predeterminado sin un motivo concreto.

COMPROBACIÓN Crear un entorno no equivale a probar que el firewall puede arrancar desde él. Para una validación completa se necesita una prueba de arranque controlada, con acceso de recuperación disponible.

9.7. Procedimiento práctico: actualización con posibilidad de retorno

En versiones modernas de pfSense Plus con ZFS, el proceso de actualización crea por defecto un nuevo Boot Environment, realiza la actualización dentro de él y comprueba determinados errores antes y durante el arranque. Si detecta un fallo de arranque puede volver automáticamente a un entorno anterior conocido como válido.

1. Revisar el estado de la red, los servicios y el almacenamiento; consultar las notas de la actualización.
2. Guardar una copia externa de la configuración y verificar que existe un método de acceso a la consola.
3. En System → Boot Environments, identificar el entorno actualmente operativo y comprobar que existe margen de disco.
4. Iniciar la actualización desde System → Update siguiendo la ventana de mantenimiento prevista.
5. Una vez reiniciado, comprobar la versión, las interfaces, el gateway, DNS, VPN y los servicios esenciales.
6. Si el funcionamiento no es correcto, seleccionar con precaución un entorno anterior o recuperarlo desde el cargador de arranque.
7. Cuando se estabilice el servicio, revisar el estado actual y predeterminado para evitar un arranque no deseado en el siguiente reinicio.

ALCANCE DE LA RECUPERACIÓN El regreso a un entorno anterior revierte las áreas del sistema conservadas por el mecanismo de Boot Environments. Cambios en datos externos, otros equipos o servicios de terceros no se revierten automáticamente.

9.8. Activación persistente frente a arranque temporal

Modalidad	Cómo se selecciona	Qué sucede
Persistente	Acción ☆ del entorno deseado.	Queda elegido como predeterminado para futuros arranques; no es un reinicio inmediato.
Temporal	Acción ▶️ del entorno deseado y confirmación.	El firewall reinicia en él una vez y posteriormente vuelve al predeterminado.
Desde Reboot	Diagnostics → Reboot y selección de entorno.	Permite un arranque puntual; la selección no es persistente.
Desde el cargador	Menú de arranque → Boot Environments.	Permite seleccionar temporalmente un entorno cuando la GUI no está disponible.

La selección temporal es útil para probar la recuperación sin modificar permanentemente el objetivo de arranque; la persistente resulta apropiada cuando se decide que un entorno debe ser el sistema habitual. En ambos casos pueden producirse interrupciones al reiniciar.

SERVICIO EN PRODUCCIÓN No use el botón ▶️ como una simple vista previa: implica un reinicio. Planee una ventana de mantenimiento, informe del corte y disponga de acceso alternativo si el equipo queda inaccesible.

9.9. Recuperación desde el cargador de arranque

Cuando la interfaz web no responde después de una actualización, el menú inicial de arranque puede permitir escoger otro entorno ZFS. Es una opción de recuperación local o mediante una consola remota fuera de banda, siempre que el equipo permita acceder al cargador.

1. Conectar a la consola local o a una consola remota de gestión fuera de banda.

2. Reiniciar y acceder al menú del cargador de arranque.
3. Seleccionar Boot Environments (a menudo corresponde a la opción 8, aunque depende de la plataforma).
4. Usar la opción del menú que recorre los entornos disponibles hasta mostrar el deseado (documentada normalmente como 2).
5. Confirmar el entorno seleccionado y arrancar mediante Enter.
6. Una vez recuperado el acceso, comprobar cuál es el entorno predeterminado; la selección realizada desde el cargador es temporal.

La opción de selección bootfs del cargador no debe cambiarse salvo que exista una indicación técnica específica; en la mayoría de instalaciones no es necesario modificarla.

9.10. Gestión del espacio y eliminación segura

Las instantáneas ZFS mantienen referencias a bloques que, de otra forma, podrían quedar liberados. Por eso, el tamaño que ocupan los entornos puede crecer con el tiempo, especialmente después de actualizaciones importantes. La columna Space permite observar esta evolución, pero las cifras no deben leerse como archivos completamente separados.

1. Comprobar el espacio disponible en el Dashboard y en la lista de Boot Environments.
2. Localizar entornos antiguos que ya no se necesitan para recuperación y revisar su fecha y descripción.
3. Confirmar qué entorno está activo y cuál es el predeterminado para el próximo arranque.
4. Mantener al menos una ruta de recuperación apropiada y una copia externa de configuración.
5. Seleccionar únicamente los entornos descartables y pulsar Delete o la papelera individual.
6. Confirmar la eliminación y volver a comprobar el espacio disponible.

La cantidad de entornos a conservar depende de la política de cambios y de la capacidad del disco. Netgate comenta como práctica habitual conservar algunos entornos recientes, sin establecer una cifra universal obligatoria.

PRECAUCIÓN Un entorno eliminado deja de estar disponible para arranque. Un descenso de espacio libre no implica automáticamente una fuga de almacenamiento: puede reflejar bloques conservados por instantáneas ZFS.

9.11. Configuration History: historial por entorno

El icono de historial permite acceder al historial de configuración correspondiente a un Boot Environment. Cada entorno mantiene su propio conjunto de entradas de Configuration History; desde Diagnostics → Backup & Restore también es posible seleccionar a qué entorno corresponde el historial que se desea consultar.

Esta capacidad ayuda a investigar qué ajustes existían en un entorno anterior, pero debe distinguirse de recuperar el sistema completo. Restaurar un archivo de configuración, activar un entorno ZFS y restaurar una copia completa del dispositivo son procedimientos con objetivos y efectos distintos.

Función	Qué recupera o consulta	Cuándo resulta apropiada
Configuration History	Versiones guardadas de la configuración de un entorno.	Investigar o restaurar ajustes concretos.
Boot Environment	Un estado de arranque del sistema ZFS.	Regresar a un entorno del sistema anterior.
Configuration Backup externo	Configuración exportada fuera del firewall.	Reinstalación, desastre o migración controlada.
Copia del dispositivo/VM	Estado de discos y otros recursos incluidos en el respaldo.	Recuperación integral según herramienta y política.

9.12. Diagnóstico de incidencias frecuentes

No aparece Boot Environments

POSIBLE CAUSA El dispositivo no tiene soporte compatible para ZFS Boot Environments.

COMPROBAR Comprobar edición, versión y sistema de archivos.

ACTUAR No buscar una casilla oculta; revisar requisitos y opciones de instalación sobre ZFS.

Después de una prueba arranca otra versión

POSIBLE CAUSA Se utilizó una activación temporal, no persistente.

COMPROBAR Comparar el entorno actual y el predeterminado.

ACTUAR Seleccionar el deseado mediante ☆ cuando corresponda.

El disco pierde espacio libre

POSIBLE CAUSA Conservación de bloques por instantáneas/clones ZFS.

COMPROBAR Revisar Space, historial de actualizaciones y widgets de disco.

ACTUAR Eliminar sólo entornos prescindibles, tras confirmar recuperación externa.

No se puede borrar un entorno

POSIBLE CAUSA Es el entorno desde el que está funcionando el equipo o está protegido por su estado.

COMPROBAR Identificar el indicador de arranque actual.

ACTUAR No forzar eliminación por shell sin un procedimiento documentado y probado.

El sistema no inicia tras actualizar

POSIBLE CAUSA Posible fallo de actualización, hardware, paquetes o arranque.

COMPROBAR Acceso a consola y presencia de un entorno anterior.

ACTUAR Intentar recuperación con el menú de Boot Environments y verificar servicios.

No es posible activar un entorno seguro

POSIBLE CAUSA La interfaz no responde o no existe consola alternativa.

COMPROBAR Comprobar medios de acceso fuera de banda y backups.

ACTUAR Aplicar el plan de recuperación de desastres; BE no sustituye ese plan.

9.13. Lista de verificación antes de un cambio importante

Existe una copia de la configuración fuera del dispositivo.

Se ha identificado el entorno actual y el predeterminado.

El espacio de almacenamiento es suficiente para mantener un nuevo entorno.

Se ha conservado un estado conocido como operativo.

Existe un procedimiento de acceso a la consola y de recuperación.

El cambio se realizará en una ventana de mantenimiento adecuada.

Se han definido pruebas posteriores: red, DNS, VPN, reglas y servicios.

El responsable conoce la diferencia entre activación persistente y arranque temporal.

9.14. Resumen

Boot Environments permite gestionar estados arrancables del sistema pfSense Plus almacenado sobre ZFS. La pantalla reúne la identificación de entornos, su versión, creación, último uso, consumo de disco y una colección de acciones para crearlos, editarlos, clonarlos, activarlos o eliminarlos.

La utilidad principal no es acumular instantáneas, sino disponer de una estrategia de recuperación: conservar estados conocidos como válidos, comprobar que es posible volver a arrancarlos, mantener espacio suficiente y respaldar la configuración también fuera del dispositivo.

9.15. Referencias técnicas

ZFS Boot Environments · Managing Boot Environments in the GUI · How Boot Environments Work · Boot Environment Status

Boot Environment Requirements · Boot Environment Disk Space Usage · Selecting Boot Environments in the Loader Menu · Upgrade Process Overview

10 System → Certificates → Authorities

Administración de autoridades certificadoras X.509: consulta, búsqueda, creación, importación, exportación, renovación y protección de claves.

Las autoridades certificadoras permiten a pfSense Plus comprobar la identidad criptográfica de servidores, usuarios y dispositivos. La pantalla Authorities presenta las entidades de confianza disponibles y concentra las operaciones necesarias para mantenerlas de forma segura.



Figura 10.1. Relación entre una autoridad certificadora, los certificados emitidos y los servicios que validan la confianza.

Qué aprenderá el lector

Diferenciar una autoridad certificadora (CA), un certificado final y una lista de revocación (CRL).

Interpretar Search y todas las columnas de Certificate Authorities.

Reconocer los iconos de edición, exportación de certificado, exportación de clave y renovación.

Crear o importar una CA con conocimiento de los campos y de sus dependencias.

Comprobar la vigencia y los usos de una CA antes de renovarla, reemplazarla o retirarla.

Proteger las claves privadas y evitar interrupciones en servicios que dependen de certificados.

ALCANCE DE LA PANTALLA El capítulo documenta la vista Authorities. Las pestañas Certificates y Revocation pertenecen al mismo gestor, pero administran otros objetos; aquí se explican únicamente para situar el funcionamiento de la PKI.

10.1. Qué es una autoridad certificadora y por qué importa

Una autoridad certificadora o CA (Certificate Authority) es una entidad criptográfica que firma certificados digitales. Los sistemas que confían en su certificado público pueden comprobar si un certificado presentado por un servicio o un cliente fue emitido por ella y si la cadena de confianza es válida.

La CA no sustituye las reglas de firewall ni la autorización de acceso: acredita identidades en los sistemas que verifican el certificado. Un servicio VPN, por ejemplo, también necesita sus políticas de autenticación, revocación, redes y permisos.

Elemento	Función	Qué puede distribuirse
Certificado público de CA	Permite verificar firmas y cadenas de confianza.	Sí, a sistemas que deban confiar en ella.
Clave privada de CA	Permite firmar nuevos certificados y CRL.	No; solo bajo un procedimiento de custodia extraordinario.
Certificado de servidor o cliente	Identifica a un servicio, equipo o usuario.	Su parte pública sí; la clave privada del titular, no.
Lista de revocación (CRL)	Enumera certificados que ya no deben aceptarse.	Sí, en los servicios que verifican revocaciones.

Elemento	Función	Qué puede distribuirse
SEGURIDAD FUNDAMENTAL Si alguien obtiene la clave privada de una CA de confianza, puede emitir certificados que otros equipos podrían aceptar como legítimos. Exportar la CA pública y exportar su clave privada son operaciones muy diferentes.		

CA raíz, CA intermedia y CA interna/externa

Una CA raíz puede ser autofirmada (self-signed), mientras que una CA intermedia está firmada por una autoridad superior. En esta pantalla, «Internal» señala que pfSense dispone de la clave privada de esa CA y puede utilizarla para firmar; una CA importada solo con certificado público se considera externa. «Self-signed» y «Internal» no son sinónimos.

10.2. Navegación por el gestor Certificates

Ruta: System → Certificates → Authorities. La interfaz puede mostrar la pestaña como «Authorities» y la documentación de Netgate como «CAs». Ambas denominaciones hacen referencia a la administración de autoridades certificadoras.

Pestaña	Contenido	Diferencia principal
Authorities	Autoridades de certificación y cadenas de confianza.	Identifica quién puede firmar y a quién se confía.
Certificates	Certificados de servidor, cliente y otras entradas.	Identifica al sujeto o servicio que utiliza un certificado.
Revocation	Listas de revocación de certificados (CRL).	Gestiona certificados anulados antes de su vencimiento.

La banda superior incorpora la ruta de navegación, el acceso a ayuda y las pestañas del gestor. Los bloques Search y Certificate Authorities pueden incluir controles para contraer o expandir su visualización.

10.3. Bloque Search: localizar una autoridad

Search term

QUÉ HACE Campo de texto que admite palabras y expresiones regulares de estilo Unix para buscar por nombre del certificado y por su nombre distinguido (Distinguished Name o DN).

VENTAJA Agiliza auditorías cuando existen numerosas autoridades.

A TENER EN CUENTA Una expresión regular mal escrita puede devolver resultados inesperados; primero utilice texto sencillo cuando solo desea encontrar una entrada.

Selector de búsqueda (Both)

QUÉ HACE Desplegable que limita el ámbito de la búsqueda. La opción visible «Both» permite consultar conjuntamente las categorías de coincidencia disponibles.

VENTAJA Permite combinar la búsqueda por nombre descriptivo e identidad sin revisar ambas por separado.

A TENER EN CUENTA Los valores exactos del selector pueden variar entre versiones; se selecciona el ámbito según el dato conocido.

Search y Clear

QUÉ HACE Search ejecuta el filtro; Clear limpia el término y permite volver a visualizar la lista completa.

VENTAJA Facilita localizar una CA sin alterar sus propiedades.

A TENER EN CUENTA Son controles de consulta: no borran certificados ni cambian la configuración de la CA.

El icono circular del encabezado del bloque permite contraer o expandir el formulario de búsqueda. No elimina el bloque ni modifica la información almacenada.

10.4. Tabla Certificate Authorities: lectura de columnas

Columna	Qué muestra	Cómo interpretarla
Selección	Casilla para seleccionar una entrada, cuando esté disponible.	No constituye una acción hasta aplicar un control asociado.
Name	Etiqueta descriptiva asignada a la CA en pfSense.	Sirve para identificarla dentro de la GUI; no es necesariamente el DN.
Internal	Indica disponibilidad de su clave privada en el gestor.	Con clave privada puede emitir certificados y firmar CRL.
Issuer	Autoridad emisora de este certificado de CA.	«Self-signed» identifica una CA autofirmada; una intermedia mostrará su emisor.
Certificates	Número de certificados relacionados registrados en el gestor.	Es una referencia administrativa local, no un censo universal de todos los certificados emitidos externamente.
Identity	Nombre distinguido (DN), información de vigencia y acceso a detalles.	Permite comprobar la identidad y la fecha de expiración.
In Use	Servicios o componentes que el sistema detecta usando la CA.	No garantiza identificar todas las dependencias, especialmente paquetes.
Actions	Accesos a editar, exportar, renovar y, si procede, borrar.	Cada icono tiene consecuencias distintas sobre la confianza.

10.5. Identity y validez: cómo leer una CA

Identity contiene el Distinguished Name (DN o nombre distinguido): un conjunto de atributos X.509 que describen la identidad de la CA. Su composición depende de cómo fue emitida. La fila también puede mostrar «Valid From», «Valid Until» y un icono de información.

Atributo	Nombre habitual	Interpretación
CN	Common Name	Nombre común que identifica a la autoridad.
O	Organization	Organización declarada en el certificado.
OU	Organizational Unit	Unidad o departamento, si fue definido.
L	Locality	Localidad declarada por el emisor.
ST	State or Province	Región o provincia declarada.
C	Country	Código de país de dos letras.
Valid From / Valid Until	Intervalo de vigencia	Periodo durante el cual la CA declara ser válida.
Icono de información	Detalles del certificado	Muestra propiedades adicionales según la versión.

Cuando una entrada se aproxima al vencimiento, la interfaz puede resaltarlo en amarillo; si ya ha vencido, en rojo. Estas indicaciones ayudan a priorizar actuaciones, pero la validez real también depende de la cadena, de la confianza configurada y de las reglas del servicio consumidor.

NOTA SOBRE PRIVACIDAD El Distinguished Name puede contener información de organizaciones, personas o ubicaciones. En capturas destinadas a documentación pública deben eliminarse esos valores, incluso cuando no aparezcan direcciones IP.

10.6. Actions: explicación de todos los iconos

Icono	Operación	Qué provoca
Lápiz	Edit (editar)	Abre la entrada para ajustar sus propiedades, como Trust Store o datos importados.

Icono	Operación	Qué provoca
Símbolo de certificado	Export certificate	Descarga el certificado público de la CA, normalmente con extensión .crt.
Llave	Export private key	Descarga la clave privada de la CA (.key), solo si está disponible.
Flecha circular	Renew / Reissue	Abre el asistente de renovación o reemisión, cuando la CA admite esta operación.
Papelera (si aparece)	Delete	Elimina la CA cuando no está en uso y la interfaz permite borrarla.

Los iconos visibles dependen de si la entrada es interna, si está en uso y de las capacidades de renovación de la versión. La ausencia de papelera en una fila en uso es una protección deliberada frente a eliminaciones que afectarían a servicios.

Editar no es renovar

Editar suele implicar cambiar datos administrativos o importados, por ejemplo incorporar una clave privada que falte o controlar si la CA entra en el almacén de confianza. Renovar/reemitir produce una copia nueva firmada y puede cambiar vigencia, clave o identificadores. Conviene tratar esta segunda operación como un cambio con posible impacto en clientes.

Certificado público frente a clave privada

El archivo de certificado CA (.crt) puede incorporarse a sistemas que deban verificar una cadena de confianza. La clave privada (.key) permite firmar y debe permanecer custodiada. Para configurar clientes de VPN, normalmente se distribuye el certificado de CA, nunca su clave privada.

10.7. Crear o importar una CA con Add

El botón verde Add abre un formulario de alta. El administrador elige un Method según quiera crear una CA raíz interna, importar una CA existente o generar una CA intermedia firmada por otra autoridad interna.

Method	Cuándo se utiliza	Condición clave
Create an Internal Certificate Authority	Crear una nueva raíz de confianza administrada por el firewall.	El sistema genera la CA y custodia su clave privada.
Import an Existing Certificate Authority	Incorporar una CA existente a la confianza o a la administración local.	Sin clave privada importada, solo puede verificar, no firmar.
Create an Intermediate Certificate Authority	Crear una CA subordinada a otra CA interna disponible.	Necesita una autoridad superior capaz de firmarla.

Campos habituales del formulario de creación / edición

Campo	Función y pauta operativa
Descriptive Name	Nombre administrativo visible en listas. No determina por sí solo la identidad X.509.
Method	Define si se genera una CA, se importa una existente o se crea una intermedia.
Trust Store	Si se activa, añade la CA al almacén de confianza del firewall y afecta a operaciones del sistema.
Randomize Serial	Genera números de serie impredecibles al emitir certificados, práctica recomendada.
Key Type / Key Length / Curve	Determina algoritmo y parámetros de la clave. RSA y ECDSA deben elegirse según la compatibilidad.
Digest Algorithm	Algoritmo de firma; evitar algoritmos considerados débiles, como SHA-1.
Lifetime	Duración de validez; ponderar seguridad y obligaciones de renovación.

Campo	Función y pauta operativa
Distinguished Name	Campos de identidad (CN, O, OU, C, etc.); evitar datos innecesarios.
Certificate Data	Certificado público en PEM cuando se importa o actualiza una CA.
Certificate Private Key	Clave privada PEM opcional al importar; solo incluirla si la CA debe firmar desde pfSense.
Next Certificate Serial	Siguiente número de serie cuando no se utiliza aleatorización.
Signing Certificate Authority	CA superior que firmará una nueva CA intermedia, si se elige ese método.

PRINCIPIO DE MÍNIMO PRIVILEGIO Importar el certificado de una CA para confiar en ella no obliga a importar su clave privada. Mantener las claves de una autoridad raíz fuera de los dispositivos que no necesitan emitir certificados reduce riesgos.

10.8. Procedimiento práctico: comprobar una autoridad existente

1. Abrir System → Certificates → Authorities.
2. Localizar la CA mediante Search y dejar visible la lista completa antes de cualquier cambio.
3. Revisar Name, Internal e Issuer para identificar su papel y si el firewall posee la clave de firma.
4. Leer Identity y las fechas de validez, usando el icono de información si hace falta.
5. Examinar Certificates e In Use, recordando que algunos paquetes pueden establecer dependencias adicionales.
6. Comprobar qué servicios confían en esa autoridad y que sus certificados no están vencidos.
7. Documentar la revisión sin copiar nombres distinguibles, claves ni datos de la instalación.

Resultado: se obtiene un diagnóstico de inventario sin editar, descargar claves privadas ni interrumpir servicios.

10.9. Procedimiento práctico: exportar una CA pública

1. Acceder a Authorities y localizar la entrada pertinente.
2. Confirmar que se necesita distribuir confianza pública, no material para firmar nuevos certificados.
3. Pulsar el icono de certificado, no el icono de llave.
4. Almacenar el archivo .crt en una ubicación controlada.
5. Importar el certificado público en el servicio o cliente correspondiente, siguiendo su procedimiento.
6. Verificar la cadena de confianza desde el sistema consumidor.

El certificado público de la CA sirve para verificar certificados emitidos por ella. No sustituye el certificado de identidad ni la clave privada del servidor o del cliente.

NUNCA POR COSTUMBRE La exportación de la clave privada solo debe contemplarse en migraciones o copias de seguridad muy controladas. En una distribución ordinaria de clientes, exportar la clave privada de la CA es un error grave.

10.10. Renovación o reemisión: analizar antes de confirmar

El asistente Renew/Reissue permite emitir una nueva copia y conservar o modificar determinadas propiedades. Las opciones Reuse Key, Reuse Serial y Strict Security tienen efectos distintos: conservar la clave mantiene continuidad criptográfica; cambiarla crea otra identidad de firma. Para una CA, cambiar la clave o el número de serie puede invalidar los certificados que dependen de ella.

Opción	Qué cambia	Impacto a estudiar
Reuse Key	Mantiene la clave existente cuando está seleccionada.	Ayuda a preservar la continuidad de la CA, aunque hay que revisar la vigencia.

Opción	Qué cambia	Impacto a estudiar
Reuse Serial	Conserva el serial de la CA al reemitir.	Puede favorecer compatibilidad con certificados existentes; algunos clientes tienen restricciones.
Strict Security	Ajusta propiedades a recomendaciones de seguridad actuales.	Puede alterar algoritmos y parámetros; exige pruebas de compatibilidad.
Confirmar renovación	Sustituye la entrada por el certificado reemitido.	Los servicios consumidores pueden reiniciarse y hay que redistribuir material actualizado.

1. Inventariar los certificados dependientes y servicios que usan la CA.
2. Disponer de copia segura de configuración y plan de recuperación fuera del dispositivo.
3. Comprobar vigencia, algoritmos y compatibilidad de los clientes.
4. Abrir Renew/Reissue y estudiar Reuse Key, Reuse Serial y Strict Security sin confirmar todavía.
5. Planificar la migración y la distribución de la nueva CA si es necesaria.
6. Ejecutar únicamente en una ventana de cambio autorizada y verificar inmediatamente servicios y clientes.

CUIDADO CON LA CADENA DE CONFIANZA Una CA renovada no es automáticamente equivalente a la original para todos los clientes. No cambiar clave privada ni serial a ciegas: pueden dejar de validar certificados previamente emitidos.

10.11. Eliminar una CA: dependencias y comprobación

Para eliminar una autoridad debe dejar de estar en uso. Es necesario revisar VPN, autenticación, servicios y paquetes. La columna In Use identifica dependencias detectadas por la interfaz, pero puede no recoger todas las referencias de componentes adicionales.

1. Identificar todos los certificados y servicios relacionados con la CA.
2. Sustituir la confianza o los certificados dependientes por los nuevos, si procede.
3. Verificar el funcionamiento de los servicios y clientes tras la migración.
4. Volver a Authorities y comprobar si aparece la acción Delete.
5. Confirmar la eliminación solo cuando exista evidencia de que la CA no es necesaria.
6. Comprobar la ausencia de errores de validación en sistemas clientes y VPN.

La ausencia de un icono de borrado puede ser normal en una CA utilizada. Nunca debe intentarse forzar una eliminación sin entender sus dependencias.

10.12. Diagnóstico: incidencias frecuentes

Síntoma	Posible causa	Primera comprobación
Un cliente no confía en un servidor	La CA emisora no está instalada como confiable o falta parte de la cadena.	Revisar la cadena y el almacén de confianza del cliente.
No puede firmarse un nuevo certificado	La CA fue importada solo con certificado público, sin clave privada.	Revisar la columna Internal y la custodia de la clave.
VPN deja de autenticar usuarios tras renovar	Se reemitió la CA cambiando clave o serial; los clientes no reconocen la nueva cadena.	Verificar cadenas y distribuir material nuevo mediante un procedimiento controlado.
No aparece la papelera	La CA sigue en uso.	Examinar In Use y dependencias de paquetes y VPN.
La CA figura caducada	Su periodo de validez terminó.	Planificar sustitución/renovación y comprobar certificados firmados.
No hay resultados en Search	Filtro restrictivo, selección de ámbito o patrón erróneo.	Pulsar Clear y repetir una búsqueda más sencilla.

10.13. Buenas prácticas y resumen

Separar las autoridades por ámbitos con niveles de confianza distintos; no reutilizar indiscriminadamente una CA para todas las VPN.

Conservar copias de configuración y claves bajo procedimientos de custodia y acceso restringido.

Revisar la vigencia de CA y certificados finales y utilizar las notificaciones de caducidad del sistema.

Evitar SHA-1 y parámetros criptográficos débiles, respetando compatibilidad documentada.

Preferir CA externas sin clave privada cuando pfSense solo necesita verificar certificados.

No borrar ni renovar sin inventario de consumidores; las dependencias pueden extenderse a paquetes.

En materiales publicados, nunca mostrar DN, nombres organizativos, direcciones, fechas de instalación ni material de claves de una infraestructura.

La pantalla Authorities es el punto de control de la confianza X.509 en pfSense Plus. Saber distinguir «certificado», «clave privada», «CA en uso» y «renovación» permite administrar VPN y otros servicios con criterios de continuidad y seguridad.

Referencias técnicas

Netgate — Certificate Management: https://docs.netgate.com/pfsense/en/latest/certificates/index.html

Netgate — Certificate Authority Management: https://docs.netgate.com/pfsense/en/latest/certificates/ca.html

Netgate — Certificate Properties: https://docs.netgate.com/pfsense/en/latest/certificates/components.html

Netgate — Renew or Reissue a CA or Certificate: https://docs.netgate.com/pfsense/en/latest/certificates/renew.html

Netgate — Certificate Revocation List Management: https://docs.netgate.com/pfsense/en/latest/certificates/crl.html

11 System → Certificates → Certificates

Inventario de certificados digitales, uso en servicios, exportación segura, firma de solicitudes y operaciones de renovación.

El gestor de certificados centraliza las identidades criptográficas utilizadas por la administración HTTPS, las conexiones VPN y otros servicios del firewall. Esta pantalla permite localizar cada certificado, comprobar quién lo ha emitido, qué identidad representa, cuál es su vigencia y dónde se utiliza.



Figura 11.1. Ciclo operativo de un certificado: generación de claves, emisión, uso, vigencia y renovación.

Objetivos del capítulo

Interpretar todos los campos de la pestaña Certificates y los iconos de acción.

Comprender la diferencia entre un certificado de servidor, uno de usuario y una CA.

Reconocer el papel del emisor, el nombre distinguido, la vigencia y el uso activo.

Crear o importar certificados y utilizar solicitudes de firma (CSR).

Exportar correctamente archivos públicos, claves privadas y contenedores PKCS #12.

Renovar, sustituir o retirar certificados sin perder la conectividad de servicios.

DÓNDE ESTAMOS La ruta es System → Certificates → Certificates. Authorities administra las CA y Revocation gestiona listas y entradas de revocación; esta pantalla administra certificados finales y solicitudes CSR.

11.1. Un certificado no es una clave privada

Un certificado digital X.509 reúne una clave pública, datos de identidad, extensiones de uso, emisor, número de serie y periodo de validez. Una firma criptográfica permite comprobar su integridad y procedencia. La clave privada asociada no forma parte de la información pública del certificado y debe permanecer bajo control de su titular.

El certificado por sí solo no abre una conexión VPN ni concede privilegios. La aplicación tiene que verificar su cadena de confianza, vigencia, finalidad, revocación cuando corresponda y demás reglas de autenticación y autorización.

Elemento	Para qué sirve	Precaución
Certificado (.crt / .pem)	Identificación pública y validación de la firma de su emisor.	Puede distribuirse donde sea necesario; validar su procedencia.
Clave privada (.key)	Demuestra posesión de la identidad y permite operaciones criptográficas.	No enviarla por canales inseguros ni publicarla.
PKCS #12 (.p12 / .pfx)	Agrupa certificado, clave y, cuando procede, cadena de confianza.	Proteger con contraseña robusta y controlar el destinatario.
CSR (.req / .pem)	Solicitud para que una CA emita un certificado.	Solo se transmite la solicitud, nunca la clave privada.

Elemento	Para qué sirve	Precaución
CA emisora	Firma el certificado y participa en su cadena de confianza.	Debe ser confiable para el sistema consumidor.

11.2. Estructura de la pantalla Certificates

La cabecera de navegación contiene las pestañas Authorities, Certificates y Revocation. La pestaña activa muestra el bloque de búsqueda, una tabla de entradas existentes y el botón Add/Sign. Los resultados visibles dependen del inventario y de las capacidades de la edición instalada.

Search: encontrar certificados sin modificar nada

Control	Uso práctico
Search term	Cadena de texto con la que localizar certificados; la ayuda de la pantalla admite también expresiones regulares de tipo Unix.
Selector de alcance (Both)	Permite definir el ámbito de búsqueda según las opciones disponibles en la interfaz; Both incluye ambos ámbitos de nombres indicados por el buscador.
Search	Aplica el texto y el alcance del filtro a la tabla.
Clear	Elimina el criterio y recupera la visualización sin filtros.
Icono de minimizar	Contrae o despliega el área Search; no elimina certificados ni filtros del inventario.

La búsqueda es una herramienta de lectura. Resulta especialmente útil cuando hay numerosos certificados de servicios, usuarios y VPN y se necesita encontrar una identidad sin desplazarse por toda la lista.

11.3. Columnas de la tabla Certificates

Name

QUÉ HACE Muestra el nombre descriptivo asignado a la entrada. Bajo el nombre pueden aparecer indicadores como CA: No y Server: Yes/No. En algunos certificados aparece un símbolo de renovación automática junto al nombre.

VENTAJA Permite reconocer el objeto por una denominación administrativa y distinguir su uso general.

ATENCIÓN El nombre descriptivo no constituye una prueba de identidad criptográfica; un nombre parecido no significa que los certificados sean equivalentes.

Issuer

QUÉ HACE Identifica la autoridad emisora. «self-signed» indica que el certificado está autofirmado; un certificado firmado por una CA interna muestra dicha autoridad como emisor.

VENTAJA Facilita seguir la cadena de confianza y determinar si el firewall puede gestionar una reemisión local.

ATENCIÓN Una CA confiable en pfSense no implica automáticamente que lo sea en todos los clientes o navegadores.

Identity

QUÉ HACE Resume el Subject o Distinguished Name (DN), las fechas Valid From y Valid Until y ofrece un botón de información para ver más propiedades.

VENTAJA Permite revisar de un vistazo quién es el titular y si el certificado se encuentra dentro del periodo válido.

ATENCIÓN No publicar la identidad de los certificados de producción en manuales o informes; el DN puede contener información organizativa.

In Use

QUÉ HACE Muestra referencias detectadas a servicios que emplean el certificado, por ejemplo la GUI o una configuración VPN.

VENTAJA Ayuda a estimar el impacto de renovar o sustituir una entrada.

ATENCIÓN La lista puede no representar todas las dependencias: algunos paquetes y consumidores externos requieren comprobación adicional.

Actions

QUÉ HACE Agrupa las operaciones disponibles: editar, exportar, renovar o eliminar según la entrada.

VENTAJA Concentra la administración del ciclo de vida.

ATENCIÓN No todos los iconos aparecen en todas las filas: depende de si la entrada está en uso y de cómo se emitió.

11.4. Interpretación de símbolos e indicadores

Símbolo o dato	Interpretación	Qué comprobar
CA: No	La entrada no es un certificado de autoridad certificadora.	No confundirlo con el estado de confianza de la CA emisora.
Server: Yes	Certificado marcado para autenticación de servidor.	EKU y SAN adecuados al servicio que lo presenta.
Server: No	No está marcado como certificado de servidor; suele corresponder a un uso de usuario/cliente.	Validar finalidad real y EKU antes de asignarlo.
self-signed	El propio certificado lo firma.	La entidad que lo use debe confiar explícitamente en él.
Valid From / Valid Until	Comienzo y fin del periodo de vigencia.	Reloj correcto, fecha próxima a caducar y cadena de confianza.
Icono de información (i)	Muestra propiedades ampliadas como identidad, extensiones o detalles criptográficos.	Revisar SAN, tipo, emisor y fechas.
Icono de renovación junto a Name	Indica Auto Renew habilitado para esa entrada.	No confundir con la acción manual de Renew/Reissue al final de la fila.

La interfaz puede resaltar fechas próximas a caducar o ya vencidas. El umbral y las notificaciones se gestionan desde System → Advanced → Notifications. Un certificado no pasa a ser válido por el mero hecho de que figure en la tabla.

COMPROBACIÓN DE IDENTIDAD En conexiones HTTPS actuales, los nombres que valida un cliente se comparan con Subject Alternative Name (SAN). El Common Name (CN) no debe tratarse como sustituto general del SAN.

11.5. Acciones: para qué sirve cada icono

Icono / operación	Resultado	Precaución esencial
Lápiz — Edit	Abre la edición de etiqueta, certificado y clave asociados, junto con opciones de exportación.	Cambiar certificado o clave en una entrada usada por un servicio requiere planificar el impacto.
Escarapela — Export Certificate	Descarga el certificado público en formato .crt.	No incluye por sí sola la clave privada necesaria para acreditar identidad.
Llave — Export Private Key	Descarga la clave privada asociada, si está disponible.	Material sensible; preferir exportación cifrada cuando sea posible.
Archivo — Export PKCS #12	Descarga contenedor .p12 con identidad, clave y cadena aplicable.	Custodia y contraseña del contenedor son fundamentales.
Flecha circular — Renew/Reissue	Inicia la reemisión de entradas compatibles con CA local.	Revisar Reuse Key, serial y redistribución antes de confirmar.

Icono / operación	Resultado	Precaución esencial
Papelera — Delete	Elimina la entrada cuando ya no está referenciada.	No equivale a revocar un certificado ya distribuido.
Add/Sign	Abre las opciones de creación, importación y firma.	Elegir método y finalidad antes de generar o mover claves.

Al situar el cursor sobre un icono, pfSense puede mostrar una descripción emergente de la acción. La presencia o ausencia de controles depende de la versión y las dependencias del certificado.

DISTINCIÓN CRÍTICA La renovación automática aparece junto al nombre cuando está habilitada. El botón Renew/Reissue al final de la fila es una operación manual distinta. La papelera normalmente no está disponible mientras la entrada esté en uso.

11.6. Add/Sign: crear, importar o firmar

El botón Add/Sign abre un formulario cuyo contenido varía según el método elegido. En el inventario se visualiza el resultado de la operación; los campos de generación y firma aparecen en el formulario posterior.

Method	Para qué se emplea	Requisito clave
Create an Internal Certificate	Emite un certificado desde una CA almacenada localmente.	La CA firmante debe tener su clave privada disponible.
Import an Existing Certificate	Incorpora un certificado emitido por otro sistema o autoridad.	Certificado y clave correspondiente, en PEM o PKCS #12 según el método.
Create a Certificate Signing Request	Genera una solicitud CSR para que una CA la firme.	Custodiar la clave privada; entregar solo la CSR al emisor.
Sign a Certificate Signing Request	Firma una CSR nueva o existente con una CA interna.	La CA local firmante debe disponer de clave privada.

Campos que deben comprenderse antes de emitir

Campo / propiedad	Sentido operativo
Descriptive Name	Etiqueta administrativa utilizada para identificar el certificado dentro de pfSense.
Certificate Authority	Autoridad que firma un certificado interno o una CSR, según el flujo.
Certificate Type	Finalidad: User Certificate o Server Certificate; determina restricciones y usos extendidos.
Key Type y tamaño / curva	Algoritmo de clave y nivel de seguridad; elegirlo de acuerdo con la compatibilidad del servicio.
Digest Algorithm	Algoritmo de resumen criptográfico para la firma; evitar SHA-1 cuando sea posible.
Lifetime	Número de días de vigencia; valorar política del emisor, seguridad y renovaciones.
Distinguished Name (DN)	Campos de sujeto como CN, O, OU, C; contienen información identificativa.
Subject Alternative Name (SAN)	Identidades adicionales, especialmente hostnames o IP que se validarán para TLS.
Certificate Data / Private Key Data	Contenido del certificado y la clave PEM al importar o sustituir entradas.
Export Password / PKCS #12 Encryption	Protección y compatibilidad de los archivos que contienen claves privadas.

11.7. Procedimiento práctico: auditar un certificado existente

1. Abrir System → Certificates → Certificates y pulsar Clear para mostrar la lista completa.
2. Localizar la entrada con Search y confirmar el nombre descriptivo y el Issuer.
3. Revisar los indicadores de finalidad: CA: No y Server: Yes/No, sin inferir que bastan para validar todos los usos.
4. Leer Valid From y Valid Until; comprobar que la hora del firewall es correcta.
5. Abrir información ampliada y revisar SAN, emisor, algoritmos y tipo si están disponibles.
6. Examinar In Use y contrastarlo con la configuración del servicio y de los paquetes que pudieran emplearlo.
7. Registrar solo el resultado funcional de la auditoría, sin copiar DN ni datos sensibles al documento de consulta.

Resultado esperado: conocer finalidad, vigencia, procedencia y dependencias, sin modificar el certificado.

11.8. Procedimiento práctico: emitir un certificado de servicio

1. Confirmar previamente qué servicio va a utilizar el certificado y qué nombre o identidad debe presentar.
2. Comprobar que existe una CA autorizada para firmar el certificado; su certificado público deberá ser confiable para los consumidores.
3. Pulsar Add/Sign y seleccionar Create an Internal Certificate.
4. Elegir la CA que firmará y establecer Certificate Type como Server Certificate.
5. Elegir parámetros criptográficos compatibles y un periodo de validez adecuado a la política aplicable.
6. Introducir el identificador de servicio y los nombres SAN correctos, sin datos adicionales innecesarios.
7. Guardar y verificar la nueva entrada en la lista de certificados.
8. Asignar el certificado al servicio correspondiente mediante su pantalla de configuración y comprobar la conexión real desde un cliente.

VERIFICACIÓN INDISPENSABLE Crear un certificado no lo asigna automáticamente a webConfigurator, OpenVPN u otro servicio. La asignación se realiza en las opciones del servicio que vaya a presentarlo.

11.9. Procedimiento práctico: importar una identidad existente

1. Asegurar el origen y la legitimidad del certificado y de la clave privada que se desea importar.
2. Entrar en Add/Sign y seleccionar Import an Existing Certificate.
3. Elegir importación PEM X.509 o archivo PKCS #12 según el material recibido.
4. Para PEM, proporcionar Certificate Data y su Private Key Data correspondiente.
5. Para PKCS #12, seleccionar el archivo y su contraseña; revisar si incorpora certificados CA intermedios.
6. Guardar, comprobar issuer, DN, vigencia y disponibilidad de la clave.
7. Asignarlo al servicio de destino y realizar una prueba de validación TLS o VPN.

Un archivo .crt por sí solo puede bastar para que un cliente verifique confianza, pero un servicio que debe identificarse con el certificado necesita su clave privada correspondiente.

11.10. Procedimiento práctico: trabajar con una CSR

1. En Add/Sign, escoger Create a Certificate Signing Request cuando la firma vaya a realizarla otra CA.
2. Definir el sujeto, las identidades alternativas y la finalidad adecuada al servicio.
3. Crear la CSR y exportar el archivo de solicitud; conservar la clave privada local bajo custodia.
4. Enviar únicamente la CSR al emisor autorizado y esperar el certificado firmado.
5. Importar o asociar el certificado emitido respetando la clave privada que generó la solicitud.
6. Verificar la cadena completa y la coincidencia de la identidad del servicio.

Cuando se dispone de una CA interna con clave privada, Sign a Certificate Signing Request permite firmar CSR propias o importadas. Firmar la solicitud no garantiza por sí solo que la clave privada esté disponible en el dispositivo que usará el certificado.

11.11. Exportar certificados de forma segura

La exportación de certificado público (.crt) puede ser apropiada para distribuir la identidad pública. La exportación de clave privada (.key) y de PKCS #12 (.p12) necesita un control sustancialmente más estricto.

Se necesita…	Archivo habitual	Regla de seguridad
Verificar un certificado público	CRT o PEM	Distribuir solo lo necesario y verificar emisor y huella.
Trasladar una identidad con su clave	P12/PFX protegido	Usar contraseña fuerte y canal autorizado distinto para comunicarla.
Migrar una clave privada por separado	KEY protegido	Limitar permisos, almacenamiento, tiempo de exposición y copias.
Solicitar un certificado a otra CA	CSR / REQ	Nunca adjuntar la clave privada a la solicitud.

En la pantalla de edición existen opciones para exportar claves y paquetes protegidos por contraseña, así como niveles de cifrado del contenedor PKCS #12. Debe preferirse el nivel seguro compatible con los sistemas de destino; los modos débiles se reservan para problemas de interoperabilidad debidamente justificados.

ERROR DE SEGURIDAD Enviar un archivo PKCS #12 que incluye clave privada sin protección, o transmitir su contraseña en el mismo mensaje, expone la identidad criptográfica. No debe utilizarse correo ordinario como método informal para compartir claves.

11.12. Renovación manual, automática y sustitución

El botón Renew/Reissue emite una nueva copia de certificados que pueden renovarse con las credenciales de firma almacenadas localmente. Para certificados emitidos externamente puede ser necesario obtener otro certificado y actualizar sus datos o importar una nueva entrada.

Alternativa	Cuándo es adecuada	Qué hay que prever
Renovación manual	Se necesita reemitir un certificado controlado por CA local.	Posibles reinicios de servicios y distribución a usuarios/clientes.
Auto Renew	Certificados TLS de servidor autofirmados o firmados por una CA interna, con compatibilidad validada.	La GUI indica la renovación automática y debe vigilarse el resultado.
Sustitución externa	El certificado lo emite un tercero o se modifica la autoridad de confianza.	Nuevas cadenas, asignación y validación en los consumidores.
Certificado de usuario/cliente	Se debe renovar una identidad entregada a una persona o dispositivo.	Reexportar, distribuir e instalar la nueva identidad; evitar Auto Renew.

Al reemitir pueden existir opciones como Reuse Key, Reuse Serial y Strict Security. Para certificados de servidor o usuario suele recomendarse un número de serie nuevo. Si una renovación implica generar otra clave, esa clave tendrá que llegar de forma segura al destino final.

Cuando el certificado renovado está asociado a servicios del firewall, pfSense puede reiniciarlos automáticamente. Las renovaciones deben realizarse con una comprobación posterior y, si procede, una ventana de mantenimiento.

11.13. Eliminación frente a revocación

Eliminar una entrada del inventario local no comunica a otros sistemas que un certificado previamente distribuido haya dejado de ser válido. La revocación se gestiona mediante la infraestructura correspondiente, normalmente una lista CRL asociada a la CA o servicios equivalentes de validación.

1. Identificar In Use y otras dependencias que la GUI pudiera no mostrar.
2. Sustituir el certificado en los servicios si se necesita conservar la funcionalidad.

3. Si la clave ha sido comprometida, gestionar también la revocación para evitar su aceptación futura.
4. Confirmar que no existen consumidores dependientes antes de usar la papelera.
5. Eliminar la entrada y verificar servicios, conexiones de clientes y registros.

NO CONFUNDIR «No aparece en la lista» no equivale a «ha quedado revocado». Revocation y el comportamiento del verificador determinan si un tercero podrá rechazar el certificado.

11.14. Diagnóstico: incidencias habituales

Situación	Causa probable	Primera comprobación
Navegador advierte sobre certificado	Certificado autofirmado, CA no confiable, SAN diferente o caducidad.	Comprobar emisor, SAN, periodo válido y cadena.
El certificado no aparece en un servicio	Certificate Type, EKU o ausencia de clave compatible.	Revisar finalidad e inventario de claves.
OpenVPN falla tras renovación	Cliente aún usa certificado/clave antigua o no confía en emisor.	Comparar identidad y material distribuido.
No se puede borrar	La entrada está referenciada por un servicio.	Revisar In Use y dependencias externas.
No aparece Renew/Reissue	No hay CA interna firmante o la entrada no admite el proceso local.	Examinar Issuer y método de emisión.
Archivo P12 no se importa	Contraseña, cifrado no soportado o contenido incorrecto.	Revisar integridad, protección y compatibilidad.
La validación falla con fecha correcta	SAN, EKU, cadena o revocación no cumplen lo que espera el consumidor.	Consultar detalles del certificado y logs del servicio.

11.15. Lista de comprobación y conclusiones

Mantener inventario de certificados con responsable, uso, emisor, vigencia y método de renovación.

No confundir certificado público, CSR, clave privada y contenedor PKCS #12.

Comprobar el tipo y SAN del certificado antes de asignarlo a una VPN o servicio HTTPS.

Revisar periódicamente los avisos de vencimiento y activar los mecanismos de notificación pertinentes.

Utilizar Auto Renew solo en certificados TLS de servidor compatibles.

No depender exclusivamente de In Use para determinar las referencias de paquetes y servicios externos.

Tras cada sustitución, verificar el servicio y sus clientes.

Custodiar las claves y planificar la recuperación antes de renovar o eliminar.

La pantalla Certificates es el inventario operativo de identidades de pfSense Plus. Su administración segura exige combinar lectura de certificados, control de dependencias, protección de claves y procedimientos de renovación verificables.

Referencias técnicas

Netgate — Certificate Management: https://docs.netgate.com/pfsense/en/latest/certificates/certificate.html

Netgate — Certificate Properties: https://docs.netgate.com/pfsense/en/latest/certificates/components.html

Netgate — Renew or Reissue a CA or Certificate: https://docs.netgate.com/pfsense/en/latest/certificates/renew.html

12 System → Certificates → Revocation

Administración de listas de revocación: retirada de confianza, control de acceso VPN, importación y verificación operativa.

Un certificado puede seguir dentro de su período de validez y, sin embargo, dejar de ser confiable antes de caducar. Las listas de revocación o CRL permiten publicar esa decisión para que los servicios que las consultan rechacen certificados afectados.

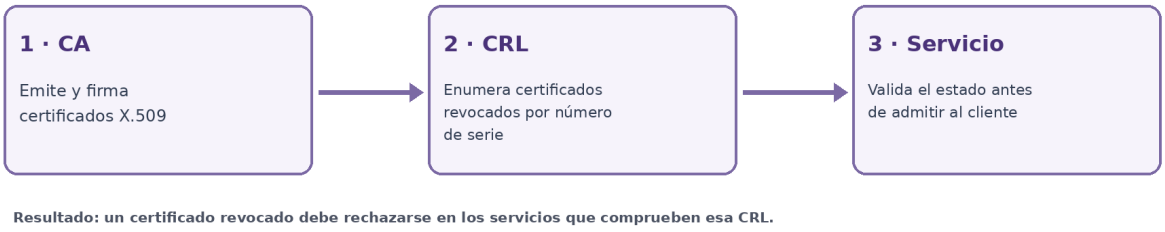


Figura 12.1. Relación entre autoridad certificadora, lista de revocación y comprobación de acceso.

Objetivos del capítulo

Interpretar la pantalla Revocation incluso cuando todavía no existen listas CRL.

Diferenciar una CRL interna de una importada y conocer sus requisitos criptográficos.

Crear, importar, editar, exportar y retirar CRL sin alterar servicios por error.

Revocar certificados por selección o número de serie y reconocer su repercusión en OpenVPN e IPsec.

Comprobar que la revocación se aplica y distinguirla de la desconexión de sesiones ya establecidas.

12.1. Qué es una CRL y para qué sirve

Una Certificate Revocation List (CRL) es una lista X.509 firmada por una autoridad certificadora (CA). Identifica, mediante sus números de serie, los certificados que esa CA ha invalidado antes de su fecha de expiración. Un certificado puede revocarse por pérdida de un dispositivo, filtración de la clave privada, baja de un usuario o sustitución de credenciales.

El certificado y la lista cumplen funciones diferentes: el primero acredita una identidad o un servicio; la segunda informa de que determinados certificados emitidos por una CA ya no deben aceptarse. La verificación de una CRL requiere que el servicio que autentica al cliente efectivamente la utilice.

IDEA CLAVE Crear una CRL vacía no revoca ningún certificado. Tampoco basta con crearla: los servicios pertinentes deben estar configurados para comprobarla.

Elemento	Función	Consecuencia práctica
CA	Firma certificados y, cuando dispone de clave privada, puede firmar CRL.	Es la raíz de confianza que determina a qué certificados afecta la revocación.
Certificado	Identifica un cliente, usuario o servicio mediante X.509.	Puede seguir existiendo en el inventario tras ser revocado.
CRL	Publica números de serie revocados de una CA.	Impide la aceptación donde se consulte esa lista.
Servicio VPN	Valida certificados al autenticar participantes.	Debe usar la CRL relevante para aplicar la revocación.

12.2. Pantalla de administración Revocation

Ruta de acceso: System → Certificates → Revocation. La zona superior contiene tres pestañas: Authorities, Certificates y Revocation. La tercera concentra la consulta de CRL y el acceso a su creación o importación.

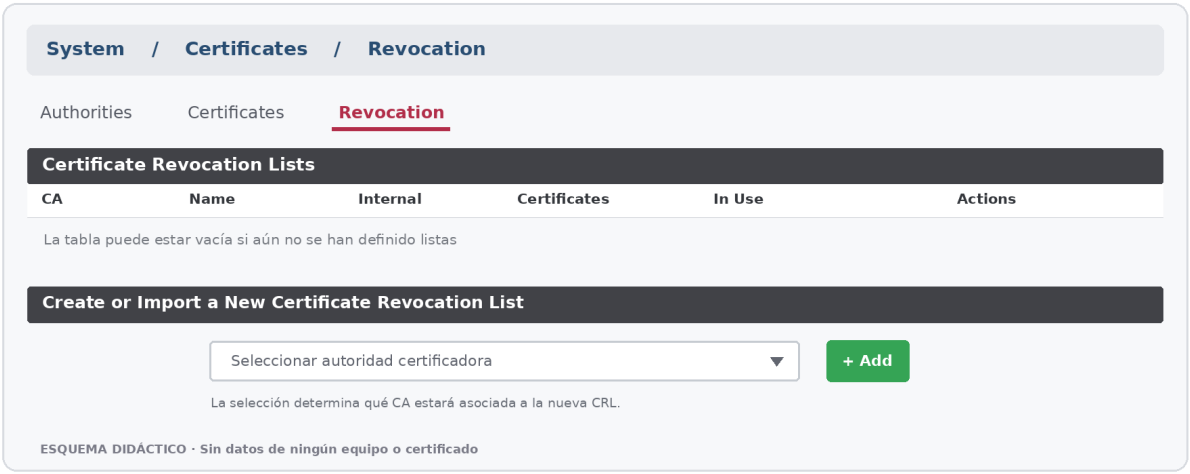


Figura 12.2. Estructura de la pestaña Revocation; representación sin valores de instalación.

La tabla Certificate Revocation Lists

Cuando la tabla está vacía no hay listas CRL registradas en ese inventario. Esta situación no indica por sí sola un error; debe valorarse según la política de revocación utilizada.

Columna	Qué representa	Cómo interpretarla
CA	Autoridad certificadora asociada a cada lista.	Permite identificar el emisor de los certificados susceptibles de revocarse.
Name	Etiqueta descriptiva asignada a la CRL.	Facilita diferenciar listas según su finalidad.
Internal	Indica si la CRL se gestiona internamente o procede de una importación.	Condiciona si se pueden revocar nuevos certificados desde la GUI.
Certificates	Número de certificados incorporados a la lista como revocados.	Es un contador de entradas de revocación, no de certificados activos.
In Use	Identifica usos conocidos de la CRL por servicios.	Ayuda a valorar el impacto de una modificación o eliminación.
Actions	Iconos disponibles para operar sobre cada entrada existente.	Pueden incluir edición, exportación y eliminación según el estado.

Create or Import a New Certificate Revocation List

Bajo la tabla aparece un selector de autoridad certificadora y el botón verde + Add. La elección de la CA determina qué emisor se vinculará a la nueva CRL. Este botón abre un formulario adicional; no revoca certificados de manera inmediata.

Control	Función	Precaución
Selector de CA	Elegir la autoridad a la que pertenecerá la CRL.	La CRL debe corresponder a la CA que emitió los certificados.
+ Add	Abrir el formulario para crear una CRL interna o importar una existente.	El método y los datos se revisan en la pantalla siguiente.
Pestañas superiores	Alternar entre CA, certificados y revocación.	Crear o borrar una CA no es lo mismo que revocar un certificado.

12.3. Crear una CRL interna

Una CRL interna se genera y firma en el propio firewall. Para crearla o agregarle certificados desde la interfaz, pfSense necesita disponer de la clave privada de la autoridad certificadora correspondiente. No debe importarse la clave privada de una CA únicamente por comodidad sin analizar el riesgo de custodia.

1. Entrar en System → Certificates → Revocation.
2. Elegir la autoridad certificadora apropiada en Create or Import a New Certificate Revocation List.

3. Pulsar + Add y seleccionar el método «Create an Internal Certificate Revocation List».
4. Asignar un nombre descriptivo que facilite reconocer su función.
5. Revisar «Lifetime», que determina la vigencia temporal de la CRL.
6. Guardar y comprobar que la nueva CRL aparece en la tabla.
7. Configurar expresamente los servicios que deban consultar la lista antes de considerarla operativa.

El valor predeterminado documentado para Lifetime es 730 días, aunque la CRL se regenera al editarla o cuando se reconfigura un servicio que la utiliza. No es una recomendación universal de renovación; deben considerarse los controles y prácticas de la organización.

VENTAJA Permite gestionar revocaciones desde el mismo firewall y mantener una lista específica para los servicios que lo requieran.

12.4. Importar una CRL externa

Si la CA está gestionada fuera de pfSense y su clave privada no reside en el firewall, la lista se genera y firma en ese sistema externo y posteriormente se importa. Así se evita trasladar la clave de firma al firewall.

1. Seleccionar la CA correspondiente en la pestaña Revocation y pulsar + Add.
2. Elegir el método «Import an Existing Certificate Revocation List».
3. Introducir un nombre descriptivo y pegar el contenido completo de la lista en «CRL Data».
4. Guardar y verificar que la lista se muestra como importada.
5. Revisar su uso real por los servicios VPN y el procedimiento de actualización periódica.

El texto importado suele estar en formato PEM e incluye las marcas BEGIN X509 CRL y END X509 CRL. No es necesario incluir en el libro datos de certificados ni bloques criptográficos reales.

DIFERENCIA OPERATIVA No se pueden añadir directamente nuevos certificados revocados a una CRL importada desde pfSense. La CA externa debe publicar una lista actualizada y el administrador debe sustituir «CRL Data» en la entrada importada.

12.5. Acciones disponibles sobre una CRL

Cuando ya hay CRL registradas, la columna Actions habilita operaciones según el tipo y el uso de la entrada.

Acción	Qué hace	Cuándo conviene utilizarla
Editar (lápiz)	Abre el contenido de la CRL para añadir o retirar revocaciones internas, o actualizar los datos importados.	Cambios de credenciales o actualización desde una CA externa.
Exportar (descarga)	Descarga el archivo de lista de revocación, habitualmente con extensión .crl.	Distribuir una CRL a un sistema externo que deba verificar certificados.
Eliminar (papelera)	Retira una CRL del gestor cuando no está en uso.	Limpieza administrativa después de comprobar dependencias.

Antes de eliminar debe consultarse la columna In Use y comprobar también referencias en paquetes o servicios que no siempre aparecen ahí. La interfaz normalmente oculta la papelera cuando la CRL está en uso.

12.6. Revocar un certificado desde una CRL interna

1. Localizar la CRL interna en la tabla y pulsar el icono de edición.
2. Elegir el motivo de revocación en «Reason». Su valor describe la causa, pero no modifica por sí mismo la validez técnica.
3. En «Revoke Certificates», seleccionar uno o varios certificados disponibles; alternativamente, escribir números de serie en «Revoke by Serial», separados por espacios.
4. Pulsar + Add dentro del editor y confirmar que los certificados figuran en la relación de revocados.

5. Comprobar que la lista está asignada al servicio que debe comprobarla y verificar el rechazo de una nueva conexión con el certificado revocado.

Es posible utilizar la selección de certificados y los números de serie en una misma operación. El número de serie identifica un certificado dentro del ámbito de su CA; una etiqueta descriptiva o un nombre de usuario no son sustitutos fiables.

SEGURIDAD Revocar un certificado no equivale a borrar su entrada del gestor, eliminar un usuario o cerrar de inmediato todas las sesiones establecidas. Son controles diferentes que pueden requerir acciones coordinadas.

Eliminar una revocación concreta

En el editor de la CRL interna se puede retirar una entrada revocada usando el icono de papelera correspondiente y confirmando la operación. Hacerlo puede devolver la aceptación de ese certificado en servicios que utilizan la lista; exige una autorización explícita y una revisión de la razón original de revocación.

12.7. Aplicación en OpenVPN e IPsec

Servicio	Relación con las CRL	Comprobación recomendada
OpenVPN	Puede elegir la CRL que comprobará cada instancia mediante «Peer Certificate Revocation List».	Revisar que la instancia utiliza la CA y la CRL correspondientes.
IPsec	La documentación indica que IPsec consulta las CRL disponibles sin permitir seleccionar una lista por instancia de la misma forma que OpenVPN.	Verificar los requisitos de validación de certificados del despliegue y el resultado de la autenticación.

Si se emplean varias CRL para una misma CA, OpenVPN puede aplicar una lista diferente en cada instancia. Esta capacidad no debe extrapolarse a IPsec. En sistemas de producción conviene priorizar una política de revocación sencilla y documentada.

Una modificación de la CRL activa puede quedar aplicada a la validación de nuevas autenticaciones, pero no se debe asumir que desconecta automáticamente una sesión VPN ya establecida. La retirada urgente de acceso puede requerir además terminar sesiones, retirar credenciales adicionales o deshabilitar cuentas.

12.8. Comprobaciones prácticas

Caso A. Dispositivo perdido con certificado de cliente

1. Localizar el certificado individual y su CA emisora; comprobar que no se comparte entre varios clientes.
2. Identificar la CRL consultada por el servicio VPN correspondiente.
3. Añadir el certificado o su número de serie a la CRL.
4. Finalizar las sesiones existentes si el incidente exige un corte inmediato y revisar las credenciales complementarias.
5. Intentar una nueva conexión de prueba: el certificado revocado debe ser rechazado donde se use esa CRL.
6. Documentar la incidencia, el momento de la revocación y su verificación.

Caso B. Revocación no surte efecto

1. Comprobar si el certificado está realmente incorporado a la CRL correcta.
2. Confirmar que la CRL corresponde a la CA emisora del certificado.
3. Revisar la configuración del servicio: una CRL creada pero no asignada puede no tener efecto.
4. Comprobar si se está probando una sesión ya abierta o una autenticación nueva.
5. Consultar el registro del servicio y el estado de la CRL (vigencia y datos cargados).

Caso C. Autoridad certificadora externa

1. Solicitar o generar una CRL actualizada desde la autoridad externa.

2. Editar la entrada importada y reemplazar «CRL Data» por el contenido completo y válido.
3. Guardar, comprobar su disponibilidad y verificar una nueva autenticación de prueba.

12.9. Recomendaciones de seguridad

Emitir certificados individuales por usuario o dispositivo cuando el modelo de autenticación lo permita.

Mantener la clave privada de la CA bajo un control estricto; la revocación no resuelve una filtración de esa clave.

Revisar que cada servicio utilice mecanismos de revocación acordes con su configuración.

Establecer una política para bajas, pérdida de dispositivos y sustitución de certificados.

No eliminar una CRL como solución rápida a un fallo de autenticación: puede restaurar accesos no deseados.

Guardar copias de seguridad seguras de la configuración y verificar que los procedimientos de recuperación contemplan la PKI.

Probar la efectividad de la revocación con nuevas autenticaciones y revisar registros, no solo el número que aparece en la tabla.

12.10. Conceptos esenciales

Término	Descripción
CA	Autoridad que emite o firma certificados y, cuando procede, sus listas de revocación.
CRL	Lista firmada de certificados revocados asociados a una CA.
Serie del certificado	Identificador que la CA asigna a un certificado emitido.
Lifetime	Período de vigencia de la CRL.
PEM	Formato textual que puede contener datos X.509 delimitados por cabeceras y pies.
CSR	Solicitud de firma de certificado; no debe confundirse con una lista CRL.
OCSP	Protocolo alternativo/complementario para consultar el estado de revocación según lo admita el servicio.

Fuentes y consulta técnica

Netgate. Certificate Revocation List Management. https://docs.netgate.com/pfsense/en/latest/certificates/crl.html

Netgate. Certificate Management. https://docs.netgate.com/pfsense/en/latest/certificates/index.html

Netgate. Cryptographic Settings (OpenVPN). https://docs.netgate.com/pfsense/en/latest/vpn/openvpn/configure-server-crypto.html

Netgate. OpenVPN Remote Access Configuration Example. https://docs.netgate.com/pfsense/en/latest/recipes/openvpn-ra.html

La posición y disponibilidad de controles puede variar entre versiones de pfSense Plus y según la configuración de certificados y servicios.

13 System → General Setup

Identidad del firewall, resolución DNS, sincronización horaria y comportamiento de la interfaz de administración.

General Setup concentra parámetros básicos con efecto transversal en los servicios del firewall y opciones de presentación que solo afectan a la experiencia de administración. Saber distinguir ambas categorías permite realizar cambios precisos y fáciles de verificar.

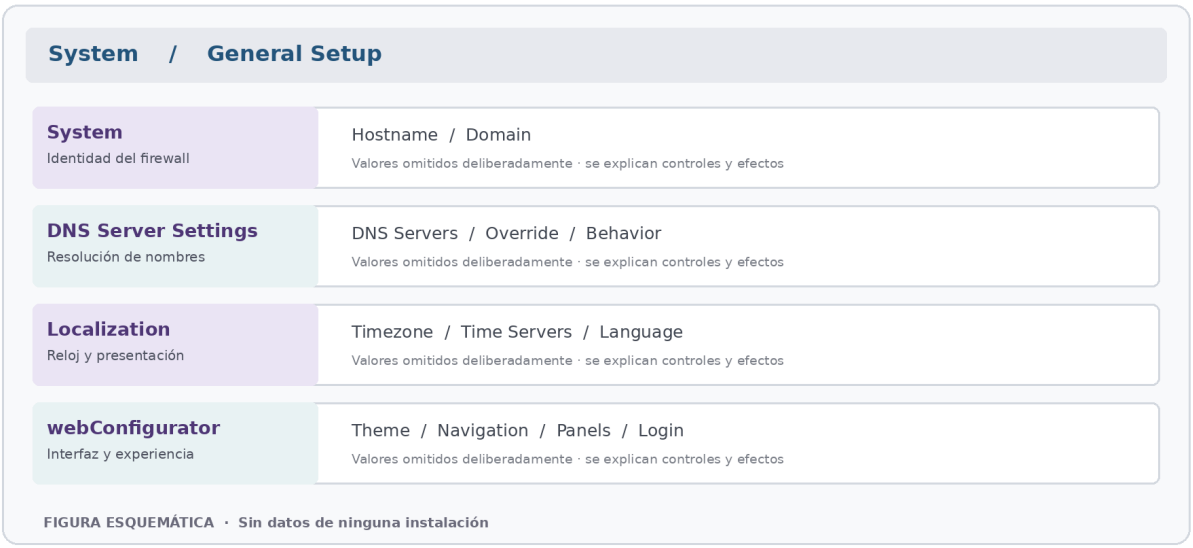


Figura 13.1. Secciones de General Setup. Esquema funcional sin datos de instalación.

Objetivos del capítulo

Configurar el nombre lógico y el dominio del sistema sin confundirlos con el acceso a la WebGUI.

Comprender el uso de DNS local, servidores externos, gateway y DNS Server Override.

Ajustar zona horaria, servidores NTP e idioma y verificar su efecto en registros.

Personalizar el webConfigurator y sus paneles sin alterar las reglas del firewall.

Aplicar un procedimiento de cambio, comprobación y reversión para evitar pérdidas de servicio.

13.1. Acceso y organización de la pantalla

Ruta: System → General Setup. La pantalla contiene los bloques System, DNS Server Settings, Localization y webConfigurator. Los controles se explican por su nombre en inglés, tal como aparecen en la GUI, junto con su función práctica.

CRITERIO EDITORIAL Los campos y funciones son reales; las figuras no incluyen nombres, direcciones, zonas horarias ni valores de ninguna infraestructura.

13.2. System — Identidad lógica

Campo	Qué hace	Ventaja y precaución
Hostname	Define el nombre corto del firewall, sin la parte de dominio.	Identificación en la GUI, servicios y registros. Debe comenzar con letra y usar caracteres admitidos: letras, números o guiones.
Domain	Establece el dominio DNS asociado al firewall.	Junto con Hostname forma su nombre completo (FQDN). Debe pertenecer al esquema de nombres previsto.

La combinación Hostname + Domain construye el FQDN del propio equipo. No crea por sí sola un registro en el DNS corporativo ni cambia automáticamente la dirección de administración. Si se quiere resolver el nombre desde otros dispositivos, debe existir una resolución DNS coherente.

La documentación desaconseja usar el sufijo «.local» para el dominio unicast convencional, porque se utiliza en mDNS por dispositivos y servicios de descubrimiento. Para redes domésticas existe un espacio reservado por estándares, pero cada organización debe elegir su convención de nombres.

ANTES DE CAMBIAR Revisar certificados del webConfigurator, referencias por nombre, monitorización y automatizaciones que puedan depender del hostname o del FQDN.

13.3. DNS Server Settings — Funcionamiento general

Esta sección regula de qué manera el propio firewall puede resolver nombres y qué servidores externos puede consultar. Conviene distinguir el DNS Resolver (Unbound) del DNS Forwarder: en modo recursivo, el Resolver puede consultar directamente servidores autoritativos, sin necesitar una lista de DNS de reenvío; en modo forwarding, consulta servidores ascendentes definidos.



Figura 13.2. Papel del DNS local y externo en las consultas realizadas por el firewall.

Campos de DNS Servers

Control	Función	Uso práctico
Address / DNS Servers	Dirección del servicio DNS al que se puede enviar una consulta.	Añadir resolutores ascendentes cuando la arquitectura requiere forwarding o un recurso de respaldo.
DNS Hostname	Nombre FQDN del servidor DNS para comprobar su identidad mediante TLS.	Importante al emplear DNS over TLS: debe corresponder al certificado del servidor.
Gateway	Ruta de salida asignada a ese DNS; puede seleccionarse un gateway concreto.	En Multi-WAN ayuda a dirigir consultas por la salida prevista.
Add DNS Server	Añade una fila de servidor a la lista.	Permite definir varios resolutores y sus parámetros de forma independiente.
Eliminar servidor	Retira una entrada de DNS de la lista.	Conviene comprobar que no era el único servidor funcional antes de guardarlo.

Que existan servidores escritos en General Setup no significa automáticamente que el DNS Resolver reenviará a ellos. Debe revisarse Services → DNS Resolver → DNS Query Forwarding, así como los ajustes del DHCP que reciben los equipos cliente.

DNS Server Override

Opción: «Allow DNS server list to be overridden by DHCP/PPP on WAN or remote OpenVPN server». Cuando está habilitada, una WAN dinámica o una conexión OpenVPN remota que proporcione DNS puede entregar resolutores que el firewall utilice para sus propios fines. No significa que se entreguen automáticamente esos DNS por DHCP a los equipos de la LAN.

Estado	Comportamiento	Cuándo puede interesar
Activado	Permite incorporar DNS recibidos por WAN/PPP o por OpenVPN remoto, según la configuración.	Redes que aceptan de forma deliberada la resolución aportada por el proveedor.
Desactivado	Evita la sustitución por esas fuentes dinámicas; se mantiene el control administrativo previsto.	Entornos con DNS definidos expresamente o restricciones de resolución.

La opción no controla el modo recursivo del DNS Resolver. Si este resuelve nombres directamente mediante consultas recursivas, la lista de servidores ascendentes no desempeña el mismo papel que en modo forwarding.

DNS Resolution Behavior — Tres políticas posibles

Política	Qué hace	Riesgo o beneficio
Local, con respaldo remoto (predeterminada)	El firewall utiliza primero el servicio DNS local y recurre a DNS externos si el local no está disponible.	Mejora la continuidad, pero puede eludir reglas de privacidad o políticas del DNS local.
Solo DNS local	Utiliza DNS Resolver / Forwarder local sin respaldo externo.	Más control sobre consultas; si el servicio local falla, el firewall puede perder resolución.
Solo DNS remoto	El firewall omite el servicio DNS local y consulta servidores externos.	Útil para separar las necesidades del firewall de las reglas DNS aplicadas a clientes.

IMPORTANTE DNS Resolution Behavior afecta a la resolución del propio firewall. No sustituye la configuración DHCP/DNS de los equipos cliente ni define por sí misma una política de filtrado de sus consultas.

13.4. Localización — Hora, sincronización e idioma

Campo	Significado	Aplicación operativa
Timezone	Zona horaria utilizada para interpretar fecha y hora locales.	Fundamental para auditoría, horarios, avisos, certificados y comparación de registros.
Timeservers	Servidores NTP (nombres o IP) usados para sincronización.	Si se introducen varios nombres se separan por espacios; requieren DNS funcional cuando no son IP.
Language	Idioma de la interfaz web.	Solo cambia las traducciones visibles disponibles; no altera reglas de seguridad ni protocolos.

Usar una zona geográfica real y adecuada evita problemas con los cambios estacionales. Una modificación de Timezone puede necesitar un reinicio para aplicarse por completo en todos los componentes, según la documentación.

Una hora incorrecta dificulta investigar incidencias y puede causar errores aparentes de vigencia de certificados y autenticación. Tras modificar NTP, conviene comprobar sincronización y fuentes horarias en la sección de estado del servicio NTP.

13.5. webConfigurator — Apariencia y navegación

Campo / opción	Qué hace	Ventaja o cuidado
Theme	Selecciona la hoja de estilos visual de la GUI.	Cambio cosmético; no altera funciones del firewall.
Top Navigation	«Scrolls with page» desplaza el menú con el contenido; «Fixed» lo mantiene visible.	Fixed puede ser práctico en pantallas grandes, pero ocupar espacio en dispositivos pequeños.
Hostname in Menu	Permite ocultar, mostrar el nombre corto o mostrar el FQDN en la barra.	Útil si se administran muchos equipos; aumenta la exposición visual de su identidad.
Dashboard Columns	Determina el número de columnas de widgets de la portada.	Adaptar el panel al ancho de pantalla; Netgate documenta hasta cuatro columnas.
Interfaces Sort	Ordena interfaces por descripción en lugar del orden natural de configuración.	Mejora ciertas listas, pero puede resultar inconveniente para comparación de nodos HA.

Associated Panels Show/Hide — Paneles desplegables

Estas casillas determinan qué paneles aparecen abiertos al cargar ciertas páginas. No activan ni desactivan los servicios correspondientes: solo modifican su presentación en la interfaz.

Opción	Dónde afecta	Qué aporta
Available Widgets	Panel de widgets disponibles en Status → Dashboard.	Acceso directo a la personalización de la portada.
Log Filter	Panel de filtrado dentro de Status → System Logs.	Menos clics al investigar registros.
Manage Log	Controles de administración de cada registro.	Más accesible cuando se ajusta con frecuencia el comportamiento visual del log.
Monitoring Settings	Panel de parámetros de gráficos en Status → Monitoring.	Facilita cambiar vistas y métricas de supervisión.

13.6. webConfigurator — Usabilidad y rendimiento

Opción	Comportamiento	Recomendación práctica
Require State Filter	No carga la tabla de estados en Diagnostics → States hasta aplicar un filtro.	Recomendable si hay cientos de miles de estados y la GUI tarda en mostrar la tabla.
Require Firewall Interface	Exige seleccionar una interfaz antes de mostrar su lista de reglas.	Reduce cargas innecesarias en instalaciones con muchas reglas; opción visible en la versión instalada.
Left Column Labels	Pulsar la etiqueta de una fila equivale a accionar su primer control.	Cómodo para algunos administradores, pero puede causar cambios involuntarios.
Alias Popups — Disable details	Muestra únicamente la descripción del alias en su ventana emergente, no toda su composición.	Evita tooltips enormes y mejora legibilidad en listas extensas.
Disable dragging	Impide arrastrar reglas de firewall/NAT con el ratón.	Facilita seleccionar y copiar texto y evita reordenaciones accidentales.

Require State Filter y Require Firewall Interface actúan únicamente sobre la carga de información en la GUI. No modifican la tabla real de estados, no desactivan el filtrado y no alteran el orden de evaluación de las reglas de firewall.

13.7. webConfigurator — Pantalla de acceso

Campo	Función	Riesgo o mejora
Login page color	Escoge el color de fondo o estilo de la pantalla de autenticación.	Permite diferenciar visualmente entornos; no es un control de seguridad.
Login hostname	Muestra el hostname del firewall antes de autenticarse.	Ayuda a identificarlo, pero revela información de inventario a quien llegue al formulario.
Login Message	Texto plano de aviso o advertencia en la pantalla de login.	Sirve para comunicar acceso restringido, políticas o condiciones de uso; no acepta HTML según la pantalla.

El mensaje de acceso debe ser breve, profesional y aprobado por la organización. No debería contener números de teléfono internos, información de red, cuentas administrativas u otras pistas que ayuden a un atacante.

SEGURIDAD Estas opciones no sustituyen las configuraciones de acceso seguro de System → Advanced → Admin Access: HTTPS, certificados, autenticación, anti-lockout y restricciones de acceso se gestionan allí.

13.8. Procedimientos prácticos

Procedimiento A. Modificar la identidad sin romper servicios

1. Anotar el nombre lógico actual y las dependencias que se conectan por FQDN (monitorización, scripts, certificados y DNS).
2. Revisar que el nuevo nombre cumple la sintaxis permitida y la convención de nombres.
3. Editar Hostname y Domain y guardar.
4. Verificar el nombre mostrado en el sistema y la resolución DNS efectiva desde un cliente autorizado.
5. Comprobar si certificados y herramientas externas deben actualizar sus referencias.

Procedimiento B. Comprobar la resolución DNS del firewall

1. Identificar si DNS Resolver actúa de forma recursiva o en modo forwarding.
2. Revisar los servidores de General Setup, sus DNS Hostname y gateways, si se utilizan.
3. Comprobar el estado de DNS Server Override y la política DNS Resolution Behavior.
4. Realizar consultas en Diagnostics → DNS Lookup y comprobar qué origen responde.
5. Si hay anomalías, revisar conectividad, gateways, configuración del DNS local y registros antes de cambiar más parámetros.

Procedimiento C. Preparar DNS para una instalación Multi-WAN

1. Verificar que cada WAN dispone de un gateway y monitorización coherentes.
2. Definir qué servicios DNS externos se utilizarán y qué gateway corresponde a cada uno.
3. Confirmar las rutas hacia esos servicios y la política DNS Resolution Behavior.
4. Probar la resolución con todas las conexiones activas y simular un fallo de una salida en una ventana de mantenimiento.
5. Comprobar si la resolución continúa, qué enlace utiliza y si aparece algún salto a un DNS no previsto.

Procedimiento D. Ajustar fecha, hora y registros

1. Seleccionar la zona horaria geográfica adecuada al despliegue.
2. Revisar los servidores NTP configurados.
3. Guardar y, cuando corresponda, programar un reinicio para aplicar completamente el cambio de zona.
4. Contrastar la fecha del Dashboard y los registros con una referencia horaria fiable.
5. Comprobar el estado de la sincronización NTP y la correlación de eventos.

Procedimiento E. Mejorar la administración de reglas grandes

1. Activar Require State Filter si la tabla de estados tarda en cargarse.
2. Habilitar Require Firewall Interface si la lista de reglas del primer interfaz resulta demasiado grande.
3. Considerar Disable dragging si hay riesgo de reordenaciones accidentales.
4. Ajustar Alias Popups para no mostrar definiciones de alias extensas.
5. Guardar, volver a abrir las pantallas afectadas y comprobar que las reglas y estados reales siguen sin cambios.

13.9. Diagnóstico: síntomas y comprobaciones

Síntoma	Causas a investigar	Primera comprobación
El firewall no resuelve nombres.	Servicio DNS local detenido, gateway sin conectividad, modo local-only o reglas de salida.	Diagnostics → DNS Lookup y estado del Resolver/Forwarder.
Los equipos cliente resuelven distinto.	DNS entregado por DHCP o consultas directas de clientes.	Revisar DHCP y DNS Resolver; General Setup gobierna el DNS del firewall.

Síntoma	Causas a investigar	Primera comprobación
Un DNS por WAN no responde.	Gateway equivocado, salida caída, rutas o políticas de firewall.	Comprobar gateway y ruta efectiva hacia cada DNS.
La hora de los registros no coincide.	Timezone errónea o falta de sincronización NTP.	Comprobar zona horaria y estado del servicio NTP.
Firewall → Rules tarda demasiado.	Gran volumen de reglas y carga de la interfaz.	Activar Require Firewall Interface y revisar rendimiento.
El nombre del firewall no aparece en el menú.	Hostname in Menu ajustado a No hostname.	Revisar el desplegable, no la configuración DNS.

13.10. Buenas prácticas y lista de comprobación

Separar decisiones de conectividad real (identidad, DNS, NTP) de preferencias de presentación (tema y paneles).

Conocer el modo de DNS Resolver antes de interpretar el listado DNS de General Setup.

En Multi-WAN, asociar intencionadamente las consultas DNS a las salidas previstas y comprobar la conmutación.

Considerar las consecuencias de DNS local-only cuando falla el servicio del firewall.

Revisar certificados y servicios dependientes después de modificar nombre o dominio.

No mostrar identificadores internos innecesarios en la pantalla de autenticación.

Guardar una copia de seguridad de configuración antes de cambios de alcance global.

Verificar resultados en la GUI y con herramientas de diagnóstico; no dar por aplicado un cambio solo porque se guardó.

13.11. Términos esenciales

Término	Definición breve
Hostname / FQDN	Nombre corto del sistema / nombre completo que incorpora su dominio.
DNS Resolver	Servicio que puede resolver consultas de forma recursiva o reenviarlas, según su configuración.
DNS Forwarder	Servicio que traslada las consultas a resolutores ascendentes.
DNS over TLS	Consulta DNS transportada mediante TLS, con validación de identidad cuando se configura adecuadamente.
NTP	Protocolo de sincronización horaria para equipos conectados en red.
Multi-WAN	Uso de varias conexiones exteriores, que requiere planificar rutas, gateways y resolución.

Referencias técnicas

Netgate — General Configuration Options: https://docs.netgate.com/pfsense/en/latest/config/general.html

Netgate — DNS Lookup: https://docs.netgate.com/pfsense/en/latest/diagnostics/dns.html

Netgate — Setup Wizard: https://docs.netgate.com/pfsense/en/latest/config/setup-wizard.html

14 System → High Availability

Sincronización de estados, réplica de configuración y continuidad operativa entre dos firewalls.

La alta disponibilidad (HA) evita que la caída de un único firewall suponga necesariamente la interrupción de toda la red. Para ello, pfSense Plus combina funciones diferentes: CARP mantiene las direcciones virtuales disponibles, pfsync replica estados de conexión y XMLRPC copia las áreas de configuración compatibles. El servicio DHCP puede disponer además de un mecanismo propio de HA.



Figura 14.1. Funciones que cooperan en un par de alta disponibilidad. Esquema conceptual sin datos de instalación.

Objetivos del capítulo

Distinguir las funciones de CARP, pfsync, XMLRPC y HA del servicio DHCP.

Comprender todos los campos de System → High Availability sin confundir estados con configuración.

Configurar la sincronización en ambos nodos respetando la dirección correcta de cada mecanismo.

Seleccionar las secciones de XMLRPC de acuerdo con dependencias y riesgos.

Comprobar el funcionamiento y diagnosticar fallos sin introducir cambios irreversibles.

14.1. Ubicación, alcance y requisitos

Ruta: System → High Availability. Esta pantalla contiene dos bloques: State Synchronization Settings (pfsync) y Configuration Synchronization Settings (XMLRPC Sync). En entornos con redundancia de direcciones se configuran, además, las direcciones virtuales CARP desde el apartado correspondiente de Firewall.

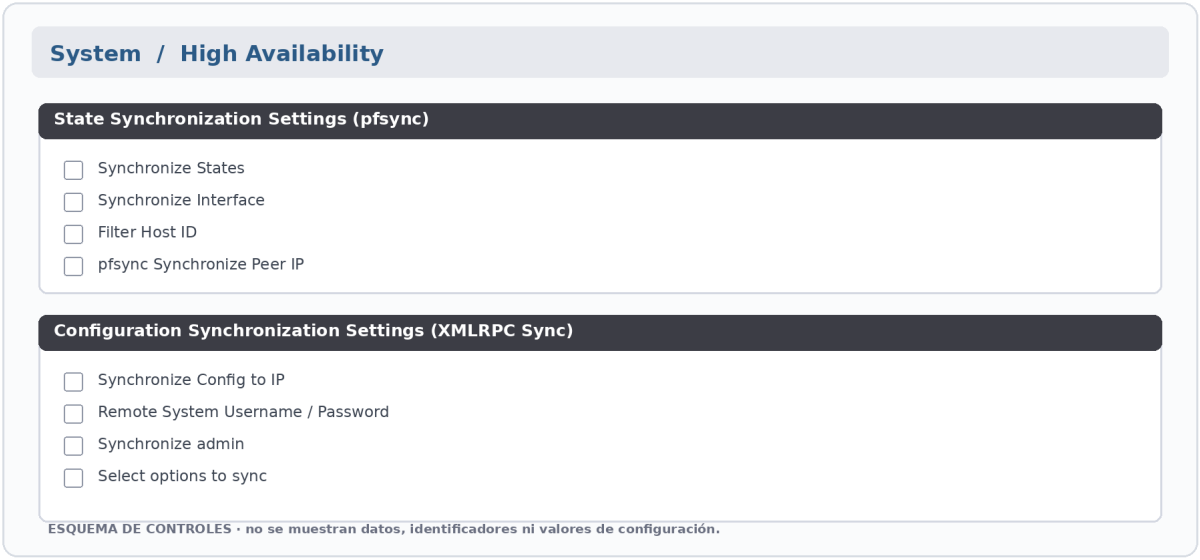


Figura 14.2. Organización de los controles visibles en High Availability, sin mostrar valores.

DISEÑO SOPORTADO La topología HA oficialmente soportada por Netgate utiliza dos nodos. Este capítulo describe el modelo habitual activo/pasivo, no una arquitectura con reparto simultáneo de todas las sesiones.

Mecanismo	Qué replica o mantiene	Dónde actúa
CARP	Direcciones IP virtuales y anuncios de disponibilidad entre nodos.	En las interfaces que albergan cada IP virtual; no en el enlace Sync.
pfsync	Altas, actualizaciones y bajas de estados del filtro PF.	A través de la interfaz de sincronización, en ambos sentidos.
XMLRPC	Secciones compatibles de configuración.	Desde el nodo principal al secundario, a través de la administración web.
Kea DHCP HA	Estado de servicio y cesiones de DHCP entre pares.	Mecanismo específico de Kea, distinto de pfsync y XMLRPC.

Requisitos previos recomendados: versión de pfSense Plus compatible en ambos equipos, interfaces asignadas en el mismo orden, conectividad entre pares, sincronización horaria, copia de seguridad reciente y un enlace específico protegido para tráfico de sincronización.

PUNTO CRÍTICO La interfaz de sincronización debe estar aislada. pfsync no incorpora autenticación: permitir acceso a usuarios o equipos no confiables permite manipular o introducir estados en el firewall.

14.2. State Synchronization Settings (pfsync)

Este bloque configura el intercambio de información dinámica sobre las conexiones que PF mantiene en la tabla de estados. El objetivo es que, si cambia el nodo activo, el secundario conozca las conexiones previamente establecidas y muchas puedan continuar sin reiniciarse.

Opción de pantalla	Qué hace	Ventaja y precaución
Synchronize States	Activa el envío y recepción de mensajes de inserción, actualización y eliminación de estados.	Se habilita en los dos nodos; no sustituye CARP ni copia reglas de firewall.
Synchronize Interface	Selecciona la interfaz por la que circula pfsync. Debe tener una dirección IP asignada.	Preferir enlace dedicado o VLAN aislada y evitar redes de usuario.
Filter Host ID	Identifica qué nodo originó un estado mediante un identificador hexadecimal PF.	Debe ser diferente en cada nodo; máximo ocho caracteres hexadecimales y valor distinto de cero.
pfsync Synchronize Peer IP	Fija el destino de los mensajes de sincronización.	En blanco funciona en multicast; definir el peer permite unicast, habitualmente más fiable en un par.

Cómo viajan los estados

1. Un cliente inicia una comunicación autorizada por las reglas del firewall activo.
2. El filtro PF crea un estado para esa comunicación.
3. pfsync transmite los cambios al otro firewall mediante la interfaz seleccionada.
4. El segundo nodo incorpora esos estados en su propia tabla.
5. Si se produce la conmutación de las IP virtuales, el nuevo activo puede reconocer gran parte del tráfico existente.

pfsync utiliza el protocolo IP 240. No es un puerto TCP ni UDP: la regla de firewall sobre el enlace de sincronización debe permitir específicamente el protocolo pfsync. Si el tráfico no pasa, la conmutación puede funcionar, pero las sesiones previas se interrumpirán.

NO CONFUNDIR El identificador Filter Host ID identifica al creador de estados PF. No es el VHID de CARP, que identifica una dirección virtual, ni es un nombre de host.

14.3. Configuration Synchronization Settings (XMLRPC Sync)

XMLRPC replica secciones seleccionadas de configuración desde el nodo principal al secundario. Esta réplica reduce el trabajo manual y las divergencias entre nodos. Al guardar cambios compatibles en el principal puede enviarse una nueva sincronización.

DIRECCIÓN OBLIGATORIA Configure XMLRPC únicamente en el nodo principal. No defina en el secundario un destino de sincronización hacia el principal: podría producir sobrescrituras inesperadas o un bucle operativo de cambios.

Opción de pantalla	Qué hace	Consideración operativa
Synchronize Config to IP	Indica la dirección de administración del nodo secundario que recibirá XMLRPC.	Usar la dirección del enlace de sincronización del secundario, no una IP virtual CARP.
Remote System Username	Cuenta del secundario usada para autenticar la réplica.	Debe tener permiso System - HA node sync o utilizar el administrador autorizado.
Remote System Password	Contraseña de esa cuenta en el secundario; dispone de confirmación.	Guardar el secreto con seguridad y revisarlo tras cambios de credenciales.
Synchronize admin	Incluye la cuenta admin y puede actualizar la contraseña utilizada por XMLRPC si cambia en la cuenta correspondiente.	Sin activar, cada nodo puede conservar distinta contraseña admin. Evaluar con cautela.
Select options to sync	Casillas para elegir las áreas que se replican.	Solo sincroniza opciones compatibles; no replica automáticamente todo el dispositivo.

Los dos equipos deben ejecutar versiones compatibles y, de acuerdo con la documentación de Netgate, la misma versión para este escenario de sincronización; sus webConfigurator deben compartir protocolo y puerto. La conexión necesita permiso de firewall a ese servicio en la red de Sync. Un desacuerdo en asignaciones de interfaces puede colocar reglas sincronizadas en la interfaz equivocada.

Si se sincronizan usuarios y grupos, la cuenta de sincronización debe existir inicialmente en el secundario antes del primer envío. Conviene crearla también en el principal para evitar inconsistencias durante la primera réplica.

14.4. Select options to sync — Todas las casillas

La lista define qué partes de la configuración se transfieren. No todas las casillas son independientes: sincronizar reglas sin sus aliases, certificados o programaciones puede generar referencias ausentes.

Casilla	Contenido sincronizado	Dependencia o precaución
User manager users and groups	Cuentas y grupos locales del User Manager.	Si las identidades enlazan con certificados, incluir también CA/Cert/CRL.
Authentication servers	Servidores LDAP, RADIUS y sus ajustes de autenticación.	Cuando usen TLS, incluir los certificados y CA necesarios.
Certificate Authorities, Certificates, and Certificate Revocation Lists	Almacén de autoridades, certificados y CRL.	Puede sustituir el almacén del secundario, incluso el certificado usado por su GUI.
Firewall rules	Reglas por interfaz, flotantes, grupos e interfaces VPN.	Requiere mismas asignaciones y, en su caso, aliases y schedules.
Firewall schedules	Calendarios y franjas horarias empleados en reglas.	Activar cuando las reglas hacen referencia a schedules.
Firewall aliases	Alias de redes, hosts, puertos y otros objetos.	Esencial si las reglas o NAT utilizan aliases.
NAT configuration	Redirecciones, outbound NAT y NAT 1:1.	Revisar que las interfaces y direcciones virtuales existen en ambos nodos.

Casilla	Contenido sincronizado	Dependencia o precaución
IPsec configuration	Túneles y parámetros IPsec.	Si hay autenticación con certificados, sincronizar el almacén PKI.
OpenVPN configuration	Servidores y clientes OpenVPN.	Implica sincronización de CA, certificados y CRL según el propio control.
DHCP Server settings	Configuración de servidor DHCP IPv4.	No confundir copia de ajustes con sincronización de concesiones: Kea tiene HA propio.
Casilla	**Contenido sincronizado**	**Dependencia o precaución**
DHCP Relay settings	Parámetros del relay DHCP para IPv4.	Revisar conectividad del destino y estado de los servicios.
DHCPv6 Server settings	DHCPv6 y anuncios RA cuando proceda.	HA para DHCPv6 requiere Kea; ISC DHCPv6 no ofrece el mismo failover.
DHCPv6 Relay settings	Parámetros de relay de DHCPv6.	Revisar rutas IPv6 y enlaces correspondientes.
WoL Server settings	Configuración de Wake on LAN.	Útil para mantener operaciones equivalentes entre nodos.
Static Route configuration	Rutas estáticas y gateways asociados.	Validar que el entorno de interfaces y salida coincide correctamente.
Virtual IPs	Direcciones virtuales compatibles con sincronización.	El comportamiento depende del tipo de VIP; no todas se copian igual.
Traffic Shaper configuration	Configuración de ALTQ Traffic Shaper.	Necesaria si las reglas aluden a colas ALTQ.
Traffic Shaper Limiters configuration	Limiters de tráfico.	Necesaria si las reglas aplican limitadores.
DNS Forwarder and DNS Resolver configurations	Configuración de los servicios de resolución y reenvío DNS.	Distinguir parámetros de servicio de valores de IP por nodo.
Captive Portal	Parámetros del portal cautivo y ciertos datos de uso.	El portal tiene intercambios complementarios específicos de sesiones y vouchers.

CERTIFICADOS La sincronización de certificados puede sobrescribir el certificado webGUI del secundario. Si se renueva un certificado, algunos servicios que lo utilizan en el secundario necesitan reiniciarse manualmente para cargarlo.

14.5. Qué NO debe suponerse que sincroniza XMLRPC

La lista anterior no equivale a replicar la configuración completa del sistema. Habitualmente no se copian las asignaciones de interfaces ni ajustes específicos del hardware, ni todos los apartados de System → General Setup o System → Advanced. Muchos paquetes tampoco se sincronizan automáticamente, aunque algunos ofrecen mecanismos propios.

Elemento	Qué hacer en cada nodo
Interfaces y orden de asignación	Definir y comparar manualmente el mismo orden y los mismos identificadores internos.
Dirección propia de administración	Asignar individualmente la dirección de cada nodo, distinta de las IP virtuales.
Certificado propio de la GUI	Revisar después de activar sincronización de PKI y volver a seleccionarlo si procede.
Paquetes no soportados por XMLRPC	Consultar el mecanismo HA específico de cada paquete y verificarlo.

Elemento	Qué hacer en cada nodo
Ajustes de hardware, plataforma o red especiales	Auditar manualmente las diferencias legítimas entre nodos.
Cesiones DHCP y salud de Kea HA	Configurar y verificar la alta disponibilidad propia del servidor DHCP.

14.6. Procedimiento práctico: preparar una pareja HA

1. Realizar copia de seguridad y verificar una vía de recuperación administrativa para ambos nodos.
2. Confirmar que la versión de pfSense Plus es compatible, que existen recursos suficientes y que los puertos e interfaces están correctamente asignados.
3. Verificar la igualdad del orden interno de interfaces en ambos equipos antes de sincronizar reglas.
4. Preparar un enlace físico o VLAN aislada para Sync, con conectividad IP entre los dos nodos.
5. Permitir en esa red únicamente el tráfico necesario: protocolo pfsync y conexión al webConfigurator del secundario para XMLRPC, más los servicios HA adicionales que se utilicen.
6. Comprobar la sincronización horaria y el acceso de administración individual de cada nodo.
7. Revisar por separado el diseño de direcciones virtuales CARP y, si se utiliza DHCP, su HA específico.

14.7. Procedimiento: activar pfsync en ambos nodos

1. Abrir System → High Availability en el nodo principal.
2. Activar Synchronize States y seleccionar la interfaz de Sync aislada.
3. Asignar un Filter Host ID único y, para un par, definir como peer la dirección de Sync del secundario.
4. Guardar y repetir las mismas operaciones en el secundario, usando otro Filter Host ID y como peer la dirección de Sync del principal.
5. Comprobar que el tráfico pfsync cruza la interfaz correcta y no es bloqueado.
6. Generar comunicaciones de prueba y consultar la sección State Synchronization Status de Status → CARP para observar identificadores de ambos nodos.

14.8. Procedimiento: configurar XMLRPC solo en el principal

1. En el nodo secundario, crear previamente una cuenta de sincronización con el privilegio System - HA node sync, o verificar la cuenta autorizada prevista.
2. Asegurar que el webConfigurator del secundario escucha con el mismo protocolo y puerto que el principal y que la red Sync permite ese acceso.
3. En el nodo principal, introducir en Synchronize Config to IP la dirección de Sync del secundario.
4. Indicar Remote System Username y Remote System Password sin compartir ni publicar las credenciales.
5. Evaluar con cautela Synchronize admin: dejarlo desactivado si se requiere contraseña admin independiente por nodo.
6. Marcar las secciones de Select options to sync realmente necesarias, incluidas sus dependencias.
7. Guardar y observar el resultado de la sincronización en los registros y en una sección de configuración no crítica del secundario.
8. Confirmar que el secundario NO tiene configurado Synchronize Config to IP hacia el principal.

AVISO DE GUARDADO Al pulsar Save con XMLRPC configurado puede forzarse una nueva sincronización y sobrescribir las secciones seleccionadas del secundario. Revisar las casillas antes de confirmar.

14.9. Verificación controlada de la conmutación

Una configuración HA no debe darse por terminada cuando ambos nodos muestran conectividad: se debe ejecutar una prueba de conmutación planificada, con acceso alternativo y posibilidad de regresar al estado anterior.

1. Comprobar desde Status → CARP que las IP virtuales están en el estado esperado: MASTER en el nodo activo y BACKUP en el secundario.
2. Abrir una sesión de aplicación de prueba y comprobar que figura en la tabla de estados.
3. Comprobar en la información de sincronización que aparecen los Host IDs de ambos nodos.
4. Provocar una transición administrada del rol activo mediante los controles de mantenimiento HA previstos para ello, sin desconectar equipos de forma improvisada.
5. Verificar la toma de control por el nodo secundario y observar si la sesión de prueba continúa, según protocolo y condiciones.
6. Comprobar conectividad, resolución DNS, VPN y servicios DHCP que formen parte del diseño.
7. Restaurar el rol previsto de forma controlada y documentar las incidencias detectadas.

No todas las sesiones se conservan siempre: algunas VPN, servicios sensibles al origen, diferencias de hardware o errores de rutas pueden requerir reconexión. También debe revisarse la compatibilidad de pfsync durante actualizaciones de versión.

14.10. Diagnóstico y resolución de incidencias

Síntoma	Causas probables	Primera comprobación
Las reglas no llegan al secundario.	Credenciales, permisos, puerto o protocolo distinto, bloqueo del tráfico XMLRPC.	Registros de sistema; acceso web entre nodos por Sync.
Reglas sincronizadas en interfaz equivocada.	Orden o identificador de interfaces distinto.	Comparación de asignaciones de ambos nodos.
Falla pfsync y se caen las sesiones al conmutar.	Protocolo 240 bloqueado, interfaz inadecuada o peer erróneo.	Tráfico en Sync y Host IDs de estados.
Ambos nodos asumen MASTER.	Anuncios CARP no llegan, fallo L2 o reglas de seguridad.	Status → CARP, logs, switches y VLAN.
XMLRPC modifica el certificado de la GUI secundaria.	Sincronización del almacén PKI.	Certificado seleccionado por el webConfigurator.
DHCP deja de asignar direcciones tras un fallo.	Kea HA sin configurar, tiempo desajustado o canal de HA caído.	Estado de Kea HA, sincronización NTP y registros DHCP.
Se duplican o pierden VIPs.	Configuración CARP y VHID inconsistente.	Verificar IP virtuales, prioridad y anuncios en ambos nodos.
Una actualización rompe la continuidad.	Cambios de protocolo pfsync o diferencias entre versiones.	Notas oficiales de actualización HA y compatibilidad.

14.11. Seguridad, operación y buenas prácticas

Mantener una red Sync dedicada o aislada; nunca transportar pfsync por una red compartida con equipos no fiables.

Gestionar XMLRPC solo desde el principal; reservar al secundario sus ajustes individuales de hardware y red.

Utilizar HTTPS, credenciales robustas y el privilegio mínimo necesario para la cuenta de sincronización.

Comparar siempre el orden de interfaces: una réplica técnicamente exitosa puede producir reglas incorrectas si no coinciden.

Sincronizar conjuntos coherentes: reglas junto con aliases, schedules, certificados o limiters cuando existan dependencias.

Planificar cómo afecta la replicación de CA/Cert/CRL al certificado webGUI y a las operaciones de renovación.

Comprobar fechas y NTP en ambos nodos, especialmente si se utiliza HA de Kea.

No administrar nodos mediante una IP virtual CARP; acceder por la dirección propia de cada equipo.

Revisar el estado de pfsync y CARP antes y después de cualquier actualización importante.

Conservar copias de configuración de ambos nodos y una prueba documentada de recuperación.

14.12. Términos esenciales

Término	Definición
HA	Diseño que permite mantener el servicio ante el fallo de un componente.
CARP	Mecanismo de redundancia de direcciones IP virtuales entre firewalls.
pfsync	Intercambio de estados de conexión del filtro PF entre nodos.
XMLRPC Sync	Réplica en una dirección de secciones de configuración compatibles.
State table	Conjunto de estados que el firewall utiliza para seguir conexiones.
Filter Host ID	Identificador PF del nodo que creó cada estado.
VIP	Dirección IP virtual que puede mantenerse disponible al cambiar el nodo activo.
Sync interface	Interfaz aislada destinada a la comunicación entre firewalls.
Kea HA	Mecanismo específico de redundancia del servicio DHCP.
Failover	Conmutación al equipo secundario después de una falla o intervención.

Referencias técnicas

Netgate — High Availability Synchronization Settings: https://docs.netgate.com/pfsense/en/latest/highavailability/settings.html

Netgate — State Synchronization (pfsync) Overview: https://docs.netgate.com/pfsense/en/latest/highavailability/pfsync.html

Netgate — XMLRPC Config Sync Overview: https://docs.netgate.com/pfsense/en/latest/highavailability/xmlrpc-sync.html

Netgate — High Availability Configuration Example: https://docs.netgate.com/pfsense/en/latest/recipes/high-availability.html

Netgate — Troubleshooting High Availability: https://docs.netgate.com/pfsense/en/latest/troubleshooting/high-availability.html

Netgate — Kea Settings (High Availability): https://docs.netgate.com/pfsense/en/latest/services/dhcp/kea-settings.html

15 System → Package Manager → Installed Packages

Control de complementos instalados, versiones, dependencias y operaciones seguras de mantenimiento.

pfSense Plus permite ampliar las funciones del firewall mediante paquetes adicionales. La pestaña Installed Packages muestra las extensiones que forman parte de la instalación y ofrece acciones para revisarlas, actualizarlas, reinstalarlas o eliminarlas. Una correcta gestión de paquetes aporta funcionalidad sin comprometer innecesariamente la estabilidad, la seguridad ni la disponibilidad de la red.

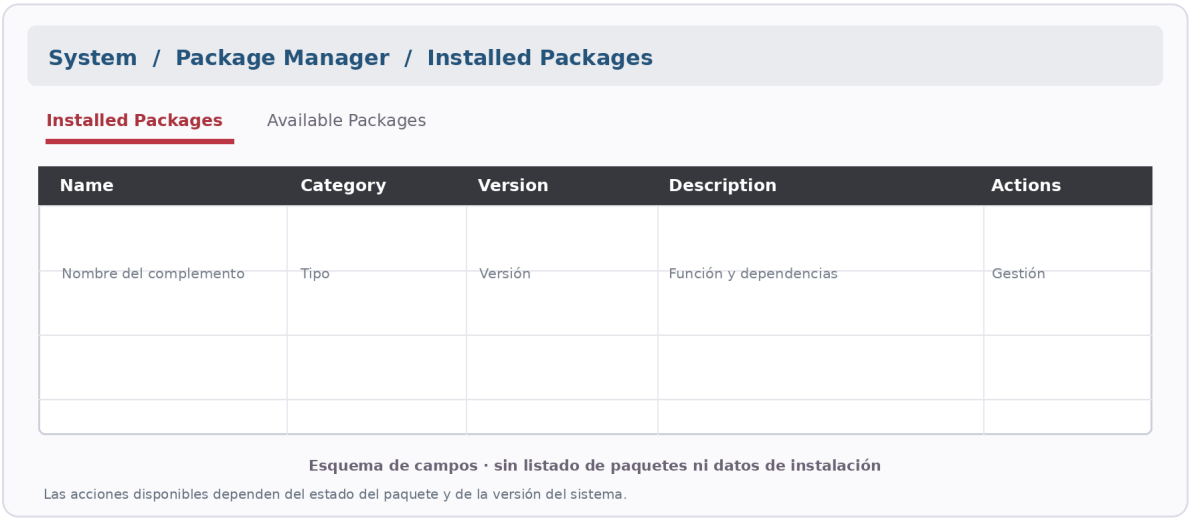


Figura 15.1. Estructura de la pestaña Installed Packages, representada sin inventario, versiones ni otros datos de instalación.

Objetivos del capítulo

Leer e interpretar todas las columnas, enlaces, indicadores y acciones de la lista.

Diferenciar el paquete de pfSense del proyecto o aplicación subyacente.

Conocer los riesgos de las dependencias y las actualizaciones incompatibles.

Aplicar procedimientos para actualizar, reinstalar o eliminar paquetes de forma controlada.

Diagnosticar problemas de repositorios, servicios e instalaciones incompletas.

15.1. Qué es el gestor de paquetes

El gestor de paquetes es el mecanismo por el que pfSense Plus incorpora software complementario disponible para su plataforma y rama de actualización. El catálogo depende de la edición, arquitectura, versión del sistema y repositorio configurado. No todas las funciones del firewall se instalan como paquete: muchas forman parte del sistema base.

Desde el menú System → Package Manager se accede a dos pestañas: Installed Packages y Available Packages. La primera reúne lo instalado; la segunda sirve para descubrir e instalar complementos compatibles. Este capítulo se concentra en el mantenimiento de los existentes.

Área	Qué permite	Diferencia esencial
Installed Packages	Revisar complementos presentes y operar sobre ellos.	No equivale a enumerar todos los componentes internos del sistema operativo.
Available Packages	Consultar el catálogo y añadir funciones.	La disponibilidad depende de la versión y el repositorio.
System → Update	Actualizar la distribución pfSense Plus.	Actualizar el sistema base es un proceso distinto de actualizar un paquete adicional.

Área	Qué permite	Diferencia esencial
REGLA DE MANTENIMIENTO La existencia de una nueva versión de un paquete no autoriza actualizarlo sin comprobar primero la rama de actualización de pfSense Plus y el impacto de los cambios.		

15.2. Estructura de la pantalla Installed Packages

La pestaña muestra una tabla. En una instalación concreta puede haber varias filas, pocas o ninguna. El contenido de las filas cambia con el software instalado; las columnas y sus operaciones son los elementos estables que debe conocer el administrador.

Columna	Qué muestra	Interpretación práctica
Indicador inicial	Símbolo visual asociado al estado del paquete cuando corresponda.	Puede resaltar situaciones que requieren revisión.
Name	Nombre identificador del paquete.	Sirve para localizarlo y relacionarlo con su documentación.
Category	Categoría en el catálogo, por ejemplo red o seguridad.	Clasifica paquetes; no indica por sí sola su criticidad.
Version	Versión del paquete de pfSense, con enlace al historial si está disponible.	Puede diferir de la versión de la aplicación o biblioteca subyacente.
Description	Función del complemento y, cuando procede, sus dependencias.	Ayuda a entender qué incorpora y qué podría verse afectado.
Actions	Acciones permitidas para ese paquete y situación.	Pueden mostrar actualización, reinstalación, eliminación o información.

Name y Category

Name es el nombre de identificación de un complemento en el catálogo. No debe confundirse con el nombre del servicio que este ejecuta, que puede diferir. Category es una clasificación informativa que facilita localizar familias de funcionalidades; no certifica que un paquete sea seguro, necesario o adecuado para cualquier infraestructura.

Version: qué significa realmente

El enlace de la versión puede llevar al historial de cambios del paquete. La numeración no tiene por qué coincidir con la versión de la aplicación que el paquete incorpora: pfSense puede añadir revisiones de empaquetado, integración o correcciones propias. Antes de actualizar es más útil leer el historial y revisar compatibilidad que fijarse únicamente en si el número es mayor.

Description y Package Dependencies

Description explica la finalidad del paquete. Si muestra Package Dependencies, enumera otros paquetes o componentes requeridos para su funcionamiento. Es normal que un complemento dependa de bibliotecas o intérpretes que no se administran manualmente desde la misma tabla. El gestor resuelve estas dependencias dentro del repositorio autorizado, pero un cambio puede afectar a varios componentes.

DEPENDENCIAS No elimine ni fuerce versiones de dependencias por consola como procedimiento rutinario. Una dependencia compartida puede afectar a más de un paquete o al funcionamiento del sistema.

15.3. Símbolos, leyendas y acciones

La leyenda ayuda a interpretar por qué determinados paquetes tienen una acción de actualización o presentan avisos de instalación. Los iconos concretos pueden variar con el tema y la versión. Debe atenderse tanto al dibujo como al texto contextual y a la pantalla de confirmación.

Leyenda o icono	Significado	Qué debe hacer el administrador
Current	El repositorio considera actual la versión instalada para la rama consultada.	No significa que el paquete carezca de vulnerabilidades o que el servicio funcione.

Leyenda o icono	Significado	Qué debe hacer el administrador
Newer version available	El repositorio anuncia una versión más reciente compatible con su catálogo.	Revisar historial, rama del sistema y ventana de mantenimiento.
Configured but not fully installed or deprecated	Existe configuración asociada, pero la instalación puede estar incompleta, ausente o el paquete obsoleto.	Inspeccionar estado y compatibilidad antes de intentar reinstalar o borrar.
Update	Solicita la actualización del paquete, cuando está disponible.	Revisar el alcance y confirmar después de leer las advertencias.
Reinstall	Vuelve a instalar el paquete según las versiones y condiciones del repositorio.	Útil ante archivos o módulos dañados; no asegura resolver problemas de configuración.
Remove	Desinstala el complemento seleccionado.	Verificar dependencias, servicios y qué sucede con la configuración.
Information	Muestra información adicional si el control está presente.	Consultar detalles antes de tomar una decisión.

Los enlaces de Version pueden abrir registros de cambios. No son lo mismo que el botón de actualizar: leer el historial no modifica el equipo. La presencia de las acciones depende del estado y de la disponibilidad de paquetes en el repositorio.

Qué NO significan las leyendas

Current no garantiza que los servicios internos estén iniciados.

Newer version available no significa que una actualización sea urgente ni que no requiera reinicio.

Reinstall no restaura necesariamente una configuración correcta ni sustituye el análisis de registros.

Remove no debe suponerse reversible ni necesariamente elimina todos los datos y ajustes conservados en otras rutas.

Una fila ausente no demuestra que el software del sistema base o las bibliotecas auxiliares no existan.

15.4. Procedimiento: revisar los paquetes sin modificar nada

1. Entrar en System → Package Manager y seleccionar Installed Packages.
2. Comprobar que la tabla termina de cargar y no muestra errores de repositorio.
3. Revisar el estado visual de cada paquete y si existe algún aviso.
4. Abrir, cuando interese, el enlace de Version y leer el historial de cambios.
5. Leer Description y Package Dependencies para comprender el alcance de cada complemento.
6. Identificar qué servicios críticos dependen de los paquetes antes de planificar operaciones.
7. Anotar solo los cambios previstos, sin activar ningún botón de mantenimiento durante la fase de revisión.

Ventaja: permite preparar una ventana de cambios con conocimiento de dependencias, novedades y posibles interrupciones, evitando actuaciones reactivas sobre software que presta servicio a usuarios.

15.5. Procedimiento: actualizar un paquete

Actualizar consiste en sustituir una versión instalada por la versión publicada en el repositorio autorizado para la rama de pfSense Plus que corresponda. Puede modificar el software, sus dependencias, servicios e incluso la presentación de sus opciones de configuración.

1. Confirmar en System → Update qué rama utiliza el firewall y descartar que apunte a una versión futura mientras el equipo sigue en la versión anterior.
2. Consultar las notas del paquete, su historial de cambios y las dependencias.
3. Guardar una copia de seguridad de la configuración y disponer de un mecanismo de recuperación adecuado. Si existe Boot Environment compatible, valorar su uso antes del mantenimiento.
4. Comprobar el estado actual de los servicios y fijar una ventana de mantenimiento según su criticidad.

5. Abrir Installed Packages, localizar la fila y pulsar Update cuando aparezca.
6. Leer la pantalla de confirmación y ejecutarla únicamente si las modificaciones son las previstas.
7. Dejar que el proceso termine sin cerrar el equipo, reiniciar servicios arbitrariamente ni interrumpir la alimentación.
8. Comprobar de nuevo el estado del paquete, sus servicios, registros y las funciones que ofrece. Registrar la actuación.

COMPATIBILIDAD Netgate advierte de que no deben actualizarse paquetes desde un repositorio de una versión de pfSense más nueva que la instalada. Primero hay que corregir la rama o seguir el procedimiento de actualización del sistema.

15.6. Procedimiento: reinstalar un paquete

La reinstalación repone el software de un paquete y puede servir para resolver una instalación incompleta o archivos dañados. No es una herramienta para reparar automáticamente toda incidencia y no sustituye las copias de seguridad ni la revisión de mensajes de error.

1. Revisar la descripción del problema y confirmar que se trata de un componente adicional.
2. Consultar los registros del paquete o del servicio, cuando estén disponibles.
3. Realizar una copia de seguridad y comprobar la rama del repositorio.
4. Seleccionar la acción Reinstall de la fila correspondiente.
5. Leer y confirmar la operación en la pantalla posterior.
6. Esperar a la finalización y revisar dependencias, servicio, configuración y registros.
7. Si persiste el problema, abandonar las reinstalaciones repetitivas y analizar su causa.

15.7. Procedimiento: eliminar un paquete

Desinstalar un paquete es retirar una funcionalidad adicional. Puede liberar recursos o reducir superficie de exposición, pero si presta un servicio activo puede interrumpir accesos, monitorización, proxy, filtrado adicional, VPN u otras funciones.

1. Identificar el servicio que ofrece el paquete y quién depende de él.
2. Verificar si hay reglas, servicios, scripts o integraciones que podrían quedar sin funcionamiento.
3. Exportar o respaldar los parámetros relevantes y la configuración general.
4. Abrir Installed Packages y pulsar Remove en el paquete elegido.
5. Leer la confirmación; cancelar si el alcance o el efecto sobre dependencias no es claro.
6. Confirmar la desinstalación y esperar a que termine.
7. Comprobar que los servicios esperados siguen funcionando y que no quedan referencias rotas; documentar el cambio.

La eliminación de un paquete no debe confundirse con restaurar el sistema a valores de fábrica. El tratamiento de los ajustes y datos asociados depende del paquete, de su desinstalador y de las opciones de copia y restauración.

15.8. Plan mínimo de mantenimiento

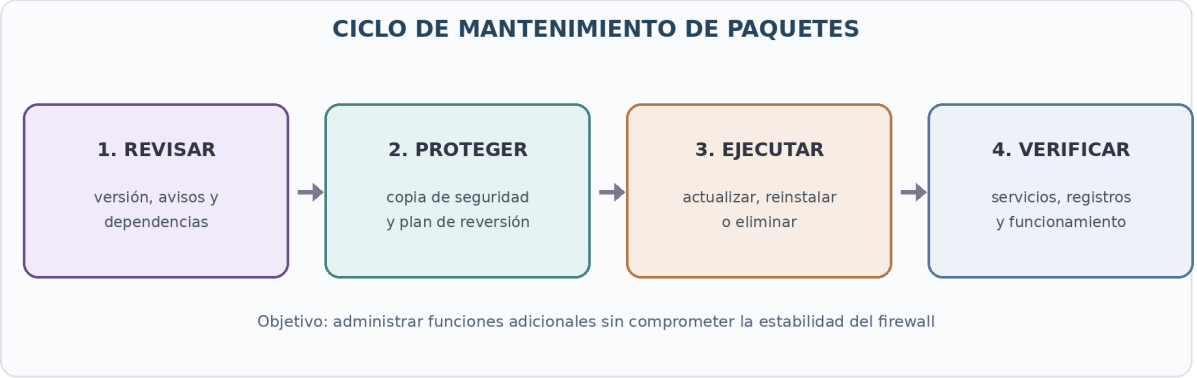


Figura 15.2. Secuencia de mantenimiento: revisar, proteger, ejecutar y verificar.

Antes del cambio	Durante el cambio	Después del cambio
Revisar rama, versión y notas.	Controlar progreso y mensajes.	Verificar lista y servicios.
Copia de seguridad validada.	No interrumpir el proceso.	Revisar registros y conectividad.
Conocer dependencias y usuarios.	Confirmar cambios previstos.	Anotar resultado y reversión.
Prever recuperación y acceso.	Evitar operaciones paralelas.	Comprobar función afectada.

15.9. Escenarios prácticos y diagnóstico

Caso A. El listado tarda mucho en abrirse

La página consulta información del repositorio de Netgate. Antes de atribuir la demora a una instalación dañada, comprobar que el propio firewall tiene conectividad a Internet, resolución DNS, una puerta de enlace válida y que puede llegar al servicio de repositorios. Si existe una incidencia externa en el servicio remoto, repetir la consulta más adelante puede ser razonable.

Caso B. Hay una versión nueva, pero el sistema base también tiene actualización

Revisar la rama configurada y el procedimiento de actualización de pfSense. La prioridad es evitar combinaciones de repositorios incompatibles. Si el sistema está configurado para obtener paquetes de una versión más reciente, no se debe actualizar solo los paquetes antes de actualizar pfSense Plus.

Caso C. Aparece “configured but not fully installed or deprecated”

El aviso puede corresponder a un paquete cuya configuración existe, pero cuya instalación no se ha completado o ya no está disponible de la misma manera. Verificar los registros y la compatibilidad actual. Una reinstalación puede ser adecuada en algunos casos, pero no es una respuesta universal: los paquetes obsoletos requieren evaluar alternativas.

Caso D. Tras actualizar, un servicio no funciona

Examinar el estado del servicio, los errores de configuración, las dependencias y los registros. Confirmar si el paquete ha cambiado requisitos o formato de configuración. No realizar actualizaciones en cadena para “probar suerte”; si el impacto es alto, seguir el plan de reversión preparado.

Caso E. Se necesita reducir el consumo del firewall

Revisar los paquetes realmente necesarios. Cuantos más servicios adicionales se ejecuten, mayor puede ser el consumo de memoria, CPU, almacenamiento y superficie de ataque. Eliminar complementos innecesarios tras evaluar dependencias puede simplificar la operación diaria.

15.10. Buenas prácticas y advertencias de seguridad

Instalar únicamente extensiones justificadas por una necesidad funcional; no ampliar el firewall de forma indiscriminada.

Utilizar los repositorios compatibles suministrados por Netgate. El empleo de repositorios ajenos no está soportado y puede comprometer la instalación.

Evitar cambios en producción sin copia de seguridad, acceso de recuperación y ventana de mantenimiento cuando sea necesaria.

Interpretar correctamente la versión: la del paquete puede ser distinta de la versión del software que encapsula.

No modificar dependencias manualmente ni ejecutar actualizaciones indiscriminadas por consola como mantenimiento rutinario.

Tras cada actualización, probar la función real que ofrece el complemento; el icono Current no prueba que esté operativo.

Proteger las copias de configuración: pueden incluir secretos y datos sensibles.

Mantener inventario interno, responsable del paquete y razón de su instalación, sin publicarlo en documentación distribuida.

15.11. Glosario esencial

Término	Significado
Paquete	Unidad de software adicional publicada para integrarse con pfSense.
Repositorio	Servicio de publicación y distribución del catálogo y sus versiones.
Dependencia	Componente que otro paquete requiere para funcionar.
Changelog	Historial de cambios, correcciones y versiones.
Update / Reinstall	Actualizar versión / reponer instalación del paquete.
Estado Current	Versión actual según los metadatos de repositorio consultados.
Rama de actualización	Canal o versión de pfSense para la que se ofrecen actualizaciones.

15.12. Resumen operativo

Installed Packages es la pantalla central para supervisar y mantener extensiones de pfSense Plus. Permite leer nombres y categorías, reconocer versiones y dependencias y aplicar operaciones controladas de actualización, reinstalación o desinstalación. Un administrador responsable distingue la información del catálogo del estado real de los servicios, valida la compatibilidad de la rama y realiza pruebas tras cualquier modificación.

15.13. Lista de comprobación para el administrador

La siguiente lista puede utilizarse en la preparación y cierre de intervenciones sobre paquetes. No representa el estado de una instalación concreta: es una pauta general de control de cambios.

Comprobación	Antes	Después
La rama del repositorio coincide con la versión del firewall.	Verificar	Revalidar
Existen copia de seguridad y mecanismo de recuperación.	Preparar	Conservar
Se han revisado el changelog y las dependencias.	Revisar	Anotar cambios
Se conoce el servicio que puede interrumpirse.	Evaluar	Probar servicio
La conectividad de administración está garantizada.	Confirmar	Confirmar
El procedimiento se realiza en ventana apropiada.	Planificar	Cerrar ventana
No quedan errores nuevos en registros o paquetes.	Registrar base	Comparar
Se ha comprobado el funcionamiento desde clientes.	Prueba inicial	Prueba final
Se ha documentado el resultado y responsable.	Abrir cambio	Cerrar cambio

Comprobación	Antes	Después
IDEA CLAVE Un paquete debe gestionarse como un componente de producción: conocer su finalidad, dependencias, riesgos y método de recuperación antes de modificarlo.		

Referencias técnicas

Netgate — Package Manager: https://docs.netgate.com/pfsense/en/latest/packages/manager.html
Netgate — Packages: https://docs.netgate.com/pfsense/en/latest/packages/index.html
Netgate — Pre-Upgrade Tasks: https://docs.netgate.com/pfsense/en/latest/install/upgrade-guide-prepare.html
Netgate — Making Backups in the GUI: https://docs.netgate.com/pfsense/en/latest/backup/configuration.html
Netgate — Contact with Netgate Servers: https://docs.netgate.com/pfsense/en/latest/general/netgate-servers.html

16 System → Package Manager → Available Packages

Catálogo de extensiones, búsqueda, instalación segura y selección de herramientas adicionales.

pfSense Plus dispone de un catálogo de paquetes que permite ampliar sus funciones sin incorporarlas todas a la instalación base. Este capítulo explica cómo leer la pantalla Available Packages, qué ocurre al instalar una extensión y cómo valorar cada complemento por su finalidad, sus requisitos y los riesgos que puede introducir.

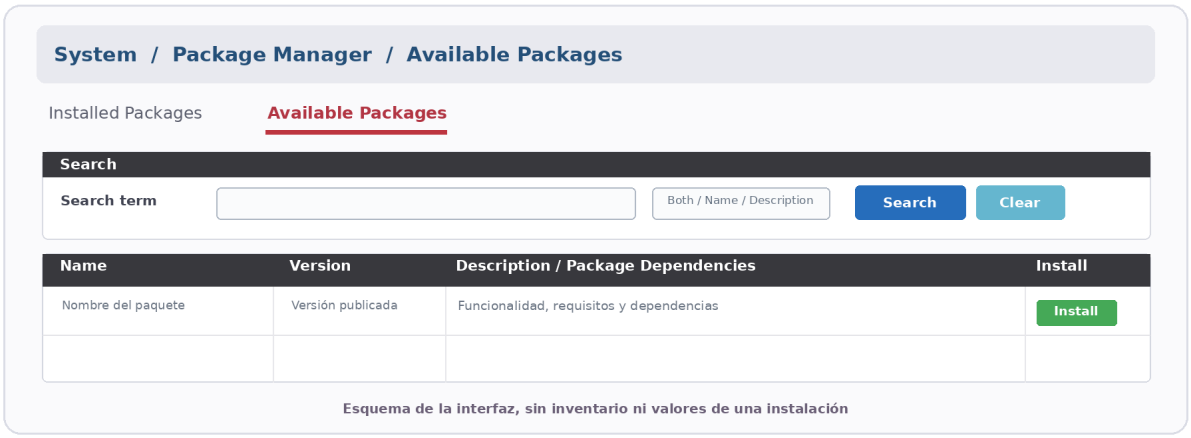


Figura 16.1. Elementos de la pestaña Available Packages: búsqueda, listado, dependencias y acción de instalación.

Objetivos del capítulo

Interpretar los controles Search term, filtro, Search, Clear y la tabla de paquetes.

Instalar una extensión con conocimiento de sus dependencias y permisos.

Identificar los 66 paquetes del catálogo mostrado según su función, sin asociarlos a una instalación.

Distinguir software disponible, software recomendado y software obsoleto.

Realizar verificaciones de servicio y aplicar un plan de recuperación si surge una incidencia.

16.1. Qué muestra Available Packages

La pestaña muestra las extensiones que el repositorio ofrece para la plataforma, la arquitectura y la rama de pfSense Plus. No es una lista de complementos ya instalados. El catálogo puede variar con el paso del tiempo y entre versiones o plataformas; por tanto, la presencia de una extensión no prueba que sea adecuada para cualquier firewall.

REGLA OPERATIVA Instalar solamente lo que resuelve una necesidad concreta. Cada nuevo paquete añade código, mantenimiento potencial y superficie de exposición; la recomendación de Netgate es conservar el mínimo necesario.

16.2. Sección Search: todos sus controles

Control	Qué hace	Utilidad / matiz
Search term	Campo para escribir el nombre, descripción o patrón de búsqueda.	Admite cadenas de texto y expresiones regulares de estilo Unix según la interfaz.
Both	Filtro que busca en nombre y descripción.	Útil si se conoce la función, pero no el paquete.
Name	Limita la búsqueda al nombre del paquete.	Reduce resultados si se conoce parte del nombre.
Description	Busca en la descripción del paquete.	Ayuda a descubrir herramientas por finalidad.
Search	Aplica los criterios introducidos.	Puede reducir de forma notable los resultados.

Control	Qué hace	Utilidad / matiz
Clear	Limpia la búsqueda o restaura el listado sin el filtro anterior.	No desinstala paquetes ni modifica la configuración.

En una búsqueda con expresiones regulares se pueden obtener resultados más amplios o restringidos que con un texto literal. Si no se domina esa sintaxis, conviene empezar por palabras sencillas y comprobar los resultados.

16.3. Sección Packages: columnas y controles

Campo	Explicación	Qué debe comprobarse
Name	Nombre único de la extensión y, cuando procede, enlace a más información.	Que el paquete sea realmente el deseado y no otra variante.
Version	Versión del paquete publicado por pfSense.	No siempre coincide con la versión del proyecto subyacente; enlace a historial de cambios cuando exista.
Description	Descripción de la finalidad, capacidades y dependencias.	Requisitos de memoria, almacenamiento, red, interfaz y seguridad.
Package Dependencies	Otros componentes requeridos para esa extensión.	Que la instalación añadirá más de un paquete y puede afectar recursos.
Install	Solicita la instalación de la extensión.	Requiere confirmar; no significa necesariamente que su servicio quede configurado o arrancado.

Las versiones y las dependencias concretas pertenecen al catálogo vigente y se consultan en la propia interfaz. Para evitar confusiones con inventarios particulares y obsolescencia editorial, este capítulo conserva los nombres públicos de los paquetes, pero no reproduce identificadores de una instalación ni fija números de versión.

16.4. Instalación paso a paso

1. Acceder a System → Package Manager → Available Packages.
2. Comprobar que el catálogo carga y que no muestra errores de conexión o repositorios.
3. Buscar el paquete por nombre o función y revisar su descripción.
4. Abrir el historial de cambios disponible y comprobar compatibilidad con la rama de pfSense Plus.
5. Revisar las dependencias, consumo estimado y cambios de seguridad o de servicio.
6. Guardar una copia de configuración y preparar recuperación y acceso alternativo.
7. Pulsar Install en el paquete seleccionado.
8. Leer la pantalla de confirmación y confirmar solamente si el alcance es el esperado.
9. Esperar a que finalice la instalación sin interrumpir la operación.
10. Comprobar Installed Packages y configurar el servicio desde el menú correspondiente cuando proceda.
11. Verificar procesos, registros, rutas, reglas y la función real para la que se instaló.
12. Registrar el cambio y establecer criterio de mantenimiento y retirada.

IMPORTANTE No confundir «instalado» con «configurado», «habilitado» o «funcionando». Cada paquete puede crear menús, servicios y requisitos específicos. La prueba útil es comprobar la función que el administrador desea obtener.



Figura 16.2. Procedimiento de selección responsable y comprobación posterior a la instalación.

16.5. Catálogo de paquetes: guía práctica de consulta

Las siguientes fichas describen los 66 nombres presentes en el catálogo de referencia de esta pantalla. Se agrupan por propósito para facilitar una selección técnica. Ninguna entrada representa información de paquetes instalados en un firewall concreto. «Precaución» indica aspectos que conviene revisar, no un diagnóstico de una instalación.

16.5.1. Certificados, VPN y cifrado

Paquete	Para qué sirve	Cuándo extremar la precaución
acme	Obtención y renovación automatizada de certificados mediante ACME.	Requiere comprobar desafíos HTTP/DNS y proteger credenciales de proveedores DNS.
openvpn-client-export	Genera configuraciones de cliente OpenVPN listas para distribuir.	Los perfiles exportados pueden incluir certificados, claves y secretos: protegerlos.
openvpn-client-import	Importa un archivo de configuración de cliente OpenVPN.	Verificar certificados, rutas, DNS y legitimidad del archivo importado.
Tailscale	Conectividad de malla VPN basada en WireGuard.	Evaluar identidad, acceso, rutas anunciadas y dependencia del plano de control.
tinc	VPN mallada entre sistemas o redes.	Revisar diseño de rutas, permisos, cifrado y necesidad real frente a opciones nativas.
stunnel	Encapsula conexiones de servicios mediante TLS.	No convierte un protocolo inseguro en servicio bien autenticado por sí solo.

16.5.2. Seguridad, filtrado y observación de ataques

Paquete	Para qué sirve	Cuándo extremar la precaución
ANDwatch	Detecta cambios de asociaciones IP–MAC e información IPv6 ND.	Interpretar cambios legítimos antes de tratar alertas como ataques.
arpwatch	Registra relaciones MAC/IP y sus cambios.	La existencia de un cambio no demuestra suplantación; investigar el contexto.
pfBlockerNG	Administra listas IP, reputación, GeoIP y bloqueo DNSBL.	Puede provocar falsos positivos o bloquear servicios críticos.
pfBlockerNG-devel	Variante de desarrollo de pfBlockerNG en el catálogo.	Comprobar mantenimiento y compatibilidad; elegir una rama, no duplicar sin análisis.
snort	Detección y posible prevención de intrusiones mediante reglas.	Definir interfaces y política; vigilar memoria, almacenamiento y falsos positivos.
suricata	Motor IDS/IPS para inspección y alertas.	Dimensionar recursos y probar reglas antes de bloquear tráfico productivo.
zeek	Análisis pasivo de protocolos y eventos de red.	Genera registros y consume recursos; requiere plan de análisis y retención.

16.5.3. DNS, descubrimiento y multidifusión

Paquete	Para qué sirve	Cuándo extremar la precaución
bind	Servidor DNS BIND con interfaz de gestión.	Diferenciarlo del DNS Resolver nativo y evitar conflictos de puerto/servicio.
Avahi	Descubrimiento mDNS/DNS-SD entre redes compatibles.	Restringir alcance para evitar anunciar servicios entre zonas no deseadas.
mDNS-Bridge	Extiende anuncios mDNS entre segmentos seleccionados.	Controlar difusión y compatibilidad con políticas de segmentación.
mcast-bridge	Reenvía tráfico UDP multicast entre interfaces.	Evitar propagación excesiva y comprobar IGMP/MLD cuando proceda.
udpbroadcastrelay	Reenvía broadcasts UDP a otras interfaces.	Seleccionar interfaces y puertos; puede aumentar exposición lateral.
LADVD	Envía/recibe información de vecinos mediante LLDP/CDP y otros.	Limitar divulgación de topología a enlaces de confianza.
lldpd	Implementa descubrimiento de vecinos LLDP y protocolos relacionados.	Evaluar solapamiento funcional con LADVD; no instalarlos por rutina.

16.5.4. Rutas, servicios de red y plataformas

Paquete	Para qué sirve	Cuándo extremar la precaución
frr	Enrutamiento dinámico con BGP, OSPF y OSPFv3.	Requiere diseño de anuncios, métricas, filtrado y vecinos.
pimd	Enrutamiento multicast mediante PIM.	Solo para redes que necesiten multicast enrutado y estén preparadas para ello.
aws-highavail	Redundancia de pfSense en AWS mediante rutas y direcciones elásticas.	Requiere permisos y arquitectura específicas de AWS.
cellular	Compatibilidad con determinados módems celulares.	Comprobar chipset, controladores, modem y cobertura antes de instalar.
freeradius3	Servidor RADIUS para autenticación y autorización.	Proteger secretos compartidos, credenciales y registros.
siproxd	Proxy SIP que ayuda a escenarios VoIP y NAT.	No activarlo sin evaluar PBX, SIP ALG y rutas de audio RTP.
tftpd	Servidor TFTP, usado en algunas tareas de aprovisionamiento.	TFTP no cifra ni autentica de forma sólida: limitarlo a redes aisladas.

16.5.5. Proxies y distribución de servicios

Paquete	Para qué sirve	Cuándo extremar la precaución
haproxy	Balanceo y proxy TCP/HTTP/HTTPS mediante HAProxy.	Planificar TLS, certificados, comprobaciones de salud y accesos.
haproxy-devel	Variante de desarrollo de HAProxy en el catálogo.	Comprobar diferencias y compatibilidad antes de seleccionar una variante.
FTP_Client_Proxy	Proxy de cliente FTP para determinados escenarios NAT.	FTP presenta riesgos y limitaciones; priorizar protocolos seguros cuando sea posible.
squid	Servidor proxy/cache HTTP y funciones relacionadas.	OBSOLETO según Netgate: no recomendado; revisar retirada y alternativas.
squidGuard	Filtrado de URL vinculado a Squid.	OBSOLETO según Netgate: no recomendado; planificar sustitución.
Lightsquid	Informes y estadísticas del proxy Squid.	OBSOLETO según Netgate: depende de Squid y no se recomienda.

16.5.6. Tráfico, telemetría y observabilidad

Paquete	Para qué sirve	Cuándo extremar la precaución
bandwidthd	Gráficos históricos de tráfico por direcciones IP.	Evaluar privacidad, volumen de datos, recursos y retención.
collectd	Recopila métricas del equipo y puede exportarlas.	Definir destinos, periodicidad y coste del muestreo.
darkstat	Analiza tráfico y ofrece estadísticas accesibles por web.	Aislar y autenticar la consulta; considerar carga y exposición.
ntopng	Análisis detallado de protocolos, hosts y patrones de uso.	Consume memoria/almacenamiento y recopila datos de actividad.
RRD_Summary	Resumen de tráfico a partir de series RRD.	Interpretar cifras según contadores, retención y discontinuidades.
softflowd	Exporta flujos de red en formatos NetFlow/IPFIX.	Proteger colector; no equivale a captura completa de paquetes.
Status_Traffic_Totals	Totales de tráfico por periodos, basados en vnStat.	Diferenciar bytes de interfaz de uso por usuario o aplicación.
net-snmp	Agente SNMP adicional con GUI.	Preferir SNMPv3 y restringir origen/destino; evitar comunidades expuestas.
snmptt	Traduce eventos SNMP Trap para su tratamiento.	Proteger emisores de traps y definir destino/retención.
syslog-ng	Servidor syslog independiente con filtrado y reenvío.	No reemplaza automáticamente al syslog base de pfSense.
Telegraf	Agente para recopilar y enviar métricas a otros sistemas.	Gestionar credenciales, permisos y carga de métricas.

16.5.7. Integración con plataformas de supervisión

Paquete	Para qué sirve	Cuándo extremar la precaución
nrpe	Ejecuta comprobaciones remotas para Nagios.	Restringir clientes y comandos; no exponer a Internet.
zabbix-agent6	Agente para integrar métricas en Zabbix 6.	Escoger la versión compatible con el servidor; proteger canales.
zabbix-agent7	Agente para integrar métricas en Zabbix 7.	Elegir una sola rama necesaria y configurar permisos mínimos.
zabbix-agent74	Agente para la rama Zabbix 7.4.	Verificar versión y compatibilidad con el entorno receptor.
zabbix-proxy6	Proxy de monitorización Zabbix 6.	Planificar almacenamiento, carga, salida y sincronización de datos.
zabbix-proxy7	Proxy de monitorización Zabbix 7.	Adecuar recursos, seguridad y topología de supervisión.
zabbix-proxy74	Proxy de monitorización Zabbix 7.4.	No desplegar proxies por rutina en firewalls con recursos limitados.
mailreport	Envía informes periódicos con logs y resultados.	Evitar incluir datos sensibles en mensajes no protegidos.
Service_Watchdog	Comprueba servicios y puede reiniciarlos si fallan.	El reinicio automático no sustituye investigar la causa del fallo.

16.5.8. Administración, automatización y mantenimiento

Paquete	Para qué sirve	Cuándo extremar la precaución
Backup	Copia y restaura determinados archivos y directorios.	No sustituye la copia de la configuración ni la recuperación completa.

Paquete	Para qué sirve	Cuándo extremar la precaución
Cron	Programa ejecución periódica de tareas.	Evitar tareas pesadas, repetidas o sin supervisión.
Filer	Permite crear o editar determinados archivos desde la GUI.	Riesgo de modificar ficheros críticos; documentar cambios.
Notes	Añade anotaciones administrativas.	No guardar contraseñas, claves privadas ni datos sensibles.
Shellcmd	Define comandos que se ejecutan en el arranque.	Puede romper arranque/seguridad; probar en laboratorio.
System_Patches	Gestiona parches específicos del sistema.	Aplicar solo parches válidos para la versión y registrar reversión.
sudo	Delegación selectiva de privilegios en consola.	Principio de mínimo privilegio y auditoría.

16.5.9. Diagnóstico de conectividad

Paquete	Para qué sirve	Cuándo extremar la precaución
arping	Comprueba respuestas ARP en la red local.	Solo alcanza el dominio L2; no demuestra conectividad IP extremo a extremo.
iperf	Mide capacidad de red entre extremos preparados.	Las pruebas generan tráfico real: programar y limitar.
mtr-nox11	Combina funciones de ping y traceroute en diagnósticos.	Pérdida ICMP en saltos intermedios no prueba fallo final.
nmap	Descubre hosts y servicios mediante sondeos de red.	Usar solo en entornos autorizados; evita escaneos indiscriminados.

16.5.10. Alimentación y continuidad eléctrica

Paquete	Para qué sirve	Cuándo extremar la precaución
apcupsd	Monitoriza y administra ciertos SAI compatibles, especialmente APC.	Comprobar modelo, protocolo de comunicación y cierre ordenado.
nut	Integra distintos SAI mediante Network UPS Tools.	Evaluar drivers, USB/SNMP y política de apagado ante batería baja.

16.6. Paquetes disponibles que no conviene instalar

La disponibilidad en el repositorio no implica recomendación técnica o seguridad suficiente. Netgate advierte expresamente de que Squid, SquidGuard y LightSquid están obsoletos en pfSense Plus y pfSense CE debido a vulnerabilidades conocidas sin corregir en los proyectos de origen. Recomienda retirarlos y señala que dejarán de funcionar en futuras versiones principales.

ADVERTENCIA OFICIAL No recomendar nuevas instalaciones de Squid, SquidGuard o LightSquid. En sistemas donde ya existan, preparar un análisis de dependencias, alternativa compatible y plan de desinstalación.

Otros paquetes requieren revisar la madurez de su rama y su compatibilidad con el sistema: por ejemplo, las variantes con sufijo -devel no deben seleccionarse por interpretar automáticamente que son más recientes o mejores para producción. Los paquetes de monitorización pueden generar mucho tráfico o almacenamiento y los IDS/IPS requieren ajuste fino.

16.7. Selección guiada por necesidad

Necesidad de administración	Herramientas que conviene estudiar	Requisito previo
Renovar certificados HTTPS	acme	Validación de dominio y ciclo de renovación.

Necesidad de administración	Herramientas que conviene estudiar	Requisito previo
Distribuir clientes OpenVPN	openvpn-client-export	PKI y VPN operativas; proteger archivos exportados.
Inspección de tráfico malicioso	snort / suricata / zeek	Objetivos, capacidad, retención y tratamiento de alertas.
Visibilidad de consumo de red	ntopng / bandwidthd / softflowd	Capacidad de recursos y datos que se quieren medir.
Enrutamiento dinámico	frr	Diseño de BGP/OSPF y filtros de anuncios.
Reverse proxy o balanceo	haproxy	TLS, backend, health checks y reglas de acceso.
Supervisión Zabbix	agentes y proxies Zabbix	Versión compatible y arquitectura de la plataforma.
Gestión de SAI	nut / apcupsd	Modelo, conexiones, driver y política de apagado.
Diagnosticar rendimiento	iperf / mtr-nox11 / arping	Permiso de pruebas y ventana de actividad.
Automatizar tareas	Cron / Shellcmd	Impacto del arranque, privilegios y trazabilidad.

16.8. Procedimientos prácticos de administración

Caso A. Instalar una herramienta de diagnóstico

1. Describir la prueba que se pretende realizar y determinar si la herramienta nativa es suficiente.
2. Localizar iperf, arping o mtr-nox11 mediante Search.
3. Revisar compatibilidad y dependencias antes de pulsar Install.
4. Ejecutar una prueba autorizada y registrar resultado, duración y alcance.
5. Mantener el paquete solo si su uso será recurrente; de lo contrario, evaluar su retirada.

Caso B. Instalar un sistema de supervisión

1. Seleccionar un objetivo concreto: métricas, flujos, alertas o informes.
2. Comparar el agente o exportador necesario con los componentes ya disponibles.
3. Evaluar CPU, memoria, disco, destino y protección de credenciales.
4. Instalar el paquete y configurar únicamente los orígenes/destinos autorizados.
5. Comprobar que el servidor receptor recibe datos correctos y que el firewall mantiene su rendimiento.

Caso C. Seleccionar un IDS/IPS

1. Diferenciar detección (IDS) de bloqueo activo (IPS).
2. Calcular las interfaces que se supervisarán y los recursos requeridos.
3. Analizar la política y la procedencia de las firmas utilizadas.
4. Comenzar con observación y revisión de falsos positivos en un entorno controlado.
5. Habilitar bloqueos solo después de comprobar la repercusión sobre servicios legítimos.

Caso D. Necesidad de una funcionalidad que aparece obsoleta

1. Revisar los avisos del fabricante y la fecha de mantenimiento del paquete.
2. Evaluar alternativas de arquitectura o productos mantenidos fuera del firewall.
3. Preparar migración y medidas de continuidad sin instalar software no recomendado.
4. Documentar dependencia, prueba, retirada y validación de funcionalidad.

16.9. Problemas habituales y su diagnóstico

Síntoma	Posible causa	Comprobación recomendada
La pestaña tarda en cargar.	Consulta al repositorio o conectividad deficiente.	DNS del firewall, gateway, HTTPS y estado del repositorio.
No aparece un paquete conocido.	No disponible para la rama/plataforma; filtro activo.	Limpiar búsqueda y contrastar compatibilidad.
Error al instalar.	Dependencia, repositorio, disco o conectividad.	Leer salida detallada y consultar logs, sin forzar pkg manualmente.
Se instaló, pero no funciona.	Configuración o servicio pendiente.	Revisar menú del paquete, Service Status, logs y reglas.
Consumo elevado tras instalar.	Inspección, indexación o métricas intensivas.	Comparar RAM/CPU/disco y frecuencias antes y después.
Problemas tras una actualización.	Rama de repositorios incompatible.	Revisar System → Update y seguir procedimiento oficial.

INTEGRIDAD DEL SISTEMA Netgate no da soporte a paquetes obtenidos de repositorios ajenos configurados manualmente. Pueden causar fallos en instalaciones, actualizaciones o arranque; no deben usarse como vía rápida para obtener una versión concreta.

16.10. Buenas prácticas

Justificar por escrito la instalación de cada paquete y mantener responsable de su mantenimiento.

Revisar la documentación oficial, condiciones de compatibilidad y avisos de obsolescencia.

No instalar varios servicios que compitan por el mismo puerto o la misma función sin diseñarlo previamente.

Evitar repositorios de terceros o procedimientos de instalación ajenos al gestor oficial.

Comprobar la rama de actualización del sistema antes de actualizar software adicional.

Reducir los privilegios, permitir únicamente el tráfico necesario y proteger API keys y credenciales.

Supervisar el efecto de IDS/IPS, analizadores y proxies sobre CPU, RAM, disco y latencia.

Preparar reversión y ventana de cambio si el paquete interviene en el tráfico de producción.

Retirar lo que no aporte valor operativo y comprobar el efecto de la desinstalación.

No conservar en libros o documentación pública un inventario particular de paquetes, direcciones o configuraciones.

16.11. Lista de verificación de instalación

Control	Qué debe revisarse
Necesidad	Existe un objetivo medible y no se duplica una función nativa suficiente.
Fuente	El paquete procede del repositorio compatible de Netgate.
Mantenimiento	No hay avisos de retirada, incompatibilidad o vulnerabilidad no corregida.
Dependencias	Se conocen las bibliotecas y servicios adicionales que instalará.
Recursos	CPU, RAM, almacenamiento y ancho de banda son suficientes.
Seguridad	Credenciales, permisos y puertos quedan restringidos.
Continuidad	Existe copia de configuración y plan de recuperación.
Verificación	Se ha probado la función y revisado logs y rendimiento.
Documentación	Se registra la actuación sin revelar datos en documentación pública.

16.12. Glosario breve

Término	Significado
Catálogo	Relación de paquetes ofrecidos por el repositorio.
Repositorio	Origen controlado desde el que se publica software y metadatos.
Dependencia	Paquete auxiliar necesario para una función.
Rama	Conjunto de versiones compatible con una edición y actualización determinada.
Variante devel	Variante diferenciada de un paquete; requiere comprobar su estatus y compatibilidad.
Obsolescencia	Estado en que un paquete deja de recomendarse o mantenerse.
Servicio	Proceso o función que puede necesitar configuración adicional tras la instalación.

16.13. Resumen operativo

Available Packages es la entrada al catálogo de extensiones de pfSense Plus. Permite localizar software por nombre o descripción y evaluar cada componente por versión, dependencias y finalidad. El trabajo profesional consiste en elegir herramientas justificadas, usar los repositorios compatibles, evitar opciones obsoletas y comprobar el funcionamiento real tras la instalación.

16.14. Fuentes y referencias

Netgate — Package Manager: https://docs.netgate.com/pfsense/en/latest/packages/manager.html
Netgate — Packages: https://docs.netgate.com/pfsense/en/latest/packages/index.html
Netgate — Package List y avisos de obsolescencia: https://docs.netgate.com/pfsense/en/latest/packages/list.html
Netgate — Pre-Upgrade Tasks: https://docs.netgate.com/pfsense/en/latest/install/upgrade-guide-prepare.html
Netgate — Solución de problemas del paquete Squid: https://docs.netgate.com/pfsense/en/latest/troubleshooting/squid.html

17 System → Register

Activación de pfSense Plus, reconocimiento de dispositivos y verificación del estado del registro.

La pantalla Register permite comprobar si una instalación de pfSense Plus necesita activación y, cuando corresponde, introducir el token suministrado por Netgate. No debe confundirse con la pantalla de acceso al firewall, la administración de suscripciones de soporte ni el registro de instancias en Netgate Nexus.

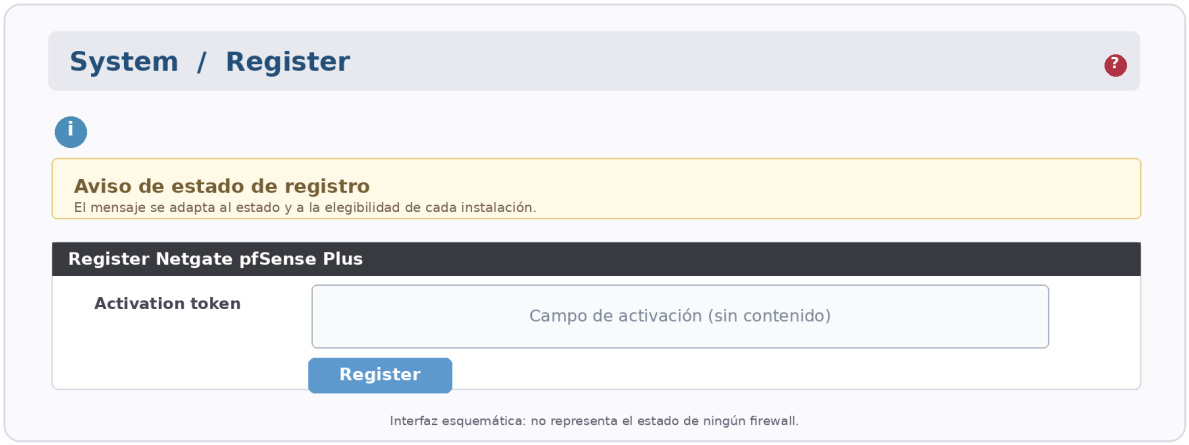


Figura 17.1. Estructura de System → Register: aviso de estado, campo Activation token y acción Register.

Objetivos del capítulo

Identificar cada elemento visible en System → Register y comprender el mensaje de estado.

Distinguir una instalación reconocida automáticamente de otra que precisa un token.

Completar el procedimiento de registro cuando es necesario y verificar el resultado.

Reconocer problemas de conectividad, elegibilidad o token sin comprometer credenciales.

Comprender la diferencia entre activación, suscripción TAC, actualización y Netgate Nexus.

17.1. ¿Qué es System → Register?

Esta sección forma parte de la administración del software pfSense Plus. Netgate la utiliza para activar instalaciones compatibles en determinados equipos físicos o virtuales y para resolver casos específicos de hardware antiguo. La pantalla también permite consultar mensajes sobre el estado de registro o los errores que se producen durante la validación.

Muchos equipos adquiridos a Netgate se reconocen automáticamente y no requieren que el administrador introduzca un token. En cambio, las instalaciones que precisan activación deben utilizar un token legítimo obtenido por los canales oficiales.

IDEA CLAVE La presencia de un cuadro Activation token no significa, por sí sola, que exista un problema de registro. Antes de realizar cualquier cambio hay que leer el mensaje informativo.

17.2. Lectura de la pantalla: controles y funciones

Elemento visible	Función	Interpretación práctica
System / Register	Ruta y encabezado de navegación.	Sitúa la página dentro de la administración del sistema.
Icono de ayuda (?)	Acceso a información contextual.	Consultar el significado de la pantalla o sus controles.
Icono informativo	Señala que hay un mensaje de estado.	No equivale a una incidencia: hay que leer el texto que acompaña al icono.
Banda de estado	Comunica el resultado del reconocimiento, necesidad de registro o posible error.	El contenido cambia con el estado y la disponibilidad del servicio de validación.

Elemento visible	Función	Interpretación práctica
Register Netgate pfSense Plus	Encabezado del formulario de activación.	Identifica la operación permitida por la página.
Activation token	Área para introducir un token oficial de activación.	Debe permanecer sin usar si el equipo no requiere activación.
Register	Envía la solicitud de registro con el token indicado.	No debe utilizarse como prueba general de conectividad ni con tokens improvisados.

17.3. Qué puede indicar el mensaje de registro

El bloque informativo se adapta al resultado de las comprobaciones realizadas por el sistema. Se puede encontrar un aviso que indique reconocimiento automático, una solicitud de activación o una descripción de un error al contactar con el servicio correspondiente. La interpretación depende de la redacción exacta del mensaje y de la plataforma.

Situación	Significado operativo	Actuación recomendada
Registro no requerido	El sistema informa de que la plataforma ya está reconocida o prerregistrada.	No introducir un token; comprobar el estado de soporte en el Dashboard.
Activación pendiente	El sistema necesita asociar un token válido a la instalación.	Obtenerlo por un canal oficial y completar el formulario.
Error de comunicación	La validación no puede completar la comunicación con el servicio remoto.	Revisar conectividad, DNS, hora y políticas de salida antes de reiterar.
Token no aceptado	No se ha completado satisfactoriamente la activación.	Comprobar elegibilidad, procedencia y uso anterior; contactar con Netgate si procede.

IMPORTANTE Un aviso de reconocimiento automático no debe interpretarse como una garantía sobre el nivel concreto de soporte comercial o la vigencia de una suscripción TAC. Esa información debe comprobarse por separado.

17.4. Reconocimiento automático y activación mediante token



Figura 17.2. Secuencia de decisión antes de utilizar la acción Register.

Instalación ya reconocida

Cuando pfSense Plus indica que reconoce el dispositivo y no necesita registrarlo, lo correcto es no modificar el formulario. La comprobación adicional se realiza en el Dashboard, dentro del widget Netgate Services and Support, cuya información ayuda a confirmar el estado de registro y las características de soporte disponibles.

Instalación que necesita activación

Para las instalaciones elegibles que requieren registro, el token de activación lo proporciona Netgate. La documentación oficial describe la generación de tokens mediante la tienda de Netgate; en algunos equipos antiguos puede intervenir Netgate TAC. Los tokens usados para migrar pfSense CE a pfSense Plus son de un solo uso.

SEGURIDAD Tratar el token como credencial. No publicarlo en capturas, documentación, tickets públicos, repositorios de código o conversaciones no autorizadas.

17.5. Procedimiento práctico: comprobar si el sistema requiere registro

1. Iniciar sesión en el webConfigurator mediante una conexión de administración autorizada.
2. Abrir System → Register desde el menú superior.
3. Leer íntegramente el texto del panel informativo antes de tocar ningún campo.
4. Si indica que no hace falta registrar el dispositivo, no introducir ningún valor.
5. Acceder a Status → Dashboard y localizar Netgate Services and Support.
6. Comprobar el estado mostrado sin copiar al informe el NDI, número de serie u otros identificadores.
7. Registrar internamente la conclusión operativa: sin acción, activación necesaria o incidencia de validación.

Resultado esperado: determinar si es necesaria una actuación administrativa sin modificar la configuración de red ni arriesgar un token de activación.

17.6. Procedimiento práctico: registrar una instalación elegible

Este procedimiento únicamente corresponde a sistemas para los que Netgate haya facilitado un token y cuyo estado requiera efectivamente la activación.

1. Comprobar previamente que el firewall dispone de acceso a Internet y que su reloj es correcto.
2. Obtener el token por los canales oficiales de Netgate y conservarlo en un repositorio autorizado de credenciales.
3. Entrar en System → Register y verificar que se encuentra en el firewall previsto.
4. Introducir el token completo en Activation token, sin añadir espacios ni texto adicional.
5. Pulsar Register una única vez y leer la respuesta de la página.
6. Si la operación termina correctamente, comprobar el estado en System → Register y Netgate Services and Support.
7. Si falla, conservar únicamente el código o descripción del error, evitando compartir el token.
8. En caso de dudas de licencia o elegibilidad, abrir una solicitud en el canal privado de Netgate correspondiente.

El procedimiento de registro no debe confundirse con una migración desde Community Edition. En la migración documentada por Netgate existe además una fase posterior en System → Update; no se produce simplemente por escribir un token.

17.7. Comprobaciones y diagnóstico de problemas

Síntoma	Qué revisar	Qué evitar
No aparece el estado esperado	Actualizar la página; revisar Dashboard y conectividad al servicio de registro.	Interpretar un aviso antiguo como estado definitivo.
No conecta con Netgate	Salida HTTPS, resolución DNS, gateway, hora y eventuales proxies o bloqueos.	Desactivar el firewall o abrir reglas indiscriminadas.
El token no funciona	Procedencia, elegibilidad, exactitud del token y si ya ha sido consumido.	Probar tokens ajenos o publicarlos para solicitar ayuda.
Dispositivo Netgate no reconocido	Comprobar datos del equipo en privado y consultar al soporte oficial.	Incluir NDI o número de serie en documentación pública.
Registro correcto, pero falta una función	Confirmar disponibilidad por versión, plataforma, licencia y configuración.	Suponer que Register instala paquetes o cambia ajustes.
La suscripción TAC no coincide con lo esperado	Comprobar por separado las condiciones y estado del servicio de soporte.	Confundir reconocimiento del equipo con todas las modalidades TAC.

17.8. Qué NO hace la pantalla Register

Concepto	Dónde se administra	Diferencia respecto a Register
Acceso de administradores	System → User Manager y Admin Access.	Register no crea cuentas ni modifica permisos de acceso.
Actualización del sistema	System → Update.	La instalación de versiones requiere un flujo de actualización específico.
Paquetes adicionales	System → Package Manager.	Registrar no instala extensiones ni habilita todos los paquetes.
Suscripciones de soporte	Servicios y portal de soporte de Netgate.	Registro y modalidad TAC son conceptos relacionados, pero distintos.
Gestión multinstancia Nexus	System → Advanced → Netgate Nexus.	El alta de una instancia en Nexus es un proceso independiente.
Copia de seguridad	Diagnostics → Backup & Restore o mecanismo disponible.	El registro no sustituye una copia de configuración.

17.9. Casos de uso habituales

Caso A. Dispositivo reconocido automáticamente

Un administrador abre Register después de una instalación o revisión. El sistema comunica que no necesita un proceso de activación. La actuación correcta consiste en confirmar el estado, no introducir tokens y continuar con la administración ordinaria.

Caso B. Instalación elegible pendiente de registro

Una instalación de pfSense Plus requiere asociar una activación oficial. El administrador verifica la conectividad, obtiene el token por el procedimiento adecuado, registra y comprueba la respuesta sin difundir el token.

Caso C. Registro que no puede verificarse

Aparece un error de contacto con el servicio. En lugar de modificar reglas de seguridad indiscriminadamente, se verifica la conectividad de salida y la resolución DNS, se revisa la hora, y se solicita ayuda mediante el canal oficial si el fallo persiste.

17.10. Lista de comprobación del administrador

- ☐ ¿Se ha leído el mensaje de registro completo?
- ☐ ¿Se ha confirmado que el dispositivo requiere realmente un token?
- ☐ ¿Se ha verificado el estado en Netgate Services and Support?
- ☐ Si se registra, ¿el token procede de Netgate y está protegido?
- ☐ ¿Se han evitado capturas con el token, NDI, número de serie o información privada?
- ☐ ¿Se ha comprobado la respuesta antes de repetir la operación?
- ☐ ¿Se han distinguido registro, suscripción, actualización y Nexus?

17.11. Conceptos fundamentales

Término	Definición
Activation token	Código proporcionado por Netgate para activar determinadas instalaciones elegibles.
NDI (Netgate Device ID)	Identificador del dispositivo utilizado en procesos de reconocimiento o soporte; requiere protección.
Prerregistro	Situación en la que el dispositivo ya es reconocido y no requiere completar el formulario.
TAC	Centro de asistencia técnica de Netgate y sus modalidades de soporte.

Término	Definición
Elegibilidad	Condiciones que determinan si una instalación puede utilizar el software o completar una activación.

17.12. Referencias oficiales

Netgate, «pfSense Plus Software Registration»:
https://docs.netgate.com/pfsense/en/latest/config/register.html

Netgate, «Migrate from pfSense CE to Netgate pfSense Plus»:
https://docs.netgate.com/pfsense/en/latest/install/migrate-to-plus.html

Netgate, «How to Sign Up for a TAC Subscription»:
https://docs.netgate.com/pfsense/en/latest/solutions/reference/tac-signup.html

La ubicación de elementos y el contenido de mensajes pueden cambiar entre versiones de pfSense Plus. Contrastar los controles disponibles con la documentación de Netgate y la versión instalada.

18 System → Routing → Gateways

System → Routing → Gateways · Edit Gateway

Configuración de puertas de enlace, selección del camino predeterminado, monitorización y reacción ante fallos.

Una gateway o puerta de enlace es el siguiente salto al que el firewall envía tráfico destinado a redes que no están directamente conectadas. En pfSense Plus las gateways son fundamentales para el acceso a Internet, las rutas estáticas y las arquitecturas con varias WAN. Este capítulo describe la lista principal y su formulario de edición, con especial atención a los efectos de cada opción.



Figura 18.1. Estructura de System → Routing → Gateways. Las filas de configuración se han omitido deliberadamente.

Objetivos del capítulo

Comprender qué representa cada columna, icono y acción de la lista Gateways.

Interpretar las opciones de Default gateway para IPv4 y para IPv6.

Editar un gateway sin confundir la dirección del siguiente salto con la IP de monitorización.

Diferenciar Disable Gateway Monitoring, Disable Gateway Monitoring Action y Mark Gateway as Down.

Comprobar cambios y localizar problemas de conectividad o failover con pruebas seguras.

18.1. Qué es un gateway y por qué importa

En una red IP, el firewall conoce de forma directa las redes conectadas a sus interfaces. Para alcanzar una red externa necesita una ruta y, por lo general, una puerta de enlace. La ruta predeterminada es aquella que se utiliza cuando no existe otra ruta más específica o una decisión de policy routing aplicable.

Una interfaz WAN activa no garantiza que se pueda navegar: el gateway puede ser inalcanzable, la ruta predeterminada puede apuntar a un destino incorrecto o el proveedor puede tener una incidencia más allá de su router. Por ello se distingue entre disponibilidad del enlace, disponibilidad del siguiente salto y calidad del destino de monitorización.

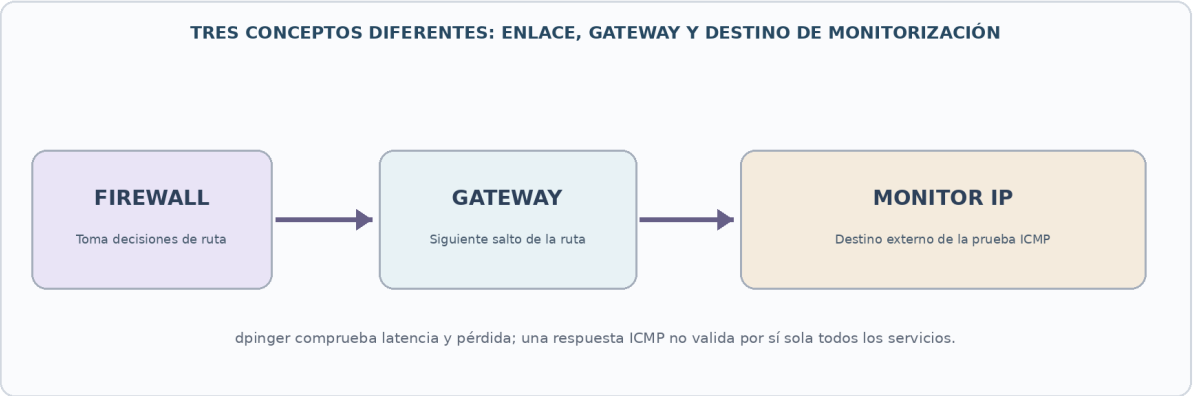


Figura 18.2. Relación conceptual entre firewall, siguiente salto y monitor IP.

IDEA CLAVE Gateway no es sinónimo de interfaz. Un mismo firewall puede definir varias gateways y una gateway puede aparecer operativa aunque una aplicación de Internet siga fallando.

18.2. Estructura de la pantalla Gateways

La sección ofrece tres pestañas: Gateways, Static Routes y Gateway Groups. Aquí se documenta Gateways; las otras dos tienen funciones propias. La tabla reúne entradas estáticas y gateways dinámicos generados a partir de DHCP, PPPoE o determinadas interfaces de túnel.

Elemento	Qué representa	Para qué sirve
Name	Identificador administrativo de la puerta de enlace.	Reconocer la gateway en listas, reglas y grupos.
Default	Marca si la entrada está actuando como ruta predeterminada.	Comprobar cuál es el camino de salida por defecto.
Interface	Interfaz asociada al siguiente salto.	Identificar por dónde se alcanza la gateway.
Gateway	Dirección del siguiente salto; en gateways dinámicas puede indicarse como dinámica.	Comprobar el próximo router o el origen dinámico del dato.
Monitor IP	Destino utilizado por la supervisión de conectividad.	Distinguir el sondeo del siguiente salto real.
Description	Texto libre de identificación administrativa.	Documentar la función de cada entrada.
Actions	Conjunto de operaciones para mantener la entrada.	Editar, clonar, deshabilitar o eliminar cuando proceda.

El indicador circular junto a una entrada ofrece información visual de su situación; para conocer latencia, pérdida y causa de una alarma debe consultarse Status → Gateways. El color o el símbolo aislado no sustituyen una prueba de diagnóstico.

Botones y acciones de la lista

Control	Función	Precaución
Lápiz · Edit	Abrir la configuración de una gateway existente.	Revisar el impacto antes de guardar.
Duplicar · Clone	Crear otra entrada a partir de una existente.	Modificar los campos que deban ser únicos.
Deshabilitar / habilitar	Cambiar la disponibilidad administrativa de la gateway.	Puede cambiar rutas y tráfico.
Papelera · Delete	Eliminar una entrada cuando está permitido.	Revisar referencias en reglas y grupos; una dinámica puede regenerarse.
+ Add	Crear una gateway nueva.	Definir interfaz, familia IP, nombre y siguiente salto.
Save	Guardar la selección de gateways predeterminadas.	Comprobar las rutas y el tráfico después.

Control	Función	Precaución
DETALLE IMPORTANTE Borrar una gateway dinámica no equivale a eliminarla definitivamente: pfSense puede recrearla a partir de la configuración de la interfaz y perder sus ajustes personalizados.		

18.3. Default gateway: salida predeterminada IPv4 e IPv6

La parte inferior de la pantalla incluye controles independientes para Default gateway IPv4 y Default gateway IPv6. Una familia puede funcionar sin ruta predeterminada aunque la otra sí la tenga.

Selección	Comportamiento	Cuándo tiene sentido
Automatic	El firewall selecciona automáticamente una gateway disponible según su lista y orden.	Entornos sencillos; conviene revisar el resultado.
Gateway concreta	Fija el siguiente salto predeterminado elegido.	Cuando se pretende mantener una ruta específica.
Gateway Group	Utiliza el grupo como salida predeterminada y conmuta por tiers.	Failover controlado, una gateway por tier.
None	No inserta ruta predeterminada de esa familia IP.	Escenarios deliberados sin salida por defecto.

En modo Automatic pueden seleccionarse gateways de VPN u otras interfaces que no están pensadas para la salida general a Internet. En redes con Multi-WAN, Netgate recomienda un grupo de gateways con prioridades explícitas cuando se necesita failover predecible. Una Gateway Group seleccionada como predeterminada debe emplearse para failover, no para balanceo de carga con varios miembros en el mismo tier.

La ruta predeterminada afecta al tráfico originado por el propio firewall y al tráfico que no coincide con rutas más específicas ni reglas de policy routing. Las reglas con un gateway o Gateway Group asignado pueden imponer otro camino.

PRECAUCIÓN Cambiar la gateway predeterminada durante una sesión remota puede afectar DNS, conexiones salientes, VPN o el propio acceso de administración. Conservar un método de acceso alternativo y una copia de configuración.

18.4. Edit Gateway: opciones generales

Se accede mediante el icono de lápiz en la fila correspondiente. La pantalla puede cambiar ligeramente según el tipo de gateway y la edición de pfSense. Los campos siguientes son los que aparecen en la interfaz descrita.

Campo	Significado y comportamiento	Recomendación
Disabled	Disable this gateway conserva la definición, pero impide utilizarla.	Útil para aislar temporalmente una ruta; prever consecuencias.
Interface	Indica la interfaz por la que debe alcanzarse el gateway.	Debe ser la interfaz correcta para ese siguiente salto.
Address Family	IPv4 o IPv6; determina el formato y el tipo de rutas admitidas.	No mezclar familias IP.
Name	Identificador usado en la interfaz, reglas y grupos.	Sin espacios; usar letras, números y guion bajo.
Gateway	Dirección IP del siguiente salto.	Normalmente debe estar en la subred de la interfaz.
Description	Comentario de referencia, no interpretado como parámetro.	Describir la finalidad sin información sensible.

La excepción a la regla de subred es una gateway no local configurada con la opción avanzada pertinente. Los enlaces punto a punto también tienen características especiales. En gateways dinámicas ciertos valores provienen del protocolo de conexión y no deben tratarse como si fuesen estáticos.

18.5. Gateway Monitoring y Gateway Action

Disable Gateway Monitoring

Al marcar Disable Gateway Monitoring se desactiva la supervisión automática mediante ICMP. Como consecuencia, pfSense no puede determinar normalmente la caída o degradación de esa gateway a través de dpinger y puede considerarla disponible sin una medición efectiva. No es una forma adecuada de solucionar falsas alarmas en una configuración que debe efectuar failover.

Disable Gateway Monitoring Action

Esta opción mantiene la supervisión, pero evita que los cambios detectados desencadenen acciones como la conmutación automática o el reinicio de servicios dependientes. Es diferente de desactivar la monitorización: pueden seguir existiendo métricas y alarmas, pero el sistema no reaccionará a ellas mediante los mecanismos habituales.

Opción	Sondeos / métricas	Reacción automática al evento
Monitorización activa y acciones habilitadas	Sí: estado, RTT y pérdida.	Sí, según gateways, grupos y reglas configurados.
Disable Gateway Monitoring	No se realiza supervisión habitual del gateway.	No dispone de eventos fiables del monitor para failover.
Disable Gateway Monitoring Action	Sí: sigue supervisando.	No ejecuta acciones de cambio por esos eventos.
Mark Gateway as Down	La gateway se fuerza administrativamente a estado Down.	Puede influir en la elección de caminos alternativos.

RECOMENDACIÓN Cuando una línea funciona pero el monitor reporta fallos, investigar el destino ICMP, las rutas de monitorización y los umbrales antes de desactivar la vigilancia. Para Multi-WAN es esencial monitorizar correctamente.

18.6. Monitor IP y ruta estática de supervisión

Monitor IP

Define el destino al que dpinger envía solicitudes ICMP para medir latencia y pérdida de paquetes. Si no se personaliza, normalmente se utiliza la propia dirección de la gateway. Supervisar únicamente el router inmediato puede dar un falso resultado favorable si el operador ha perdido conectividad aguas arriba.

Conviene elegir un destino estable, accesible por esa WAN y que responda a ICMP. Cada gateway supervisada debe contar con una dirección de monitorización exclusiva. Un resultado Online significa que el destino responde a las sondas: no demuestra que todas las aplicaciones o rutas estén operativas.

Static route: Do not add static route for gateway monitor IP address

De forma predeterminada pfSense crea una ruta específica para llegar al Monitor IP por la gateway seleccionada. Esta casilla inhibe dicha ruta automática. Solo debe activarse si el administrador controla por otro mecanismo la salida de las sondas; de lo contrario, podrían circular por una WAN distinta y ofrecer un diagnóstico engañoso.

Ejemplo conceptual sin direcciones

Si el router del proveedor sigue respondiendo pero no existe salida efectiva a Internet, el firewall puede interpretar que el enlace está Online. Al utilizar un destino externo fiable, la supervisión puede detectar la pérdida de conectividad aguas arriba. La selección debe considerar también si el destino responde a ICMP y si la ruta de comprobación está fijada a la WAN prevista.

18.7. Force State y cierre de estados

Mark Gateway as Down

Fuerza la condición administrativa Down incluso si el destino responde a los sondeos. Puede utilizarse temporalmente para apartar una WAN inestable de una política de failover o de balanceo. No apaga el

puerto físico ni demuestra que la conexión haya desaparecido: cambia cómo pfSense considera la gateway.

State Killing on Gateway Failure

Modo	Efecto	Cuándo evitarlo
Use global behavior	Hereda la política definida en System → Advanced → Miscellaneous.	Si se desconoce la política global.
Do not kill states on gateway failure	No elimina automáticamente estados de esa gateway por este mecanismo.	Cuando se necesita mover conexiones existentes de inmediato.
Kill states using this gateway when it is down	Elimina estados pertinentes de ese gateway al detectarse la caída.	En aplicaciones que no toleran reconexiones.

Este cierre selectivo se aplica a estados originados mediante policy routing y reply-to; no es equivalente a vaciar toda la tabla de estados. Puede no actuar ante determinadas pérdidas de enlace en gateways dinámicas, y carece de efecto si se deshabilitó la monitorización, sus acciones o se forzó manualmente el estado Down.

RIESGO OPERATIVO Eliminar estados interrumpe sesiones establecidas. Los clientes normalmente deben reconectarse por el camino alternativo, por lo que puede haber cortes de aplicaciones, transferencias o túneles.

18.8. Procedimiento práctico: revisar las gateways sin modificar nada

1. Abrir System → Routing → Gateways y reconocer las entradas existentes.
2. Identificar en cada fila Name, Interface, Gateway y Monitor IP, sin copiar estos datos a documentación pública.
3. Comprobar por separado las selecciones Default gateway IPv4 e IPv6.
4. Acceder a Status → Gateways y revisar los estados reales, RTT, pérdida y observaciones.
5. Consultar Diagnostics → Routes para confirmar la ruta predeterminada aplicada.
6. Si existen alarmas, revisar Status → System Logs → Gateways y contrastar con pruebas de diagnóstico.
7. Registrar únicamente el resultado de la revisión y los pasos necesarios, sin incorporar topologías particulares al libro.

Resultado esperado: comprender el recorrido de salida actual y distinguir una gateway configurada de una gateway realmente supervisada y utilizable.

18.9. Procedimiento práctico: corregir una monitorización engañosa

1. Comprobar si el gateway inmediato responde a ICMP aunque no exista salida funcional a Internet.
2. Abrir Edit Gateway y verificar si Disable Gateway Monitoring está desmarcada.
3. Revisar el Monitor IP actual y confirmar que responde de forma estable por la WAN prevista.
4. Seleccionar un destino apropiado a la política de supervisión, evitando destinos utilizados por otra gateway.
5. Dejar activa la ruta de monitorización automática salvo que exista una justificación técnica para gestionarla manualmente.
6. Guardar la configuración y aplicar los cambios cuando la interfaz lo solicite.
7. Verificar Status → Gateways, los logs y la estabilidad de la medición antes de interpretar el resultado.

Resultado esperado: una monitorización que represente mejor la disponibilidad real de la salida prevista, sin cambios indiscriminados de reglas de firewall.

18.10. Procedimiento práctico: preparar un failover controlado

1. Confirmar que existen gateways válidas para las conexiones que van a participar y que cada una se monitoriza de forma fiable.

2. Comprobar que las acciones de monitorización no están deshabilitadas en las gateways participantes.
3. Crear un Gateway Group en la pestaña correspondiente, con prioridad distinta por cada tier si se pretende failover.
4. Revisar si las reglas de Firewall → Rules necesitan policy routing hacia ese grupo para el tráfico de los clientes.
5. Si se desea redundancia de la salida del propio firewall, seleccionar el grupo apropiado como Default gateway de la familia IP correspondiente.
6. Guardar, verificar la tabla de rutas y realizar la prueba de conmutación únicamente en una ventana autorizada.
7. Restablecer el enlace y comprobar el retorno esperado, prestando atención al tratamiento de los estados existentes.

NO CONFUNDIR La gateway predeterminada del firewall y las reglas de policy routing del tráfico LAN son mecanismos relacionados, pero no idénticos. Una configuración de failover correcta exige revisar ambos.

18.11. Problemas habituales y diagnóstico

Síntoma	Posibles causas	Comprobación
Gateway Online, sin Internet	El Monitor IP es el router local; hay un fallo aguas arriba; DNS o rutas fallan.	Diagnóstico de rutas, ping/traceroute y pruebas de servicios.
Gateway Offline, enlace funcional	Destino ICMP no responde; ruta de sonda errónea; umbrales inadecuados.	Probar otro destino y revisar logs de dpinger.
Failover no entra	Monitorización o acciones deshabilitadas; grupo o reglas incorrectos.	Status → Gateways; grupos y reglas policy routing.
Cambió la ruta inesperadamente	Default gateway en Automatic; gateway de VPN seleccionada.	Diagnostics → Routes y ajuste del default.
Sesiones no cambian de línea	Estados existentes no se purgan selectivamente o usan ruta predeterminada.	Revisar política de estados y reglas; evitar borrado global.
Se pierde acceso tras guardar	Cambio de gateway o ruta de retorno; administración a través de WAN/VPN afectada.	Usar acceso local autorizado y restaurar la ruta/configuración.

18.12. Buenas prácticas de administración

Separar las comprobaciones de estado de los cambios de configuración; Status → Gateways no sustituye a Routing → Gateways.

Preferir la monitorización activa cuando una gateway participa en failover o balanceo.

Elegir un Monitor IP que represente el camino útil y no solamente la disponibilidad del router del operador.

No usar Automatic sin revisar qué interfaces o túneles pueden convertirse en gateway predeterminada.

Configurar una gateway por tier para los grupos empleados como salida predeterminada con failover.

Evitar eliminar estados de forma global salvo necesidad justificada y con conocimiento del impacto.

Disponer de copia de configuración y acceso alternativo antes de intervenir en la ruta por la que se administra el firewall.

Documentar el propósito técnico de cada gateway sin dejar direcciones ni detalles internos en publicaciones externas.

18.13. Lista de comprobación

□ ¿Conozco la diferencia entre interfaz, gateway y Monitor IP?

□ ¿He identificado las rutas predeterminadas IPv4 e IPv6?

□ ¿La monitorización está habilitada en las líneas que deben conmutar?

□ ¿El Monitor IP responde de forma estable y por la ruta correcta?

□ ¿No he confundido Disable Gateway Monitoring con Disable Gateway Monitoring Action?

□ ¿He comprobado el impacto de Mark Gateway as Down y de State Killing?

□ ¿Se han validado Status → Gateways, Diagnostics → Routes y los registros?

□ ¿Dispongo de acceso de recuperación antes de modificar gateways en producción?

18.14. Referencias oficiales

Netgate, «Gateways»: https://docs.netgate.com/pfsense/en/latest/routing/gateways.html

Netgate, «Gateway Settings»: https://docs.netgate.com/pfsense/en/latest/routing/gateway-configure.html

Netgate, «Gateway Groups»: https://docs.netgate.com/pfsense/en/latest/routing/gateway-groups.html

Netgate, «Gateway Status»: https://docs.netgate.com/pfsense/en/latest/monitoring/status/gateways.html

Netgate, «Troubleshooting Multi-WAN»: https://docs.netgate.com/pfsense/en/latest/troubleshooting/multi-wan.html

Las denominaciones y la posición de algunos controles pueden variar entre versiones. Las opciones descritas corresponden al contenido de las pantallas tratadas y a la documentación oficial de Netgate.

19 System → Routing → Static Routes

System → Routing → Static Routes · Add / Edit Static Route

Creación, administración y verificación de rutas estáticas de IPv4 e IPv6 en pfSense Plus.

Una ruta estática comunica al firewall qué siguiente salto debe utilizar para llegar a una red concreta. Se utiliza cuando el destino no está directamente conectado y no debe alcanzarse mediante la puerta de enlace predeterminada. Este capítulo explica la pantalla principal y los campos del formulario Add, junto con sus efectos, las precauciones de seguridad y los métodos de comprobación.



Figura 19.1. Estructura de la pantalla Static Routes sin filas de ninguna instalación.

Objetivos del capítulo

Distinguir una ruta estática de la ruta predeterminada y del enrutamiento por políticas.

Interpretar todas las columnas y acciones de Static Routes.

Comprender los campos Destination Network, Gateway, Description y Disabled del formulario Add.

Crear una ruta y confirmar que el cambio se ha aplicado correctamente.

Diagnosticar fallos de conectividad derivados de reglas, retorno, NAT o asimetría.

19.1. ¿Qué es una ruta estática y para qué sirve?

La tabla de enrutamiento determina por dónde sale un paquete según la dirección de destino. Para las redes directamente conectadas, pfSense conoce automáticamente el camino. Para otras redes puede utilizar la ruta predeterminada o una ruta más específica. Una ruta estática define de forma explícita la red de destino y la gateway que lleva hasta ella.



Figura 19.2. Camino de una red remota mediante un router de siguiente salto, sin direcciones ni nombres concretos.

Cuándo aporta valor

Conectar subredes internas ubicadas detrás de otro router, sin modificar la ruta predeterminada.

Definir una ruta específica hacia una infraestructura remota alcanzable mediante una gateway existente.

Mantener trayectos previsibles para determinadas redes o destinos de infraestructura.

Resolver escenarios de VPN en los que el tipo de túnel utiliza gateways y rutas estáticas específicas.

IDEA CLAVE Crear una ruta únicamente determina el camino: no concede acceso por sí misma ni crea reglas de firewall. También deben existir permisos y un camino de retorno.

19.2. Pantalla principal: lista Static Routes

La pestaña Static Routes aparece junto a Gateways y Gateway Groups. Si no existe ninguna ruta configurada, la tabla muestra sus cabeceras sin filas; ello no implica que el firewall carezca de rutas, porque aún puede tener rutas conectadas, automáticas y predeterminadas.

Columna	¿Qué indica?	Lectura práctica
Network	Red o destino para el que existe una ruta explícita.	Comprobar que el prefijo expresa el destino previsto.
Gateway	Nombre de la puerta de enlace que actuará como siguiente salto.	Debe estar definida y resultar alcanzable.
Interface	Interfaz asociada a la gateway utilizada.	Ayuda a identificar por dónde se encamina el tráfico.
Description	Comentario que describe el propósito de la ruta.	Aporta contexto, no modifica el enrutamiento.
Actions	Controles de edición y mantenimiento.	Editar, clonar, activar/desactivar o eliminar según estado.

Controles de la pantalla

Control	Función	Advertencia
Add	Abre el formulario de nueva ruta estática.	Debe existir previamente una gateway compatible.
Edit (lápiz)	Permite modificar una ruta existente.	Cambiar destino o gateway puede alterar comunicaciones.
Clone	Duplica los datos de una ruta para crear otra.	Revisar que no haya solapamientos involuntarios.
Disable / Enable	Inhabilita o vuelve a habilitar una entrada sin borrarla.	El tráfico puede pasar a otra ruta disponible.
Delete	Elimina la definición de una ruta.	Puede dejar destinos remotos sin camino válido.
Apply Changes	Aplica cambios pendientes cuando pfSense muestra el aviso.	No confundir Save con cambio ya aplicado.

19.3. Formulario Add / Edit Static Route

El botón Add abre el formulario de ruta estática. Los mismos conceptos se aplican a Edit, que permite modificar una ruta creada previamente. Los valores concretos dependen del diseño de red; aquí se explica el significado de cada control sin representar ninguna instalación.

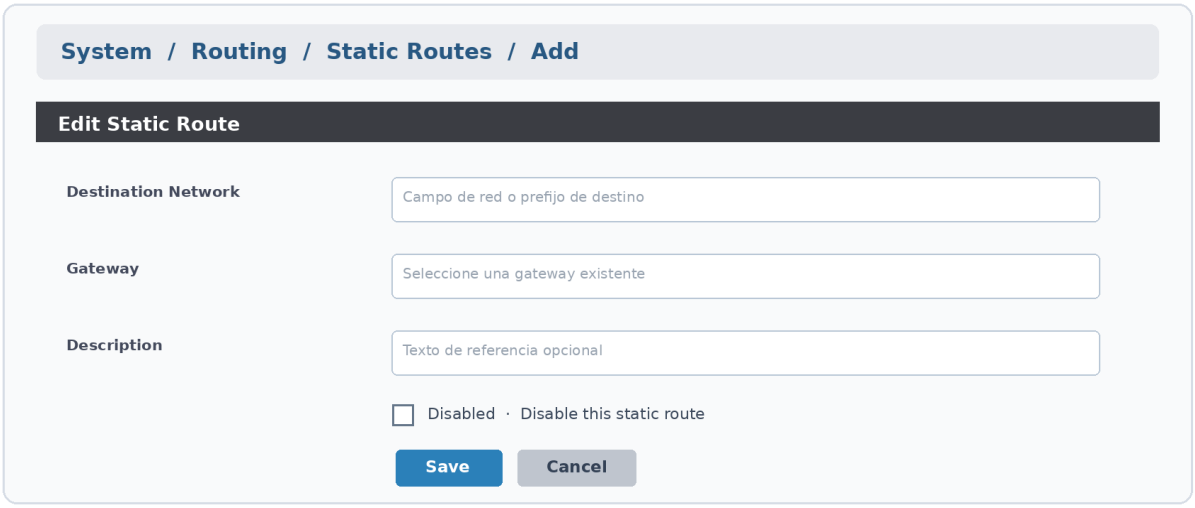


Figura 19.3. Formulario Add recreado como esquema editorial sin datos de red, direcciones ni nombres de gateways.

Destination Network

Es el destino para el que se desea crear la ruta. Puede expresarse como subred IPv4 y su longitud de prefijo, como prefijo IPv6 o mediante un alias admitido por pfSense. No representa la dirección del propio firewall ni la de la gateway. Es importante utilizar el identificador de red correcto y un prefijo ajustado al alcance real deseado.

Una ruta hacia una red completa abarcará todos los hosts comprendidos por ese prefijo. Las rutas a un único host utilizan longitud de prefijo /32 para IPv4 o /128 para IPv6. Un prefijo excesivamente amplio puede desviar tráfico que no estaba previsto.

Gateway

Selecciona el siguiente salto por el que se llega al destino. El desplegable utiliza gateways que ya se encuentran configuradas en System → Routing → Gateways. Si no aparece la gateway correcta, debe crearse primero en esa sección y luego regresar al formulario. La familia de direcciones del destino y de la gateway debe coincidir: IPv4 con IPv4 o IPv6 con IPv6.

No es necesario convertir una interfaz interna en una interfaz de tipo WAN seleccionando una upstream gateway en Interfaces. Para alcanzar subredes detrás de un router interno se puede definir una gateway asociada a la interfaz interna desde System → Routing y emplearla en la ruta estática.

Disabled

La casilla Disable this static route conserva la definición pero impide que se utilice. Resulta útil para preparar una ruta antes de habilitarla, retirar temporalmente un camino o realizar una prueba controlada. No elimina automáticamente conexiones que ya estuvieran establecidas: el comportamiento de las sesiones dependerá de rutas vigentes, reglas y estados.

Description

Texto libre de referencia administrativa. Es recomendable describir el propósito y el alcance funcional de la ruta sin colocar datos confidenciales en documentación distribuida a terceros. No participa en la decisión de enrutamiento.

Save y Apply Changes

Save guarda la definición. Cuando pfSense muestra un banner de cambios pendientes, debe pulsarse Apply Changes para aplicar la configuración al sistema. Cancel abandona el formulario sin guardar. La confirmación de que se ha aplicado una ruta se realiza consultando la tabla de enrutamiento.

Campo	Pregunta que debe responder el administrador	Error habitual
Destination Network	¿Qué red remota exacta quiero alcanzar?	Confundir la red de destino con el IP del siguiente salto.
Gateway	¿Qué router conoce el camino hasta esa red?	Seleccionar una gateway de otra familia IP o no accesible.

Campo	Pregunta que debe responder el administrador	Error habitual
Disabled	¿La ruta debe entrar ya en funcionamiento?	Dejarla deshabilitada y asumir que está en uso.
Description	¿Qué propósito cumple esta definición?	No documentar el motivo de la ruta.

19.4. Procedimiento: alta completa de una ruta

1. Revisar el diagrama y confirmar que el destino no está directamente conectado a una interfaz del firewall.
2. Verificar en System → Routing → Gateways que existe una gateway adecuada y alcanzable para esa familia de direcciones.
3. Abrir System → Routing → Static Routes y pulsar Add.
4. Introducir en Destination Network el destino exacto; utilizar la máscara o longitud de prefijo que corresponda.
5. Seleccionar la gateway de siguiente salto correcta en el control Gateway.
6. Mantener desmarcada la opción Disabled si la ruta debe entrar en servicio al aplicarse.
7. Añadir una Description que explique de manera clara su finalidad y pulsar Save.
8. Pulsar Apply Changes cuando aparezca el aviso, y comprobar en Diagnostics → Routes que existe la entrada esperada.
9. Verificar con pruebas de conectividad y registros que los paquetes llegan y regresan correctamente; revisar también reglas de filtrado y NAT.

Resultado esperado: una ruta activa visible en la tabla del sistema, cuyo siguiente salto corresponde a la gateway elegida. La prueba funcional debe hacerse con el tráfico real necesario, no únicamente mediante ping.

19.5. Verificación tras guardar

Herramienta o vista	Qué se comprueba	Interpretación
Diagnostics → Routes	Destino, máscara, gateway e interfaz aplicados.	La entrada debe coincidir con la definición prevista.
Diagnostics → Ping	Accesibilidad del siguiente salto y del destino, cuando ICMP esté permitido.	La ausencia de ping no demuestra por sí sola fallo de ruta.
Diagnostics → Traceroute	Secuencia de saltos hacia el destino.	Identifica desvíos; los saltos pueden omitir respuestas ICMP.
Diagnostics → Packet Capture	Entrada y salida de paquetes en las interfaces afectadas.	Permite comprobar por dónde circula la solicitud y si vuelve.
Status → System Logs → Firewall	Bloqueos y reglas que coinciden con el tráfico.	Un bloqueo indica problema de política, no necesariamente de ruta.
Reglas y NAT	Permisos en la interfaz de entrada y traducción de direcciones.	En ciertos diseños deben contemplarse las redes remotas en Outbound NAT.

PUNTO DE COMPROBACIÓN Una ruta visible en Diagnostics → Routes demuestra que la entrada existe, no que el destino sea accesible de extremo a extremo. Compruebe gateway, reglas, retorno y servicio final.

19.6. Qué ocurre cuando falta la ruta de retorno

El enrutamiento IP necesita caminos compatibles para el trayecto de ida y de vuelta. Si un host remoto recibe la petición pero responde mediante una gateway que no tiene un camino de regreso hacia la red de origen, la sesión fallará aunque la ruta del firewall esté bien definida. Esta situación es frecuente cuando existe un router interno adicional.

1. Comprobar primero que el firewall tiene la ruta hacia la red remota.
2. Revisar que el router intermedio conoce la red de origen y que su siguiente salto es válido.

3. Verificar que los hosts del destino o su router tienen configurada una ruta de retorno adecuada.
4. Revisar las reglas de firewall de entrada y salida, y las traducciones NAT aplicadas.
5. Utilizar captura de paquetes en ambos extremos cuando no se pueda determinar dónde se pierde la respuesta.

19.7. Rutas estáticas, reglas y enrutamiento asimétrico

Cuando el tráfico entra y sale por la misma interfaz de pfSense para alcanzar una red que está detrás de otro router, el estado de las conexiones puede verse afectado por el enrutamiento asimétrico. Netgate documenta tanto reglas específicas con un manejo apropiado de estados como la opción avanzada Bypass firewall rules for traffic on the same interface.

RIESGO DE SEGURIDAD La opción de bypass puede permitir tráfico que antes estaba sometido a filtrado. No debe activarse como solución genérica ante un fallo de conectividad: primero hay que entender el recorrido, las reglas y los estados de cada flujo.

También pueden intervenir los mensajes ICMP Redirect cuando un router identifica un camino más directo hacia otra subred. Su presencia en capturas o registros exige revisar el diseño y no sólo añadir rutas en el firewall.

19.8. Rutas y aliases: una consideración importante

pfSense permite utilizar determinados aliases como destino de una ruta estática. Este mecanismo facilita mantener varias entradas lógicas, pero introduce una consecuencia relevante: si se modifica un alias que se está utilizando en una ruta, el sistema puede actualizar la tabla de enrutamiento al guardar el alias sin esperar a que el administrador pulse Apply Changes desde la pantalla de rutas. Por ello, el cambio de un alias asociado a rutas debe tratarse como una modificación activa de enrutamiento.

19.9. Procedimiento: desactivar, corregir y recuperar una ruta

1. Identificar la ruta correcta por su destino, gateway y descripción.
2. Documentar la situación previa y verificar qué tráfico depende del camino actual.
3. Si se necesita una suspensión temporal, utilizar Disable en lugar de Delete.
4. Guardar y aplicar los cambios; comprobar que la ruta deja de participar en la tabla de enrutamiento.
5. Corregir la configuración de la ruta o de la gateway implicada, si corresponde.
6. Volver a habilitar la ruta, aplicar los cambios y repetir las verificaciones de Diagnostics → Routes y del tráfico.

19.10. Diagnóstico: síntomas y causas más probables

Síntoma	Posibles causas	Primera comprobación
La ruta no aparece en la tabla	Sin Apply Changes, ruta deshabilitada o error de configuración.	Estado de la ruta y Diagnostics → Routes.
No aparece una gateway en Add	Gateway no creada, familia incompatible o configuración inadecuada.	System → Routing → Gateways.
La ruta existe, pero no hay respuesta	Ausencia de retorno, reglas, servicio o siguiente salto inaccesible.	Captura en la interfaz y reglas.
Tráfico inesperado por una interfaz	Ruta más específica, policy routing o regla con gateway asignada.	Tabla de rutas y reglas aplicadas.
Conexiones intermitentes	Estados, rutas asimétricas, ICMP Redirect o cambio de gateway.	Packet Capture, States y logs.
Un alias provoca un cambio imprevisto	Modificación del contenido de un alias usado en una ruta.	Historial del alias y la tabla de rutas.

19.11. Buenas prácticas y lista de comprobación

Definir únicamente las rutas necesarias y con prefijos tan concretos como permita el diseño.

Crear y verificar el gateway de siguiente salto antes de definir la ruta.
No utilizar rutas estáticas como sustituto de reglas de firewall o de una política NAT correcta.
Prever siempre el camino de retorno y las posibles rutas superpuestas.
Evitar modificaciones críticas desde una sesión remota sin procedimiento de recuperación.
Conservar una copia de configuración antes de cambios con impacto en producción.
Realizar pruebas de conectividad, traceroute y consulta de tabla de rutas tras Apply Changes.
Usar desactivación temporal para aislar problemas sin eliminar inmediatamente la definición.

19.12. Glosario breve

Término	Definición
Ruta estática	Entrada de enrutamiento configurada expresamente por un administrador.
Destino / prefijo	Red o host al que se aplica una entrada de la tabla de rutas.
Next hop / gateway	Dispositivo al que se envía el paquete para continuar hacia el destino.
Ruta predeterminada	Ruta que se utiliza si no existe una coincidencia de destino más específica.
Policy routing	Selección de ruta o gateway mediante reglas y criterios adicionales al destino.
Asimetría	Situación en la que ida y vuelta no siguen recorridos equivalentes.

Referencias técnicas

Netgate: Static Routes — https://docs.netgate.com/pfsense/en/latest/routing/static.html
Netgate: Gateway Settings — https://docs.netgate.com/pfsense/en/latest/routing/gateway-configure.html
Netgate: Troubleshooting Routes — https://docs.netgate.com/pfsense/en/latest/troubleshooting/routes.html
Netgate: Interface Configuration — https://docs.netgate.com/pfsense/en/latest/config/interface-configuration.html

20 System → Routing → Gateway Groups

System → Routing → Gateway Groups · Add / Edit Gateway Group

Configuración práctica de failover, balanceo de conexiones y selección de gateways.

Los grupos de gateways permiten que pfSense Plus trate varias puertas de enlace como una unidad de decisión. Según la prioridad asignada, el grupo puede mantener una conexión de respaldo, repartir conexiones nuevas entre varios enlaces o combinar ambos comportamientos. Su aplicación depende de las reglas de firewall y del uso concreto del grupo.



Figura 20.1. Panel Gateway Groups recreado sin grupos, direcciones ni identificadores de ninguna instalación.

Objetivos del capítulo

Interpretar la pantalla Gateway Groups y los iconos de gestión.

Configurar correctamente Tier, Virtual IP, Trigger Level y Keep Failover States.

Distinguir balanceo por conexiones de failover y del aumento real de ancho de banda.

Aplicar grupos a reglas de firewall o a la puerta de enlace predeterminada cuando sea compatible.

Comprobar la conmutación, analizar incidencias y recuperar el servicio.

20.1. ¿Qué resuelve un grupo de gateways?

Un gateway representa el siguiente salto para una ruta. Un grupo reúne varios gateways y les asigna criterios de prioridad y disponibilidad. El firewall selecciona el camino apropiado cuando se utiliza ese grupo en una regla con policy routing, en ciertos servicios o como ruta predeterminada de failover.



Figura 20.2. Diferencia conceptual entre failover, balanceo por conexiones y combinación de ambos.

CLAVE TÉCNICA Tier 1 tiene prioridad sobre Tier 2; varios gateways en el mismo Tier reparten nuevas conexiones cuando es posible. Una única descarga o sesión TCP no multiplica automáticamente su velocidad por combinar dos conexiones.

20.2. Pantalla principal: Gateway Groups

Ruta: System → Routing → Gateway Groups. La tabla se encuentra vacía cuando todavía no se han creado grupos; el botón Add abre el formulario de alta. Cuando existen entradas, cada fila representa un grupo configurado.

Columna	Qué muestra	Utilidad para el administrador
Group Name	Identificador del grupo usado en otros apartados de la interfaz.	Localizar la política correcta en reglas y servicios.
Gateways	Puertas de enlace incluidas en el grupo.	Reconocer sus miembros sin entrar en edición.
Priority	Distribución de prioridades o tiers configurados.	Distinguir enlaces principales, secundarios o compartidos.
Description	Texto explicativo introducido por el administrador.	Documentar la finalidad del grupo.
Actions	Controles para gestionar cada grupo cuando hay filas.	Editar, duplicar o eliminar, según los iconos presentes.
Add	Permite crear un nuevo grupo.	Iniciar una nueva política de selección de gateways.

Las pestañas Gateways, Static Routes y Gateway Groups representan funcionalidades distintas del mismo menú: alta y supervisión de gateways, rutas estáticas explícitas y políticas de selección multi-WAN. Su configuración debe ser coherente, pero ninguna de las tres sustituye a las otras.

20.3. Formulario Add / Edit Gateway Group

Al pulsar Add se abre “Edit Gateway Group Entry”; se emplea el mismo formulario básico para modificar grupos existentes. Se describen a continuación todos los controles visibles, sin utilizar valores particulares de una infraestructura.

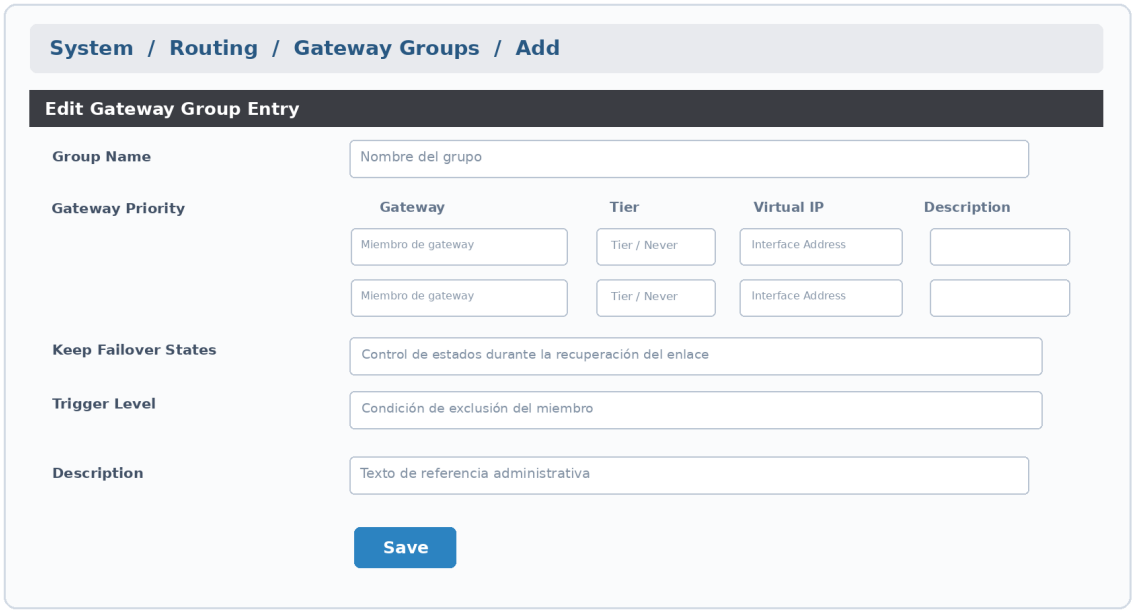


Figura 20.3. Estructura del formulario Add/Edit con campos genéricos y sin configuraciones.

Group Name

Nombre único con el que se identificará el grupo en la GUI y en los selectores de gateway de las reglas. Netgate documenta un máximo de 31 caracteres, con letras, cifras y guion bajo. Es obligatorio; conviene que describa la finalidad del grupo y no datos internos que no deban difundirse.

Gateway Priority: Gateway

Cada fila corresponde a una gateway ya definida en System → Routing → Gateways. Sólo pueden combinarse miembros de la misma familia de direcciones: un grupo IPv4 no incorpora gateways IPv6, y viceversa. La lista es de miembros potenciales: asignar Never excluye a ese miembro de la operación del grupo.

Gateway Priority: Tier

Define el nivel de prioridad de cada gateway. Se utilizan Tier 1 a Tier 5 y Never. Un número menor representa mayor prioridad. Si hay miembros en niveles distintos, el firewall utiliza el nivel de prioridad más alto disponible; si varios miembros comparten nivel, las nuevas conexiones se pueden distribuir entre ellos.

Selección	Interpretación	Efecto previsto
Tier 1	Prioridad máxima.	Se utiliza antes que cualquier Tier 2–5 disponible.
Tier 2 a Tier 5	Prioridades progresivamente menores.	Entran en uso al quedar indisponibles los tiers precedentes.
Dos gateways en Tier 1	Misma prioridad.	Reparto de conexiones nuevas entre ambas cuando el grupo se aplica mediante reglas.
Never	Miembro excluido.	No participa en este grupo, aunque exista como gateway en el sistema.

AVISO Un grupo destinado a ser gateway predeterminado o extremo de ciertas VPN debe configurarse como failover: sólo un miembro por Tier. Estos usos no admiten un grupo de balanceo con varios miembros simultáneos en el mismo Tier.

Gateway Priority: Virtual IP

Controla qué dirección de la interfaz se utilizará cuando determinados servicios enlacen su extremo local con un grupo, como Dynamic DNS, IPsec u OpenVPN. Interface Address es la selección habitual si no se necesita una dirección virtual específica. En un clúster HA puede resultar apropiado seleccionar una VIP CARP; esto requiere una arquitectura de HA configurada y coherente.

La elección de Virtual IP no crea una VIP por sí sola y tampoco cambia la ruta del tráfico de los clientes. No debe confundirse con un pool de IP públicas, con la dirección del gateway ni con NAT.

Gateway Priority: Description

La descripción mostrada junto a la gateway en el formulario ayuda a identificar cada miembro. No debe confundirse con el campo Description global del grupo, situado al final. La descripción es administrativa y no modifica la prioridad del enlace.

20.4. Link Priority: cómo se selecciona el enlace

El texto de ayuda de la pantalla explica la relación entre tiers y prioridad. Los miembros de una misma prioridad pueden balancear conexiones; al agotarse los miembros disponibles de un tier, el sistema pasa al siguiente. El algoritmo de balanceo se aplica a conexiones, no a los bytes de cada enlace.

En un escenario mixto, varios miembros del primer tier pueden distribuir conexiones; si ninguno está disponible, otros miembros de una prioridad secundaria entran en servicio. El reparto no garantiza porcentajes idénticos de tráfico en Mbps: cada conexión puede consumir una cantidad distinta de ancho de banda.

20.5. Keep Failover States

Afecta al comportamiento de los estados de firewall creados mediante policy routing cuando se recupera un gateway de mayor prioridad. Es un control asociado al retorno del enlace preferente, distinto del que determina qué sucede al fallar un enlace.

Opción	Qué sucede cuando se recupera el gateway preferente	Cuándo interesa
Use global behavior (default)	Aplica el comportamiento definido en System → Advanced → Miscellaneous.	Cuando se desea una política uniforme para varios grupos.

Opción	Qué sucede cuando se recupera el gateway preferente	Cuándo interesa
Keep states on gateway recovery	Mantiene los estados existentes por el gateway secundario hasta que las conexiones finalicen o se restablezcan.	Favorece la continuidad de sesiones largas.
Kill states on gateway recovery	Cierra estados de policy routing establecidos por gateways de menor prioridad para que las conexiones puedan restablecerse por el preferente.	Permite retorno más inmediato, con interrupción de sesiones activas.
LIMITACIÓN Conservar un estado no garantiza que la sesión siga funcionando si cambia la IP pública de salida, la NAT, la ruta real o el extremo remoto. Kill/Keep trata estados del firewall, no crea continuidad de sesión a nivel de aplicación.		

Los cambios de tiers o prioridades suelen afectar a conexiones nuevas. Los estados ya existentes pueden permanecer hasta expirar, salvo que se eliminen de forma explícita o por las políticas de fallo/recuperación.

20.6. Trigger Level: cuándo se excluye un miembro

La condición de activación es una de las decisiones más importantes del grupo. Utiliza resultados de monitorización de gateways y debe ser congruente con las características de los enlaces y sus umbrales individuales.

Trigger Level	Condición de exclusión	Ventaja y precaución
Member Down	Excluye cuando la gateway está considerada caída de forma efectiva.	Evita cambios por degradaciones leves; puede reaccionar tarde a enlaces muy deteriorados.
Packet Loss	Excluye al rebasarse el umbral de aviso de pérdida configurado.	Detecta enlaces con pérdidas antes de una caída completa; cuidado con falsos positivos.
High Latency	Excluye al rebasarse el umbral de aviso de latencia.	Útil para aplicaciones sensibles al retardo; puede oscilar en redes de alta latencia.
Packet Loss or High Latency	Excluye al cumplirse cualquiera de las dos condiciones.	Mayor sensibilidad ante degradación; exige umbrales bien ajustados.

Los umbrales de latencia y pérdida se gestionan en los ajustes avanzados de la gateway y afectan a cómo se clasifica su salud. El Trigger Level no sustituye a configurar un Monitor IP significativo: si el destino de monitorización sigue contestando aunque el acceso a Internet esté roto, el grupo podría mantener el enlace equivocado.

Description y Save

Description es un campo libre para explicar qué tráfico o prioridad cubrirá el grupo. Save guarda la definición. Si la GUI muestra Apply Changes, habrá que aplicarlo antes de realizar pruebas. Crear el grupo no implica automáticamente que la LAN o todos los servicios empiecen a usarlo: debe seleccionarse donde corresponda.

20.7. Procedimiento práctico: crear un grupo de failover

1. Verificar en System → Routing → Gateways que existen las puertas de enlace necesarias y que cada una dispone de una monitorización útil.
2. Abrir System → Routing → Gateway Groups y pulsar Add.
3. Escribir un nombre identificativo del propósito del grupo.
4. Asignar Tier 1 a la puerta de enlace preferente y Tier 2 a la alternativa de respaldo, ambas de la misma familia IP.
5. Elegir el Trigger Level conforme a la tolerancia a pérdida o latencia; Member Down resulta menos sensible a degradaciones parciales.
6. Mantener Interface Address como Virtual IP si ningún servicio exige una VIP específica.
7. Elegir Keep Failover States según la importancia de conservar sesiones durante la recuperación y documentar la decisión.
8. Añadir una descripción comprensible, pulsar Save y aplicar los cambios pendientes.

9. Asociar el grupo a la regla de firewall o al gateway predeterminado, según lo que se necesite proteger.
10. Comprobar Status → Gateways y probar la pérdida y recuperación del enlace en una ventana controlada.

RESULTADO ESPERADO Las conexiones nuevas emplean el gateway preferente mientras esté apto; si deja de estar disponible según la política del grupo, los flujos nuevos se dirigen al siguiente tier. Las sesiones en curso pueden requerir reconexión.

20.8. Procedimiento práctico: balanceo de conexiones

1. Confirmar que los dos gateways comparten familia IP y tienen monitorización operativa.
2. Crear un grupo nuevo y asignar Tier 1 a ambos gateways.
3. Elegir Trigger Level y guardar el grupo.
4. Acceder a Firewall → Rules en la interfaz por la que ingresa el tráfico de los clientes.
5. Editar la regla de paso pertinente, abrir sus opciones avanzadas y seleccionar el grupo en el campo Gateway.
6. Guardar, aplicar y crear varias conexiones nuevas hacia destinos adecuados para observar la distribución.
7. Verificar en la tabla de estados, los registros y Status → Gateways qué conexiones usan cada camino.

El reparto predeterminado es por conexiones y puede ser ponderado mediante Weight en los ajustes de cada gateway. No equivale a sumar caudales para una única conexión. La opción Use sticky connections, disponible en System → Advanced → Miscellaneous, ayuda a mantener afinidad de origen en aplicaciones que requieren una IP pública de salida estable.

20.9. ¿Dónde se aplica el grupo creado?

Contexto	Ruta o lugar	Consideración clave
Tráfico de usuarios	Firewall → Rules → interfaz de entrada → Gateway en opciones avanzadas.	Policy routing dirige las conexiones que coincidan con esa regla.
Tráfico originado por el firewall	System → Routing → Gateways → Default gateway.	Para la ruta predeterminada se admite un grupo de failover; no balanceo en el mismo Tier.
Servicios vinculados a enlaces	Opciones específicas del servicio: Dynamic DNS, IPsec u OpenVPN, si son compatibles.	Pueden necesitar Virtual IP o una configuración propia de failover.
Redes conectadas y VPN	Reglas de excepción y rutas específicas.	Evitar que policy routing desvíe tráfico destinado a subredes internas o túneles VPN.

NO CONFUNDIR Configurar Default gateway permite gobernar la ruta de tráfico sin una regla de policy routing, incluido el originado por el firewall. Para dirigir categorías de tráfico de clientes con políticas concretas, se utilizan reglas de firewall con el grupo como Gateway.

20.10. Verificación del failover y del balanceo

Las pruebas deben contemplar la detección del problema, la elección de gateway, la continuidad o reconexión de las sesiones y la recuperación posterior. Una sola prueba de ping no basta para demostrar el funcionamiento integral.

Comprobación	Dónde	Qué se busca
Estado de gateways	Status → Gateways.	Miembros Online o con alertas coherentes con el escenario.
Estado del grupo	Status → Gateways → Gateway Groups.	Tiers y selección efectivos.
Regla de policy routing	Firewall → Rules.	Gateway Group elegido y orden de reglas adecuado.
Tabla de estados	Diagnostics → States.	Comportamiento de sesiones con cada salida.

Comprobación	Dónde	Qué se busca
NAT de salida	Firewall → NAT → Outbound.	Traducción adecuada en cada WAN utilizada.
Registro de fallos	Status → System Logs → Gateways o vistas equivalentes.	Eventos de dpinger y cambios de estado.
Prueba de fallo	Desconexión controlada del enlace o simulación autorizada.	Tráfico nuevo usa el enlace de respaldo.
Prueba de recuperación	Restituir el enlace y repetir conexiones.	Tráfico nuevo regresa según tiers y política de estados.

20.11. Diagnóstico: problemas habituales

Síntoma	Causa probable	Revisión prioritaria
No conmuta al enlace secundario	La monitorización no declara caído el primario o el grupo no se usa.	Monitor IP, Trigger Level y reglas.
El grupo existe pero la LAN sigue igual	No se ha aplicado a la regla de entrada ni al default gateway pertinente.	Campo Gateway en firewall rules.
Los enlaces no reparten conexiones	Diferentes Tier, reglas que no coinciden, sticky sessions o pruebas con una sola conexión.	Tiers, reglas y estados nuevos.
Al volver el primario se cortan sesiones	Kill states on gateway recovery o política global equivalente.	Keep Failover States y Miscellaneous.
Se pierde resolución DNS al fallar WAN	DNS configurado sólo para una WAN o salida por gateway equivocado.	System → General Setup y DNS Resolver/Forwarder.
VPN falla pese al failover	Enrutamiento, endpoint, certificados, negociación y dirección de salida no compatibles.	Logs VPN y uso permitido del grupo.
Un enlace degradado sigue activo	Trigger Level no supervisa la degradación o umbrales demasiado permisivos.	Thresholds del gateway y Trigger Level.
Una sesión sale por una WAN inesperada	Enrutamiento por políticas, orden de reglas o estados previos.	Reglas, tabla de estados, NAT y reply-to.

20.12. Riesgos y buenas prácticas

No mezclar gateways IPv4 e IPv6 dentro del mismo grupo; tratar cada familia por separado.

Crear un grupo de un solo gateway por Tier cuando se use como ruta predeterminada o extremo VPN compatible.

Seleccionar Monitor IP que permita distinguir la pérdida real de Internet del funcionamiento del equipo del operador.

Evitar que tráfico hacia redes internas, rutas estáticas o VPN sea forzado por error hacia las WAN.

Comprobar NAT de salida, DNS por WAN, policy routing, reply-to y estados antes de pasar a producción.

No suponer continuidad de sesiones al cambiar de IP pública; probar aplicaciones críticas.

Programar una ventana y contar con acceso de recuperación si se modifican reglas remotas.

Guardar una copia de configuración y documentar cambios en las prioridades y disparadores.

Verificar el failover físicamente y también ante degradación, si ésa es la condición de activación prevista.

Usar grupos y ponderaciones adecuados al coste, límite de datos y rendimiento de cada enlace, no sólo a su disponibilidad.

20.13. Glosario operativo

Concepto	Definición breve
Gateway Group	Conjunto de gateways tratados como una unidad en determinadas opciones de pfSense.
Tier	Nivel de prioridad; menor número equivale a preferencia superior.

Concepto	Definición breve
Failover	Conmutación a otro gateway cuando no está disponible el nivel preferente.
Load balancing	Distribución de conexiones nuevas entre gateways de la misma prioridad.
Policy routing	Selección de gateway mediante reglas que coinciden con el tráfico.
Trigger Level	Condición que determina cuándo un miembro deja de participar.
dpinger	Servicio de monitorización de gateways y calidad del enlace.
State	Registro de una conexión que PF mantiene para procesar sus paquetes.
Virtual IP	Dirección virtual seleccionable para ciertos servicios que usan el grupo.

20.14. Matriz de decisiones en producción

Necesidad operativa	Configuración habitual	Advertencia
Continuidad con segundo acceso de respaldo	Un gateway en Tier 1 y otro en Tier 2.	Probar que el monitor detecta una caída real del proveedor.
Reparto de conexiones nuevas	Dos o más gateways compatibles en el mismo Tier.	No acelera una conexión única; revisar afinidad de sesiones.
Enlace de respaldo con límite de datos	Failover por tiers y reglas selectivas.	Evitar que actualizaciones o copias consuman el enlace de reserva.
Servicios sensibles a latencia	Trigger de High Latency o Packet Loss or High Latency.	Ajustar umbrales para evitar conmutaciones constantes.
Sesiones largas y retorno del primario	Keep states on gateway recovery.	El tráfico nuevo puede preferir otro enlace antes que el existente.

20.15. Procedimiento de reversión y control del cambio

1. Registrar el estado de los miembros y del grupo en Status → Gateways.
2. Guardar una copia de la configuración antes de modificar tiers, reglas o disparadores.
3. Identificar la regla de firewall o servicio que utiliza el grupo; anotar su selección anterior.
4. Si el tráfico no sigue el camino esperado, restituir primero el gateway o grupo anterior de esa regla.
5. Recuperar los valores previos de Tier, Trigger Level y política de estados, aplicar cambios y repetir una prueba funcional.
6. Comprobar que las conexiones nuevas utilizan la salida prevista y registrar el resultado de la intervención.

CRITERIO DE ACEPTACIÓN Una configuración Multi-WAN se considera verificada cuando se han probado de forma controlada el funcionamiento normal, el fallo, la recuperación y el comportamiento de los servicios críticos, sin depender únicamente del color Online de la pantalla.

Referencias técnicas

Netgate · Gateway Groups: https://docs.netgate.com/pfsense/en/latest/routing/gateway-groups.html
Netgate · Load Balancing and Failover: https://docs.netgate.com/pfsense/en/latest/multiwan/load-balance-and-failover.html
Netgate · Gateway Configuration: https://docs.netgate.com/pfsense/en/latest/routing/gateway-configure.html
Netgate · Policy Routing Configuration: https://docs.netgate.com/pfsense/en/latest/multiwan/policy-route.html
Netgate · Verifying Multi-WAN: https://docs.netgate.com/pfsense/en/latest/multiwan/test.html
Netgate · Troubleshooting Multi-WAN: https://docs.netgate.com/pfsense/en/latest/troubleshooting/multi-wan.html

21 Setup Wizard → Bienvenida

Pantalla de bienvenida, navegación y preparación de la configuración inicial

Ruta de acceso: System → Setup Wizard | Encabezado mostrado: Wizard / pfSense Plus Setup

OBJETIVO Comprender la pantalla inicial del asistente, conocer qué ocurre al continuar y preparar una intervención segura antes de modificar parámetros de red.

21.1. Qué es el asistente de configuración

El Setup Wizard de pfSense Plus es un recorrido guiado pensado para establecer los parámetros esenciales de funcionamiento del firewall. Se presenta habitualmente tras el primer acceso a la interfaz web y puede iniciarse de nuevo desde System → Setup Wizard. Su uso es opcional: el equipo también puede administrarse desde los menús de configuración.

El asistente facilita la secuencia inicial de trabajo, pero no sustituye el conocimiento del diseño de red ni configura automáticamente todos los servicios empresariales avanzados. Resulta especialmente útil en instalaciones nuevas y en tareas de puesta en marcha controladas.

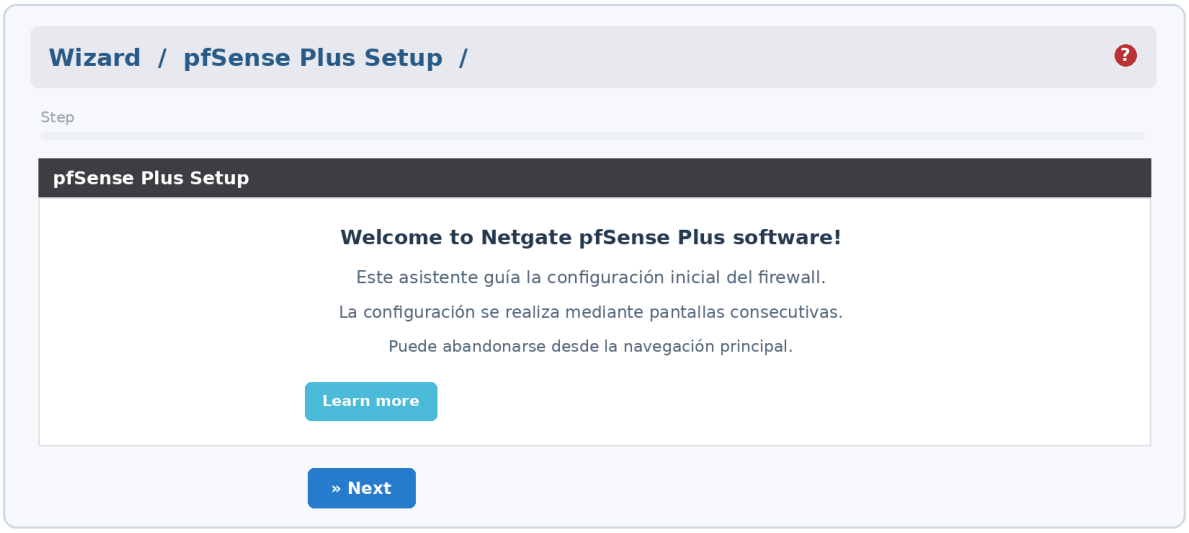


Figura 21.1. Reconstrucción esquemática de la bienvenida del asistente, sin datos de ninguna instalación.

21.2. Lectura completa de la pantalla de bienvenida

Elemento visible	Función	Interpretación práctica
Wizard / pfSense Plus Setup	Ruta de navegación que identifica el asistente.	Permite reconocer que se está en el flujo de configuración y no en un formulario aislado.
Step / barra de progreso	Indicador de avance por etapas del asistente.	Al comienzo puede aparecer vacío o sin progreso significativo.
pfSense Plus Setup	Título del panel de bienvenida.	Delimita el área donde se presentan las instrucciones y controles.
Mensaje Welcome	Presenta el objetivo del asistente y su carácter guiado.	Es informativo; no contiene todavía valores de configuración.
Learn more	Enlace a información adicional del producto.	Puede abrir información externa; no guarda ni aplica parámetros de red.
Next	Continúa hacia la pantalla siguiente.	Inicia la navegación por el asistente, no activa por sí mismo una nueva configuración.
Icono de ayuda (?)	Acceso a ayuda contextual de la interfaz.	Útil para contrastar el significado de las opciones antes de avanzar.
Logotipo o navegación superior	Permite abandonar el recorrido.	La configuración manual sigue disponible fuera del asistente.

21.3. Qué ocurre al pulsar Next

En esta primera pantalla, Next avanza a una página informativa sobre las opciones de asistencia y soporte de Netgate. Tras ella, el asistente pasa a las pantallas de configuración, donde se introducen los parámetros del firewall. No debe confundirse avanzar por la bienvenida con aplicar cambios al sistema.

Los valores reunidos por el asistente se aplican cuando se completa el proceso y se ejecuta su paso final de recarga. Ese momento puede provocar reinicios de servicios o cambios de conectividad, particularmente si se modifica la dirección de administración o la conexión WAN.



Figura 21.2. Secuencia conceptual: bienvenida, configuración, aplicación y comprobación.

21.4. Preparación antes de continuar

Antes de entrar en las pantallas de parametrización, la decisión profesional es comprobar el estado del equipo y reunir la información mínima necesaria. En un firewall activo, ejecutar el asistente de nuevo puede afectar a servicios existentes si se modifican sus parámetros.

Qué revisar	Por qué importa	Comprobación recomendada
Acceso administrativo	Un cambio de IP o de credenciales puede cortar la sesión actual.	Disponer de acceso local o por consola y de un plan de reconexión.
Topología y cableado	La WAN y la LAN deben corresponder con las interfaces previstas.	Identificar físicamente los puertos y su función antes de modificar nada.
Acceso del proveedor	Algunos enlaces necesitan parámetros que no pueden deducirse.	Tener disponibles los datos de conexión, si son necesarios.
Direccionamiento LAN	Cambiar subred o puerta de enlace afecta a clientes y servicios.	Comprobar que no se solapa con redes VPN o conectadas.
DNS y horario	Influyen en resolución de nombres, certificados, logs y actualizaciones.	Conocer la política DNS y la zona horaria prevista.
Credencial administrativa	La contraseña inicial no debe conservarse en producción.	Preparar una contraseña robusta y gestionarla de forma segura.
Copia de configuración	Puede ser necesario volver al estado anterior.	Exportar una copia desde Diagnostics → Backup & Restore antes de reconfigurar.

ADVERTENCIA En un firewall en producción, ejecutar de nuevo el Setup Wizard no equivale a abrir una guía de lectura. Si se guardan y aplican parámetros nuevos, pueden cambiar la WAN, la LAN o las credenciales. Preparar una ventana de mantenimiento.

21.5. Procedimiento: entrar, avanzar o salir de forma segura

1. Acceder a la interfaz de administración y confirmar que se está trabajando sobre el firewall autorizado.
2. Abrir System → Setup Wizard o continuar desde la pantalla inicial si se muestra automáticamente.
3. Leer la bienvenida y utilizar Learn more o la ayuda contextual si se necesita información complementaria.
4. Comprobar que están disponibles los parámetros de red y un método alternativo de administración.
5. Pulsar Next para mostrar la información de soporte e iniciar la secuencia guiada.

6. Si no se desea configurar el equipo mediante el asistente, salir desde el logotipo o la navegación principal sin completar ni aplicar cambios.
7. Si se continúa hasta el final, revisar detenidamente los valores introducidos antes de ejecutar la recarga final.

Resultado esperado: el administrador comprende en qué fase se encuentra y distingue una pantalla informativa de una operación que puede modificar la configuración. La bienvenida no exige introducir IP, contraseñas ni datos del proveedor.

21.6. Qué configura el asistente y qué queda fuera

La secuencia estándar de Netgate guía por aspectos generales del sistema, resolución DNS, sincronización horaria, parámetros WAN, dirección LAN y contraseña administrativa, antes de realizar la recarga y finalización. El contenido exacto y el orden de pantallas pueden cambiar entre versiones; cada formulario debe interpretarse según su interfaz real.

Área	Alcance habitual del asistente	Tratamiento posterior
Identidad del equipo	Nombre del equipo y dominio.	System → General Setup, si se requiere ajuste avanzado.
DNS y hora	Servidores DNS, NTP y zona horaria.	DNS Resolver/Forwarder y políticas de resolución.
WAN y LAN	Parámetros esenciales de conectividad.	Interfaces, VLAN, gateways y reglas específicas.
Administración	Cambio inicial de contraseña.	Usuarios, permisos, MFA y acceso administrativo.
Funciones empresariales	No constituye una implantación completa de todas ellas.	VPN, Multi-WAN, HA, NAT, IDS/IPS y servicios adicionales.

21.7. Errores frecuentes y formas de evitarlos

Situación	Posible explicación	Acción adecuada
Next no responde	Sesión caducada, error de navegador o fallo de interfaz.	Recargar la página tras comprobar el estado de la sesión; revisar logs si persiste.
La pantalla informa de parámetros no conocidos	Falta información del proveedor o del diseño interno.	No inventar valores. Consultar los datos necesarios y reanudar después.
Se pierde acceso tras terminar	Cambio de la IP LAN o del segmento usado por el cliente.	Adaptar la dirección del ordenador o renovar la concesión DHCP; acceder por la IP nueva.
La WAN no conecta tras la aplicación	Tipo de conexión o credenciales incompatibles con el proveedor.	Revisar configuración de la WAN, estado del enlace y gateway.
No hay acceso a determinados servicios	El asistente sólo aplica una configuración inicial.	Completar las reglas, rutas, DNS y servicios que el diseño requiera.
El administrador quiere volver atrás	Se ha terminado el asistente con valores incorrectos.	Revisar configuración y, si procede, restaurar un respaldo verificado.

21.8. Buenas prácticas de administración

Utilizar el asistente principalmente para la puesta en marcha y no como método habitual de cambios sobre un firewall en servicio.

Planificar la asignación de interfaces, direccionamiento y conectividad antes de iniciar la configuración.

Evitar trabajar únicamente a través de un acceso remoto que podría perderse al cambiar la WAN o la LAN.

No dar por configuradas políticas de seguridad complejas sólo porque el asistente haya finalizado correctamente.

Cambiar las credenciales predeterminadas y comprobar posteriormente que el acceso web está restringido a redes autorizadas.

Probar resolución DNS, sincronización horaria, conectividad desde LAN, salida a Internet y estado de los servicios tras finalizar.

Conservar copias de la configuración y documentar los cambios relevantes con criterios operativos.

21.9. Lista de comprobación al finalizar

Verificación	Criterio de aceptación
Acceso a la GUI	Se puede iniciar sesión con las credenciales previstas por la red administrativa autorizada.
Interfaces	WAN y LAN corresponden a los puertos y parámetros definidos en el diseño.
Gateway	La ruta de salida y la monitorización se comportan de forma coherente.
DNS	El firewall y los clientes autorizados pueden resolver nombres según la política establecida.
Hora	La fecha, la zona horaria y la sincronización NTP son coherentes.
Seguridad	Las reglas efectivas y los servicios expuestos coinciden con la política aprobada.
Respaldo	Existe una copia de configuración utilizable y almacenada de forma segura.

IDEA CLAVE La pantalla de bienvenida no realiza una configuración por sí misma: introduce un recorrido que debe completarse con datos correctos, aplicarse de forma controlada y verificarse después.

Referencias técnicas

Netgate · Setup Wizard: https://docs.netgate.com/pfsense/en/latest/config/setup-wizard.html

Netgate · Initial Configuration: https://docs.netgate.com/pfsense/en/latest/solutions/netgate-2100/initial-configuration.html

Netgate · Backup and Restore: https://docs.netgate.com/pfsense/en/latest/backup/index.html

22 System → Update

Actualizaciones, ramas de firmware, entornos de arranque y verificación segura

Ruta de acceso: System → Update | Pestañas: System Update · Update Settings

OBJETIVO Identificar correctamente las actualizaciones disponibles, comprender las opciones de Boot Environments y ejecutar una actualización planificada, comprobable y reversible cuando la plataforma lo permita.

22.1. Actualizar el firewall: finalidad y alcance

El mantenimiento de pfSense Plus incluye la instalación de nuevas versiones del sistema base, correcciones de seguridad, mejoras de compatibilidad y cambios en componentes incluidos con el producto. System → Update centraliza la comprobación de versiones y las opciones que condicionan el comportamiento de la actualización.

Una actualización de sistema puede afectar a reglas, conectividad, servicios VPN, paquetes adicionales, controladores y disponibilidad durante el reinicio. Antes de actuar hay que distinguir tres procesos: consultar el estado, seleccionar la rama de seguimiento y ejecutar realmente la actualización.

PRINCIPIO OPERATIVO La indicación «Up to date» se interpreta siempre respecto de la rama elegida y de la comprobación efectuada; no garantiza que el firewall utilice la última rama estable publicada.

22.2. Pantalla System Update

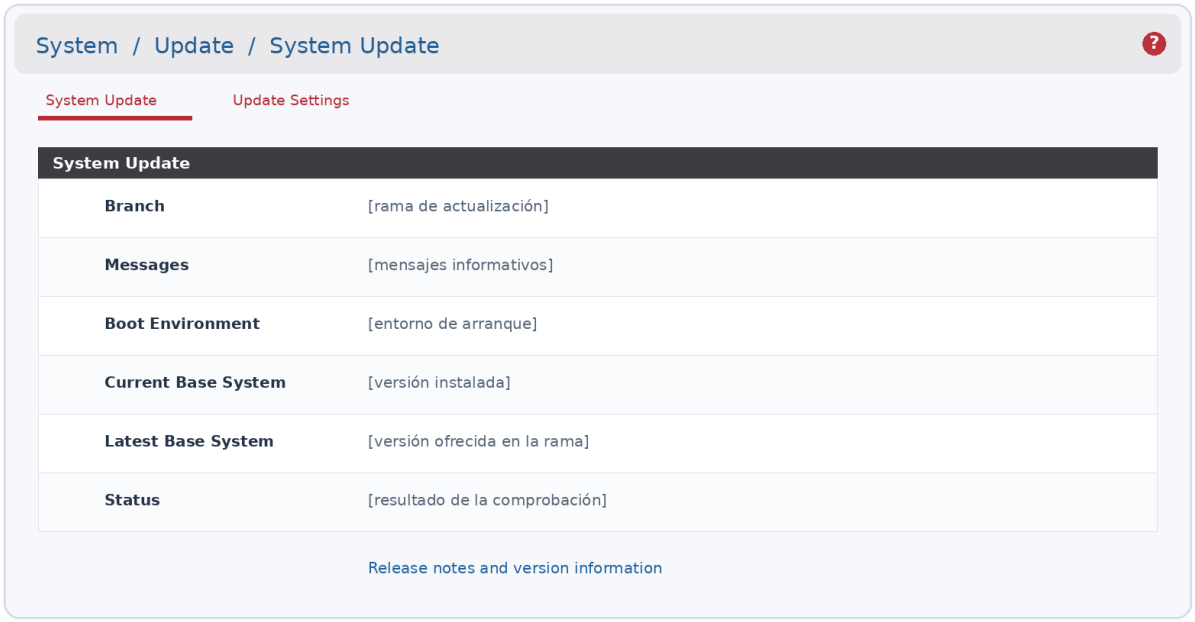


Figura 22.1. Representación neutra de System Update: etiquetas auténticas, valores deliberadamente omitidos.

Esta pestaña muestra qué rama de firmware se consulta, la versión base actualmente instalada y el resultado de la verificación frente al repositorio elegido. Su contenido varía si se detecta una actualización o si hay incidencias de acceso a repositorios.

Campo	Qué significa	Utilidad práctica
Branch	Rama del repositorio contra la que se comprueba el software.	Determina qué versiones se ofrecen; no expresa por sí sola la versión instalada.
Messages	Mensajes informativos del servicio de actualización o del derecho a obtener software.	Permite interpretar advertencias sin confundirlas con el estado de la conexión WAN.
Boot Environment	Entorno ZFS del sistema asociado a la instalación, si procede.	Identifica el contexto de arranque desde el que se supervisa la actualización.

Campo	Qué significa	Utilidad práctica
Current Base System	Versión del sistema base que ejecuta el firewall.	Dato para comparar con el destino de actualización y las notas de versión.
Latest Base System	Versión de destino disponible dentro de la rama seleccionada.	No debe confundirse con la última versión de todas las ramas existentes.
Status	Resultado de la consulta a los repositorios y estado de actualización.	Puede indicar que no hay novedades, que existe una versión o que hay un error.
Release notes and version information	Enlace a notas oficiales de versión y cambios.	Permite anticipar incompatibilidades, cambios funcionales y requisitos.
Confirm / control de actualización	Acción que aparece cuando la comprobación ofrece una actualización aplicable.	Inicia la operación tras la confirmación; no pulsarlo sin preparación.

22.3. Branch: comprender las ramas de firmware

La lista de ramas cambia durante el ciclo de desarrollo. Las denominaciones de la interfaz se deben interpretar funcionalmente, no como una clasificación inmutable: una rama «Previous Stable» puede ofrecer componentes de una versión anterior mientras el administrador espera una ventana de mantenimiento.

Rama orientativa	Propósito	Uso aconsejable
Latest Stable Version	Seguimiento de la versión estable publicada.	Referencia habitual en producción, tras revisar notas y compatibilidad.
Previous Stable Version / Legacy	Mantener temporalmente una rama estable anterior.	Transición planificada; no equivale a estar en la versión estable más reciente.
Latest Development Snapshots	Compilaciones de desarrollo con cambios recientes.	Laboratorio y pruebas, no producción.
Next Major Version	Pruebas de la siguiente versión principal, si la rama existe.	Validaciones especiales y entornos aislados; elevado riesgo de cambios.
Otras ramas especiales	Aparecen según licencia, ciclo o procedimiento de migración.	Consultar siempre la documentación aplicable antes de seleccionarlas.

ADVERTENCIA Seleccionar una rama de desarrollo puede introducir fallos o incompatibilidades. Un cambio de rama tampoco garantiza un mecanismo automático de downgrade seguro; recuperar un entorno anterior es un proceso distinto.

22.4. Interpretar los resultados de la comprobación

Mensaje o situación	Qué implica	Cómo actuar
Up to date	No se ofrece una versión superior en la rama consultada.	Revisar la rama y las notas oficiales si se esperaba una actualización.
Update available / versión ofrecida	El repositorio proporciona una versión candidata.	Verificar prerequisitos y programar su instalación.
Error al consultar	No se pudo determinar el estado con fiabilidad.	Comprobar conectividad, DNS, hora, repositorios y registros.
Mensajes de derecho de actualización	Informan sobre la modalidad de acceso al software.	No inferir de ahí que el sistema esté actualizado o desactualizado.
Versión de destino no cambia	La rama seleccionada puede apuntar al mismo nivel que el instalado.	Comparar origen, rama y versión publicada; evitar conclusiones apresuradas.

22.5. Pantalla Update Settings

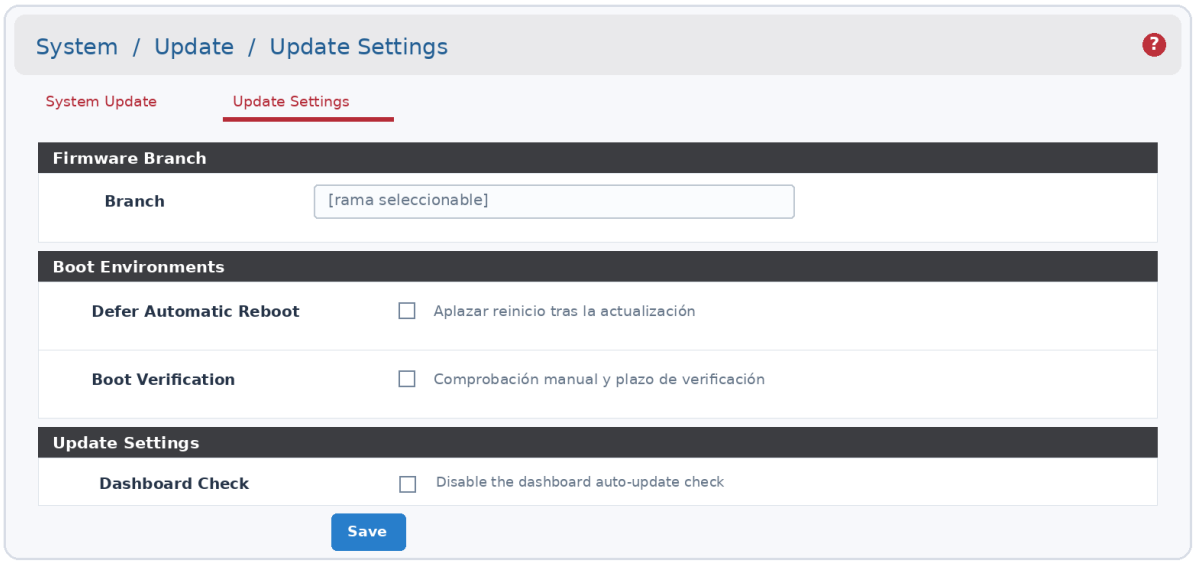


Figura 22.2. Reconstrucción de Update Settings sin ramas, versiones ni estados de una instalación.

Esta pestaña agrupa las preferencias del repositorio y el comportamiento del arranque después de una actualización. Algunas opciones se muestran exclusivamente en instalaciones con ZFS Boot Environments.

Opción	Efecto real	Precaución
Firmware Branch · Branch	Selecciona el canal de versiones utilizado en la comprobación.	Confirmar que la rama coincide con el plan de mantenimiento.
Defer Automatic Reboot	Impide el reinicio automático al terminar la instalación; el reinicio queda pendiente.	La nueva versión no se considera operativa hasta arrancarla y comprobarla.
Boot Verification · Manual Boot Verification	Exige confirmar manualmente en la interfaz que el nuevo Boot Environment funciona.	Si no se verifica a tiempo, puede activarse el retorno al entorno anterior.
Boot Verification · plazo	Tiempo disponible para validar el arranque antes del retorno automático.	Debe permitir acceso y pruebas de salud; el valor documentado por defecto es 300 s.
Dashboard Check · Disable dashboard auto-update check	Evita que el widget System Information realice una comprobación de actualizaciones al abrir el Dashboard.	Reduce cierta carga, pero obliga a comprobar las novedades por otros medios.
Save	Guarda las preferencias de actualización.	No inicia por sí mismo una nueva instalación de firmware.

22.6. Boot Environments: el mecanismo de recuperación

En pfSense Plus instalado sobre ZFS, el proceso moderno de actualización crea un Boot Environment adicional e instala allí los cambios antes del reinicio. Así se conserva una base anterior desde la que se puede volver a arrancar en determinadas incidencias. En UFS no existe este mismo sistema de entornos de arranque.

Antes de confiar en una recuperación automática conviene comprobar las condiciones que la hacen posible. El administrador debe identificar el sistema de archivos, comprobar que el entorno anterior existe y asegurarse de que la versión restaurada sigue siendo compatible con los datos de configuración que se pretenden recuperar.

Condición	Con ZFS y Boot Environments	Sin Boot Environments
Instalación del firmware	El proceso puede preparar y validar un nuevo entorno antes del reinicio.	Se utiliza el método de actualización que corresponda al sistema de archivos.
Recuperación	Puede seleccionarse un entorno arrancable anterior, si permanece disponible.	El plan depende de copias externas y procedimientos de reinstalación.

Condición	Con ZFS y Boot Environments	Sin Boot Environments
Protección contra fallo de disco	No queda resuelta: los entornos se almacenan localmente.	Tampoco queda resuelta: es imprescindible el respaldo externo.



Figura 22.3. Flujo de mantenimiento: preparación, instalación, reinicio y verificación.

22.6.1. Reinicio automático frente a reinicio diferido

Con la opción Defer Automatic Reboot sin marcar, el proceso normalmente reinicia al finalizar la instalación. Si se marca, el administrador controla el momento del reinicio. Esta segunda posibilidad ayuda a coordinar la interrupción del servicio, pero no la elimina: el nuevo entorno necesita arrancar para hacerse efectivo.

22.6.2. Verificación del arranque

Cuando se habilita Manual Boot Verification, el firewall exige una confirmación del nuevo entorno desde la interfaz, dentro del plazo configurado. El Dashboard muestra una solicitud de verificación. Si la confirmación no se realiza dentro del intervalo, el equipo puede reiniciar de nuevo desde el entorno anterior considerado válido. Esta política debe planificarse especialmente en emplazamientos con acceso exclusivamente remoto.

22.6.3. No confundir tres conceptos

Concepto	Qué protege	Qué no sustituye
Backup de configuración	Parámetros, reglas y definición de servicios exportables.	No es una imagen completa del firmware.
ZFS Boot Environment	Estado del sistema arrancable conservado localmente.	No es una copia externa ni protege frente a fallo físico del disco.
Reinicio diferido	Permite elegir cuándo arrancar el nuevo entorno.	No es una prueba de compatibilidad ni implica actualización sin corte.

22.7. Preparación profesional antes de actualizar

1. Consultar las release notes oficiales de la rama de destino y comprobar avisos, requisitos del hardware, compatibilidad de VPN y de paquetes instalados.
2. Exportar una copia completa desde Diagnostics → Backup & Restore y conservarla fuera del firewall; confirmar que puede recuperarse.
3. Revisar System → Boot Environments: comprobar que existe capacidad libre suficiente y conservar al menos un entorno anterior funcional, cuando proceda.
4. Verificar el estado de interfaces, gateways, DNS, rutas, fecha, servicios esenciales, registros y acceso administrativo antes de cambiar nada.
5. Registrar el inventario de paquetes adicionales y comprobar que los repositorios corresponden a la versión y rama previstas; no adelantar la actualización de paquetes desde un repositorio de versión posterior.
6. Programar ventana de mantenimiento y asegurar un método de acceso a consola o recuperación, especialmente en equipos remotos.
7. Si se trata de un clúster HA, revisar el procedimiento de Netgate y hacer respaldo de ambos nodos; no actualizar ambos simultáneamente.

PRECAUCIÓN En equipos de recursos limitados, el espacio ZFS y la memoria pueden condicionar la actualización. Netgate recomienda revisar Boot Environments y liberar recursos no esenciales antes de una intervención importante.

22.8. Procedimiento: actualización estable desde la interfaz

1. Acceder a System → Update y comprobar Current Base System, rama seleccionada y resultado de la consulta.
2. Seleccionar o confirmar la rama estable autorizada; dejar que la interfaz realice la nueva comprobación de versiones.
3. Abrir las notas de versión y verificar compatibilidad, estado de respaldos y preparación del plan de recuperación.
4. Decidir en Update Settings si se difiere el reinicio y, cuando haya Boot Environments, cómo se realizará la verificación posterior.
5. Guardar las preferencias con Save y regresar a System Update.
6. Si se ofrece una actualización, utilizar Confirm únicamente dentro de la ventana aprobada y observar el progreso sin interrumpirlo.
7. Permitir que el sistema finalice la instalación y reinicie, o ejecutar el reinicio manual cuando la opción de aplazamiento esté activada.
8. Volver a acceder a la GUI, comprobar la versión que realmente se ejecuta y, si se exige, confirmar el Boot Environment antes de vencer el plazo.
9. Realizar las pruebas de servicios, conectividad y aplicaciones críticas, y documentar el resultado.

Cuando el proceso no puede realizarse por la GUI, Netgate documenta la opción 13 de la consola como alternativa de actualización. No conviene recurrir a comandos de reparación de paquetes sin haber identificado la causa de un fallo.

22.9. Mantenimiento con alta disponibilidad

En clústeres con CARP, la actualización debe realizarse por fases. El procedimiento general es actualizar primero el nodo secundario, verificarlo, forzar de forma controlada una conmutación desde el primario mediante el modo de mantenimiento persistente CARP, actualizar el primario y validar de nuevo todo el conjunto.

Durante la coexistencia temporal de distintas versiones pueden existir diferencias en la sincronización pfsync y las sesiones podrían interrumpirse al conmutar. Por ello se deben seguir las notas específicas de cada versión y comprobar siempre la salud del nodo secundario antes de trasladar tráfico real.

22.10. Incidencias habituales y diagnóstico

Síntoma	Causa posible	Verificación y respuesta
No se ofrece una versión esperada	Rama anterior, repositorio no accesible o consulta fallida.	Revisar Branch, DNS, fecha, gateway y conectividad al repositorio; no cambiar a desarrollo como solución.
Estado «Up to date» inesperado	Comparación limitada a la rama elegida.	Comprobar si la rama de seguimiento corresponde a la última estable.
Fallan las descargas	Problema de salida a Internet, proxy, TLS o rutas.	Revisar configuración de conectividad y proxy del sistema; consultar registros.
Falta espacio	Demasiados entornos ZFS o almacenamiento insuficiente.	Revisar espacio antes de borrar entornos antiguos; conservar uno utilizable.
El equipo no reaparece tras el reinicio	Arranque fallido, cambio de conectividad o demora de servicios.	Consultar consola y Boot Environments; aplicar procedimiento oficial de recuperación.
Se produjo retorno a la versión anterior	No se verificó a tiempo el arranque o falló su validación.	Consultar causa y plazo de verificación; verificar versión y entorno que están activos.
El Dashboard no anuncia nuevas versiones	La comprobación automática puede estar desactivada.	Abrir System → Update para realizar una consulta explícita.

Síntoma	Causa posible	Verificación y respuesta
Paquete o VPN falla tras actualizar	Cambio de compatibilidad, servicio o dependencia.	Revisar logs y estado del paquete, respaldos, notas de versión y opciones de recuperación.

Netgate indica que el registro del último intento de actualización puede consultarse en /conf/upgrade_log.latest.txt. Su contenido debe tratarse como información operativa sensible y revisarse antes de compartirlo externamente.

22.11. Lista de comprobación posterior

Área	Prueba que debe superarse
Versión ejecutada	Coincide con el destino aprobado; no basta con que se haya completado la descarga.
Boot Environment	El entorno correcto está activo y, si aplica, verificado.
Acceso de administración	La GUI y el canal de consola previsto responden.
Red y gateways	Las interfaces y rutas funcionan; se verifica la salida y los enlaces secundarios.
Firewall y NAT	Las reglas, traducciones, aliases y rutas críticas siguen actuando correctamente.
VPN	Túneles y servicios de acceso remoto disponibles; se comprueba tráfico real.
Servicios	DNS, DHCP, NTP y paquetes relevantes levantados y operativos.
Registros	No se observan errores recurrentes de actualización, arranque o paquetes.
Recuperación	Copia externa preservada y Boot Environment anterior conservado hasta validar estabilidad.

IDEA CLAVE Actualizar de forma profesional no es pulsar Confirm: es preparar una copia, seleccionar la rama correcta, controlar el reinicio, validar el nuevo entorno y comprobar que los servicios siguen funcionando.

Referencias técnicas

Netgate · Upgrade Guide: https://docs.netgate.com/pfsense/en/latest/install/upgrade-guide.html

Netgate · Pre-Upgrade Tasks: https://docs.netgate.com/pfsense/en/latest/install/upgrade-guide-prepare.html

Netgate · Perform the Upgrade: https://docs.netgate.com/pfsense/en/latest/install/upgrade-guide-update.html

Netgate · Upgrade Process Overview: https://docs.netgate.com/pfsense/en/latest/install/upgrade-guide-overview.html

Netgate · Managing Boot Environments: https://docs.netgate.com/pfsense/en/latest/backup/zfsbe/gui.html

Netgate · Upgrading HA Clusters: https://docs.netgate.com/pfsense/en/latest/install/upgrade-guide-ha.html

Netgate · Troubleshooting Upgrades: https://docs.netgate.com/pfsense/en/latest/troubleshooting/upgrades.html

23 System → User Manager

Usuarios, grupos, sesiones, contraseñas y servidores de autenticación

Ruta: System → User Manager | Pestañas: Users · Groups · Settings · Change Password · Authentication Servers

23.1. Finalidad: gestionar quién accede y qué puede hacer

User Manager centraliza las cuentas locales, los grupos, los privilegios y las fuentes de autenticación del firewall. Es una función crítica: permite separar tareas administrativas, limitar accesos y utilizar identidades locales o directorios externos para la interfaz web y determinados servicios como VPN y portal cautivo.

IDEA CLAVE Autenticación significa demostrar una identidad. Autorización significa determinar las funciones a las que esa identidad tiene acceso. Una contraseña válida no equivale a permiso de administración.

El menú se organiza en cinco pestañas. Su contenido varía en función de la edición y del tipo de cuenta. Las ilustraciones de este capítulo son reconstrucciones neutras: muestran etiquetas y estructuras, nunca datos de sistemas concretos.

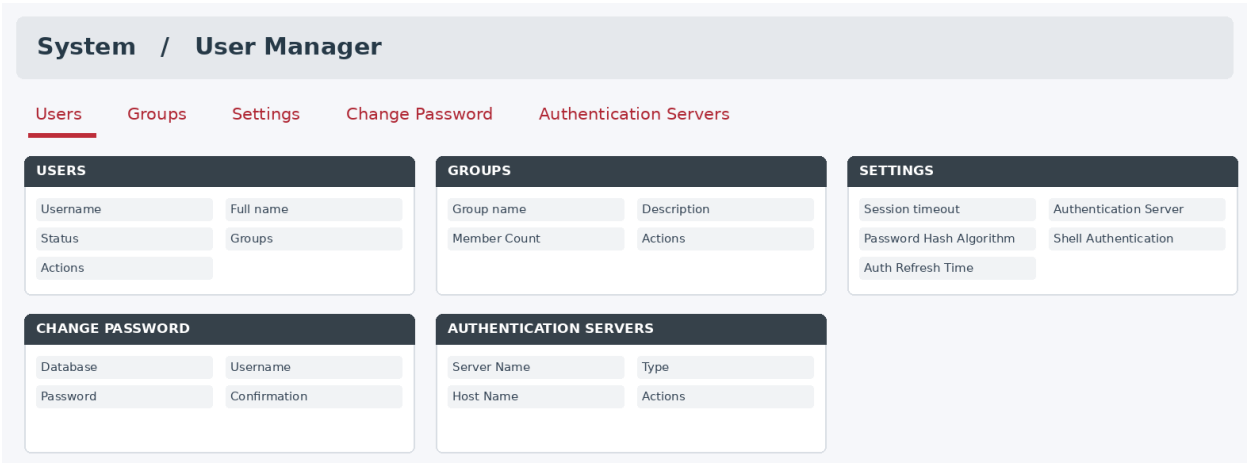


Figura 23.1. Estructura general de User Manager. Los paneles están representados sin información de usuarios ni servidores.

Pestaña	¿Qué permite gestionar?
Users	Cuentas locales, estado, membresías y privilegios efectivos.
Groups	Conjuntos reutilizables de usuarios y permisos.
Settings	Política de sesión, autenticación y hash de contraseñas.
Change Password	Cambio de contraseña de la cuenta local actual.
Authentication Servers	Definiciones de servidores LDAP y RADIUS para autenticación externa.

23.2. Users: lectura de la pantalla principal

La pestaña Users muestra una tabla con las cuentas locales registradas. No debe confundirse con un listado íntegro de usuarios de un dominio externo: en autenticación remota puede ser necesario conservar cuentas o grupos locales de referencia para asignar permisos.

Columna o control	Interpretación y utilidad
Casilla de selección	Permite seleccionar cuentas para una operación colectiva cuando la interfaz lo admita; antes de eliminar, comprobar dependencias y privilegios.
Username	Identificador utilizado para iniciar sesión; no implica por sí solo permiso de GUI, VPN o SSH.
Full name	Nombre descriptivo o función administrativa, con utilidad documental.

Columna o control	Interpretación y utilidad
Status	Permite reconocer si la cuenta figura activa o inhabilitada; verificar siempre la ficha en caso de duda.
Groups	Grupos a los que pertenece la cuenta; los permisos pueden heredarse de ellos.
Actions · lápiz	Abre la edición de la cuenta seleccionada.
Add	Inicia el alta de una cuenta nueva.
Delete	Solicita la eliminación de cuentas seleccionables; verificar antes el impacto en servicios y certificados vinculados.
PROTECCIÓN DEL SISTEMA La cuenta integrada «admin» no puede eliminarse ni renombrarse. No se recomienda utilizar un único usuario compartido para todas las tareas administrativas.	

23.3. Alta y edición de usuarios: campos y permisos

El formulario Add permite crear usuarios y definir sus opciones. Los campos y permisos disponibles dependen de la versión y del método de autenticación; la documentación de Netgate permite contrastar las opciones de cada instalación.

Campo del formulario	Uso administrativo
Disabled	Inhabilita temporalmente la cuenta sin borrar su configuración.
Username	Nombre de inicio de sesión. En cuentas locales, el identificador admite hasta 16 caracteres con las restricciones descritas por Netgate.
Password / Confirm Password	Establecen y confirman el secreto de acceso; no se almacenan en claro sino como hash con sal.
Full Name	Descripción legible de la cuenta.
Expiration Date	Caducidad opcional de la cuenta; útil para accesos temporales.
Group Memberships	Asignación de grupos y, por tanto, herencia de permisos.
Effective Privileges	Vista de los privilegios directos o heredados; se presenta al editar una cuenta ya creada.
Certificates	Permite emitir o vincular certificados asociados a usuarios, según la CA disponible.
Authorized SSH keys	Claves públicas autorizadas para acceso SSH/SCP, si la cuenta posee permisos pertinentes.
Keep Command History	Conservación del historial de comandos de un usuario con shell.
IPsec Pre-Shared Key	Parámetro específico para determinados métodos IPsec heredados; no habilita por sí solo IKEv2 o XAuth.

Una cuenta nueva se guarda primero y después se revisan sus privilegios. Netgate indica que los privilegios solo pueden añadirse a usuarios o grupos que ya existen; es preferible asignarlos a un grupo si varias personas necesitan el mismo perfil.

01. Abrir System → User Manager → Users y elegir Add.
02. Definir la cuenta, una contraseña robusta y, si procede, una fecha de expiración.
03. Guardar la cuenta y volver a editarla.
04. Asignar la pertenencia al grupo apropiado y revisar Effective Privileges.
05. Comprobar el inicio de sesión con esa cuenta, idealmente desde una sesión distinta, sin cerrar la sesión de administración de respaldo.

23.4. Groups: lectura de la pantalla y modelo de permisos

Los grupos reúnen privilegios asignables a varias cuentas y reducen errores de mantenimiento. Las entradas integradas «all» y «admins» forman parte de pfSense; no pueden eliminarse.

Columna / acción	Explicación práctica
Group name	Identificador del grupo. Para directorios externos debe corresponder con el nombre esperado por el sistema de autenticación.
Description	Descripción administrativa de la finalidad del grupo.
Member Count	Número de miembros asociados al grupo; no indica el número de sesiones abiertas.
Actions · lápiz	Permite editar miembros, configuración y privilegios del grupo.
Actions · copia	Crea una copia cuando la acción está disponible en esa fila; revisar el resultado antes de guardar.
Add	Abre el formulario para crear un nuevo grupo.

En los grupos, el ámbito **Local** permite usos del sistema operativo; el ámbito **Remote** se utiliza para grupos vinculados a fuentes como LDAP o RADIUS. El origen remoto no concede permisos mágicamente: pfSense debe reconocer el nombre del grupo y tener asignados los privilegios locales adecuados.

MÍNIMO PRIVILEGIO Evitar conceder «WebCfg - All Pages» cuando el trabajo puede realizarse con permisos específicos de diagnóstico, monitorización o gestión de VPN. Los permisos heredados no se retiran editando solo una cuenta: deben revisarse en el grupo que los concede.

23.5. Crear un grupo y delegar tareas

1. Abrir Groups y seleccionar Add.
2. Definir nombre, descripción y el ámbito Local o Remote según corresponda.
3. Guardar el grupo y volver a abrir su ficha.
4. Asignar únicamente los privilegios necesarios en Assigned Privileges.
5. Incorporar miembros y verificar Effective Privileges de las cuentas afectadas.
6. Iniciar una sesión de prueba para asegurar que los menús visibles coinciden con el perfil de trabajo.

Algunos privilegios de especial relevancia son «WebCfg - All Pages», «WebCfg - Dashboard (all)», «WebCfg - System: User Password Manager», «User - Config - Deny Config Write» y «User - System - Shell account access». La restricción de escritura de configuración no impide todas las acciones operativas; siempre hay que evaluar cada permiso por separado.

23.6. Settings: configuración de sesiones y autenticación

Esta pestaña configura el comportamiento del inicio de sesión y la validación de identidades. Su alcance es superior al de una cuenta individual: cambiar el servidor de autenticación o la duración de sesión puede afectar a varios administradores simultáneamente.

Campo visible	Función, significado y precauciones
Session timeout	Tiempo máximo de inactividad de una sesión web, en minutos. Referencia documentada: 240 min. El valor 0 evita la expiración y crea un riesgo en terminales desatendidos.
Authentication Server	Selecciona la fuente primaria para entrar a la GUI: Local Database o un servidor LDAP/RADIUS configurado. Existe retorno a la base local cuando la autenticación remota falla; conviene verificarlo antes de depender de él.
Password Hash Algorithm	Define el algoritmo de hash para contraseñas locales nuevas o modificadas. Las opciones mostradas son bcrypt y SHA-512-based crypt; bcrypt presenta un límite de 72 caracteres.
Shell Authentication	Permite usar el servidor de autenticación seleccionado también para SSH/consola. Requiere privilegios y preparación correctos de cuentas o grupos.
Auth Refresh Time	Intervalo de caché de resultados, expresado en segundos. Referencia documentada: 30 s por defecto y 3600 s como máximo.
Save	Guarda los valores establecidos.
Save & Test	Guarda y ejecuta la comprobación prevista por la interfaz; confirmar resultado y revisar logs si aparece error.

Campo visible	Función, significado y precauciones
ACLARACIÓN SOBRE HASH Bcrypt y SHA-512-based crypt son dos métodos distintos de almacenar hashes de contraseñas, no cifrado reversible. La documentación de Netgate considera bcrypt más resistente en este contexto; seleccionar el método exige tener en cuenta políticas, compatibilidad y la longitud admitida.	

23.7. Sesiones: equilibrio entre seguridad y operación

Una sesión excesivamente larga eleva el riesgo de acceso desde un navegador dejado abierto. Una sesión demasiado corta puede interrumpir tareas de mantenimiento. La política adecuada depende del nivel de exposición del puesto de administración y de las medidas de bloqueo automático del equipo.

- La expiración de la sesión web no sustituye el cierre de sesión manual, la seguridad del sistema operativo ni el control físico de la consola.
- La caché Auth Refresh Time afecta a la frecuencia con la que se revalidan credenciales remotas: valores más bajos incrementan consultas y reducen el periodo de permanencia de resultados cacheados.
- Antes de cambiar Authentication Server, mantener probada una vía de recuperación mediante la cuenta local y acceso de consola autorizado.

23.8. Change Password: modificación de credenciales locales

La pantalla User Password Manager permite modificar la contraseña de la cuenta que ha iniciado sesión, siempre que pertenezca a Local Authentication. No cambia contraseñas que estén almacenadas en LDAP, RADIUS u otros servidores externos.

Campo	Significado
Database	Identifica la fuente de autenticación local a la que afecta el cambio.
Username	Identifica la cuenta actual; es un dato mostrado por la interfaz, no una clave.
Password	Nueva contraseña para la cuenta.
Confirmation	Repetición obligatoria para evitar errores de escritura.
Save	Guarda el cambio de credencial.

01. Acceder a User Manager → Change Password.
02. Introducir una contraseña nueva, única y suficientemente larga.
03. Repetirla en Confirmation y guardar.
04. Comprobar el acceso con la nueva credencial desde otra sesión antes de cerrar la sesión vigente.
05. Actualizar de forma segura el registro de credenciales autorizado y revisar servicios dependientes.

REQUISITO DE SEGURIDAD La contraseña no puede coincidir con el nombre de usuario ni con el valor predeterminado de fábrica. El formulario de autoservicio no altera las contraseñas de cuentas LDAP o RADIUS.

23.9. Authentication Servers: lectura de la pantalla

Esta pestaña presenta los orígenes de autenticación definidos para el firewall. La tabla visible contiene Server Name, Type, Host Name y Actions; el botón Add permite crear una nueva definición. La entrada Local Database es la fuente local integrada.

Elemento	Uso
Server Name	Nombre administrativo de la fuente de autenticación.
Type	Tipo de autenticación cuando procede: LDAP o RADIUS; la base local es una opción especial.
Host Name	Identificador del servidor o destino al que debe conectarse pfSense; nunca necesita publicarse en documentación de terceros.

Elemento	Uso
Actions	Controles de administración presentes según el tipo de entrada; las fuentes integradas pueden tener restricciones.
Add	Abre el formulario de nueva fuente LDAP/RADIUS.

23.10. LDAP y RADIUS: elegir la tecnología adecuada

Criterio	LDAP	RADIUS
Uso frecuente	Consultar usuarios, grupos y pertenencias en un directorio.	Centralizar decisiones de autenticación y contabilidad según el servicio.
Contexto	Directorios como Active Directory, OpenLDAP o FreeIPA.	Infraestructuras AAA, VPN y acceso de red.
Transporte y protección	Preferir SSL/TLS o STARTTLS y validar el certificado del servidor.	Proteger el transporte y los secretos compartidos; considerar arquitectura y encapsulamiento utilizado.
Permisos de GUI	Se requieren grupos/cuentas locales equivalentes para asignar privilegios.	Se requieren cuentas locales con el mismo nombre y permisos esperados para GUI.
Diagnóstico	DNS, certificados, CA, búsquedas, contenedores y grupos.	Conectividad, secreto compartido, puertos, timeout y política AAA.

En LDAP, la identidad del certificado debe corresponder al nombre del servidor; el uso de TLS no implica que la validación sea correcta si falta la CA. RADIUS suele emplear puertos UDP 1812 (autenticación) y 1813 (contabilidad), aunque la configuración real depende del proveedor.

Authentication Servers presenta el inventario de servidores de autenticación. Los parámetros de LDAP y RADIUS se configuran en sus formularios de alta o edición, que se explican a continuación.

23.11. Procedimiento general para incorporar autenticación externa

01. Verificar conectividad, DNS y sincronización horaria entre el firewall y el servicio remoto.

02. Crear un respaldo de configuración y conservar una cuenta local de recuperación.

03. Abrir Authentication Servers → Add, seleccionar LDAP o RADIUS y completar los parámetros correspondientes.

04. En LDAP cifrado, importar previamente la CA de confianza y validar nombre de host, certificado y modo de conexión.

05. Guardar la definición y realizar una prueba con Diagnostics → Authentication.

06. Crear los usuarios o grupos locales equivalentes que sean necesarios para conferir permisos a la GUI.

07. Seleccionar el Authentication Server en Settings y comprobar acceso con una cuenta limitada.

08. Verificar registros y confirmar el acceso de recuperación local antes de cerrar sesiones existentes.

NO CONFUNDIR PRUEBA CON AUTORIZACIÓN Una prueba satisfactoria en Diagnostics → Authentication indica que las credenciales fueron aceptadas por el origen probado. No demuestra por sí sola que el usuario tenga privilegios de GUI o acceso a una VPN determinada.

23.12. Cinco escenarios de diagnóstico

Síntoma	Qué comprobar
Una cuenta valida credenciales pero no ve menús	Privilegios directos, grupos locales reconocidos y derechos efectivos; no equivale a fallo de contraseña.
No responde LDAP	Ruta, DNS, puerto y TLS, vigencia del certificado, CA importada, contenedores y credenciales de consulta.
RADIUS autentica pero el usuario no administra	Coincidencia del nombre con una cuenta local y privilegios asociados.

Síntoma	Qué comprobar
Una sesión se desconecta con demasiada frecuencia	Session timeout, actividad de sesión, políticas del navegador y Auth Refresh Time si se usan servidores remotos.
Cambiar contraseña local no afecta al dominio	La contraseña externa se mantiene en el directorio o servidor RADIUS correspondiente.

23.13. Buenas prácticas y revisión periódica

- Mantener cuentas nominativas para administración y evitar compartir credenciales.
- Aplicar mínimos privilegios mediante grupos y limitar especialmente acceso total a la GUI o a la consola.
- Desactivar o caducar cuentas que ya no necesitan acceso; revisar si sus certificados o permisos VPN continúan vigentes.
- Documentar decisiones sobre servidores externos, sin registrar contraseñas, secretos RADIUS, claves privadas o DN sensibles en documentos públicos.
- Verificar acceso administrativo de emergencia, respaldos y procedimientos de recuperación en una ventana de mantenimiento.
- Revisar registros de autenticación para distinguir problemas de contraseña, disponibilidad y autorización.
- Si un cambio de grupo no se refleja, revisar pertenencia, nombre exacto del grupo remoto, fuente seleccionada, caché y sesión nueva.

23.14. Lista de comprobación del administrador

Control de verificación	Resultado esperado
Cuentas de administración	Solo cuentas necesarias, diferenciadas y con privilegios justificados.
Grupos	Permisos coherentes, sin herencias excesivas ni denominaciones remotas ambiguas.
Caducidad de sesión	Valor razonable; desaconsejado 0 salvo necesidad excepcional documentada.
Contraseñas locales	Credenciales robustas y mecanismo hash elegido de forma consciente.
LDAP / RADIUS	Fuente probada, permisos coherentes y acceso de recuperación disponible.
Acceso SSH	Solo cuentas explícitamente autorizadas; métodos de autenticación verificados.
Auditoría	Registros, altas, bajas y cambios comprobados.

23.15. Referencias técnicas

Netgate Documentation · User Management and Authentication: https://docs.netgate.com/pfsense/en/latest/usermanager/index.html

Manage Local Users: https://docs.netgate.com/pfsense/en/latest/usermanager/users.html

Manage Local Groups / Privileges: https://docs.netgate.com/pfsense/en/latest/usermanager/groups.html · https://docs.netgate.com/pfsense/en/latest/usermanager/privileges.html

User Manager Settings / User Password Manager: https://docs.netgate.com/pfsense/en/latest/usermanager/settings.html · https://docs.netgate.com/pfsense/en/latest/usermanager/changepassword.html

Authentication Servers / Troubleshooting: https://docs.netgate.com/pfsense/en/latest/usermanager/authentication-servers.html · https://docs.netgate.com/pfsense/en/latest/troubleshooting/authentication.html

La nomenclatura de los controles corresponde a las pantallas documentadas. Las opciones adicionales se han separado y contextualizado conforme a la documentación pública de Netgate; su presencia concreta puede variar entre versiones de pfSense Plus.

Parte II Interfaces

24 Interfaces → Introducción general

Asignaciones, conmutación integrada y configuración de interfaces de red

Ruta principal: Interfaces | Accesos habituales: Assignments · Switches (según hardware) · WAN · LAN · Interfaces adicionales



Figura 24.1. Representación del menú Interfaces sin valores, nombres propios ni configuración de ningún entorno.

24.1. Introducción: por qué las interfaces son la base del firewall

Una interfaz es el punto por el que pfSense Plus se conecta a una red física o lógica. A través de ella recibe y envía paquetes, aplica reglas de filtrado, participa en el encaminamiento y, cuando corresponde, proporciona servicios como DHCP o facilita la traducción de direcciones mediante NAT.

El menú Interfaces reúne dos tareas diferentes: asignar recursos de red a funciones lógicas y configurar el comportamiento de cada interfaz. Separar ambas tareas evita errores: asignar un puerto no equivale a dotarlo de conectividad ni a permitir todo el tráfico.

Idea clave. Cada red conectada puede tener políticas, direccionamiento y servicios propios. La función WAN, LAN u OPT no depende únicamente del texto del nombre que aparece en el menú.

24.2. Cómo se organiza el menú Interfaces

Entrada	Qué permite hacer	Cuándo resulta útil
Assignments	Vincular puertos físicos o interfaces virtuales con entradas lógicas del firewall; administrar tipos de interfaces adicionales.	Ampliar redes, crear VLAN, sustituir adaptadores o reorganizar asignaciones.
Switches	Administrar puertos y características del conmutador integrado, cuando el dispositivo dispone de uno.	Separar o agrupar puertos y revisar VLAN internas en hardware compatible.
WAN	Configurar la interfaz que habitualmente conecta con el proveedor o una red de tránsito.	Revisar conexión ascendente, IPv4/IPv6 y parámetros de enlace.
LAN	Configurar una interfaz destinada habitualmente a usuarios y sistemas internos.	Administrar red interna y acceso a servicios locales.
OPTx / adicionales	Configurar redes o enlaces extra asignados al equipo, con nombres personalizables.	Crear zonas separadas, enlaces adicionales o segmentos para servicios.

La relación exacta de entradas varía según la plataforma y las interfaces creadas. La documentación oficial de Netgate indica que el menú utiliza los nombres configurados por el administrador y que Switches solo aparece en determinadas plataformas con conmutador integrado.

24.3. Assignments: una interfaz física no es necesariamente una red

El sistema detecta adaptadores Ethernet y otros dispositivos, pero el administrador decide qué papel tendrá cada uno. En Interfaces → Assignments se relaciona un recurso de red con una interfaz lógica identificada habitualmente como WAN, LAN u OPT. También pueden intervenir interfaces virtuales como VLAN, LAGG o PPP, dependiendo de la configuración.

Los tres conceptos que conviene diferenciar

Concepto	Qué representa	Qué no implica por sí solo
Puerto físico	Conector y controlador de red identificado por el sistema operativo.	Una dirección IP, una regla que permita tráfico o un servidor DHCP.
Interfaz virtual	Recurso lógico construido sobre otra tecnología o interfaz, por ejemplo VLAN o LAGG.	Un puerto físico exclusivo.
Interfaz asignada	Entrada que pfSense presenta y permite configurar mediante el menú.	Que esté habilitada, conectada o correctamente encaminada.

Una nueva asignación suele recibir un nombre OPT correlativo hasta que se le asigna una descripción más clara. Crear una VLAN y asignarla es distinto de crear una red en un conmutador gestionable: ambas partes deben tratar el etiquetado de forma compatible.

Precaución de administración. Modificar la asignación del puerto que sostiene la sesión de gestión puede cortar el acceso al webConfigurator. Antes de una reasignación conviene disponer de consola local o acceso alternativo de recuperación.

24.4. Switches: una opción dependiente del equipo

En ciertos dispositivos de Netgate, varios conectores visibles corresponden a un conmutador Ethernet integrado. Interfaces → Switches permite administrar su comportamiento, pero las pestañas, nombres de puerto y funciones varían por modelo.

El conmutador puede utilizar VLAN internas para aislar puertos que aparentan ser independientes. Por ello, cambiar la pertenencia a una VLAN o la configuración de un puerto puede provocar que una interfaz deje de llegar a la red esperada incluso aunque su configuración IP no haya cambiado.

Aspecto	Regla de lectura
Puerto de switch	Es el conector físico del conmutador; puede mapearse a una VLAN interna.
VLAN del switch	Determina cómo conmuta o etiqueta tramas el hardware; no equivale necesariamente a la VLAN creada en Assignments.
Interfaz pfSense	Es la entrada lógica del firewall que procesa tráfico de una red o VLAN.
Disponibilidad	Switches no aparece en todo hardware. Si no existe, no debe interpretarse como un error.

24.5. WAN, LAN y OPT: nombres útiles, no garantías de función

WAN y LAN son convenciones de administración. WAN suele designar una red ascendente y LAN una red de confianza interna. OPT identifica interfaces adicionales que pueden actuar como redes internas, zonas expuestas de servicios (DMZ), conexiones entre equipos o nuevos enlaces de salida.

La diferencia operativa entre tipos WAN y LAN afecta a determinadas funciones, entre ellas NAT IPv4. Según Netgate, en interfaces con direcciones estáticas la presencia de un gateway ascendente influye en esa clasificación; las interfaces dinámicas, como DHCP y PPP, tienen particularidades propias. Por eso no basta con renombrar una interfaz para cambiar su comportamiento.

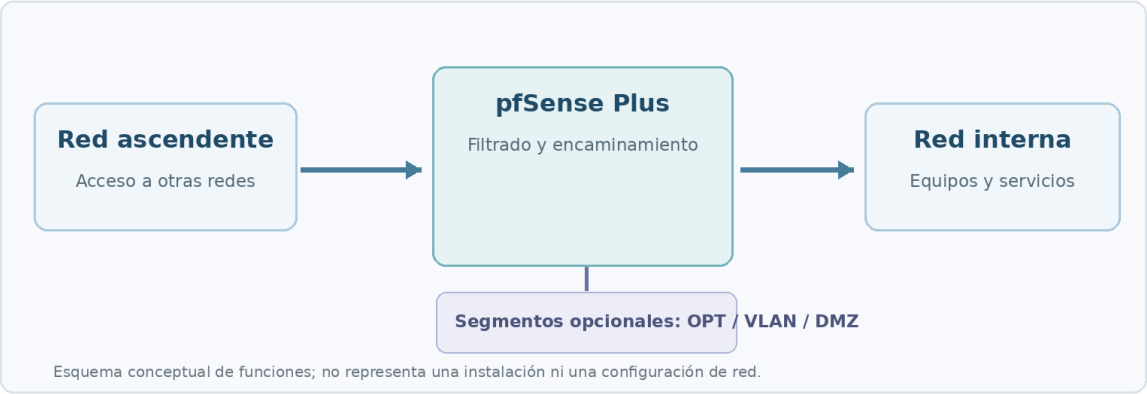


Figura 24.2. Relaciones funcionales entre redes e interfaces. Esquema conceptual sin topología, direcciones ni datos reales.

Escenarios habituales

Necesidad	Función de interfaces	Qué revisar además
Conexión ascendente	Una interfaz configurada con el tipo de conexión exigido por el enlace.	Gateway, rutas, DNS y, en su caso, NAT.
Red de usuarios	Una interfaz interna con direccionamiento coherente.	Reglas, DHCP si procede y acceso de administración.
Segmento independiente	Interfaz adicional física o lógica.	Aislamiento, VLAN, reglas y servicios.
Conexión secundaria	Otra interfaz configurada para un segundo enlace.	Gateway monitorizado y grupo de gateways si se necesita failover.

24.6. Qué encontraremos al abrir una interfaz

Las páginas individuales de interfaz comparten muchos controles, aunque muestran campos adicionales según el tipo de IPv4 o IPv6 seleccionado y las características del hardware. En sus formularios se encuentran habitualmente los siguientes bloques de decisión:

Familia de opciones	Finalidad	Precaución
Enable / Description	Habilitar y denominar claramente la interfaz.	Un nombre nuevo no cambia por sí solo el cableado ni las reglas.
IPv4 / IPv6 Configuration Type	Seleccionar métodos de direccionamiento tales como estático o dinámico.	Cambiar el método puede alterar la IP y cortar la sesión.
Gateway ascendente	Indicar el siguiente salto cuando el tipo de interfaz lo admite.	No configurarlo de manera incorrecta en una red interna.
MTU / MSS	Ajustar tamaños de transmisión y segmentos TCP cuando procede.	Usar valores especiales solo con una causa identificada.
Speed / Duplex	Gestionar la negociación del enlace físico si la interfaz lo permite.	Evitar modos forzados incompatibles entre extremos.
Protecciones de red	Filtrado de redes privadas y bogon en escenarios apropiados.	No activar indiscriminadamente en enlaces con redes privadas legítimas.

La creación de una interfaz no abre automáticamente los accesos que necesitarán los clientes. El funcionamiento completo suele involucrar también Firewall → Rules, System → Routing y las páginas de servicios correspondientes.

24.7. Primera inspección práctica del menú, sin modificar nada

01. Abrir Interfaces y enumerar visualmente las entradas de asignación, switch integrado (si existe) e interfaces configuradas.

02. Entrar en Assignments y reconocer la diferencia entre recursos de red detectados e interfaces ya asignadas. No cambiar aún su correspondencia.

03. Consultar una interfaz desde el menú y reconocer su estado de habilitación, descripción y tipo de configuración IPv4/IPv6.

04. Revisar Status → Interfaces para distinguir «enlace activo» de «conectividad validada».

05. Identificar en qué otras páginas se controlan las rutas, las reglas y los servicios de esa interfaz.

06. Registrar los hallazgos en la documentación operativa autorizada, sin exportar identificadores ni valores sensibles a materiales de formación.

Comprobación orientada a resultados

Pregunta	Dónde comprobarla	Interpretación correcta
¿Existe la interfaz?	Interfaces → Assignments	Asignación lógica presente; aún no confirma que tenga conectividad.
¿Está enlazada?	Status → Interfaces	Estado físico/lógico; no implica acceso a otros segmentos.
¿Tiene ruta de salida?	System → Routing / Diagnostics	La ruta y su siguiente salto deben ser coherentes.
¿Se permite el tráfico?	Firewall → Rules / Logs	Se aplican las reglas según el sentido y la interfaz de entrada.
¿Se presta el servicio esperado?	Services y diagnósticos correspondientes	No asumir que DHCP o DNS están activos por configurar una IP.

24.8. Errores frecuentes y prevención

Síntoma	Causa posible	Primera actuación segura
Desaparece el acceso a la GUI	Cambio de asignación, dirección, VLAN o reglas.	Usar ruta de gestión alternativa o consola; revisar el último cambio.
La interfaz figura Up, pero no hay tráfico	Gateway, regla, ruta de retorno, VLAN o servicio ausente.	Separar pruebas de enlace, puerta de enlace y aplicación.
No se ve Switches	Hardware sin conmutador administrable desde pfSense.	Consultar la documentación del equipo, no buscar una instalación adicional.
Un enlace ascendente no pasa tráfico	Dirección IP correcta pero sin ruta, NAT o reglas adecuadas.	Revisar Status → Interfaces, gateways y registros.
Dos redes no se comunican	Falta de regla, direccionamiento o ruta de retorno.	Verificar trayecto completo sin abrir reglas indiscriminadas.
Criterio profesional. Antes de editar interfaces de producción: copia de configuración, acceso de recuperación, ventana de cambio y plan de reversión. Priorizar la lectura y la verificación frente a cambios de prueba.		

24.9. Resumen operativo

Interfaces define las entradas y salidas lógicas del firewall; Assignments las relaciona con puertos y dispositivos, Switches administra determinadas funciones del conmutador integrado, y las entradas WAN, LAN u OPT abren la configuración de cada interfaz. La conectividad efectiva depende también de rutas, NAT, reglas y servicios. Comprender esta separación facilita ampliar la red sin perder control ni seguridad.

Referencias técnicas

Netgate. Interfaces — guía del menú: https://docs.netgate.com/pfsense/en/latest/menuguide/interfaces.html

Netgate. Interface Configuration: https://docs.netgate.com/pfsense/en/latest/interfaces/configure.html

Netgate. WAN vs LAN Interfaces: https://docs.netgate.com/pfsense/en/latest/interfaces/wanvslan.html

Netgate. Integrated Switches: https://docs.netgate.com/pfsense/en/latest/interfaces/switches.html

Netgate. Interface Naming Terminology: https://docs.netgate.com/pfsense/en/latest/general/interface-names.html

25 Interfaces → Assignments

Asignación de puertos, grupos, VLAN y tecnologías de interfaces virtuales

Ruta principal: Interfaces → Assignments | Pestañas: Interface Assignments · Interface Groups · Wireless · VLANs · QinQs · PPPs · GREs · GIFs · VXLANs · Bridges · LAGGs

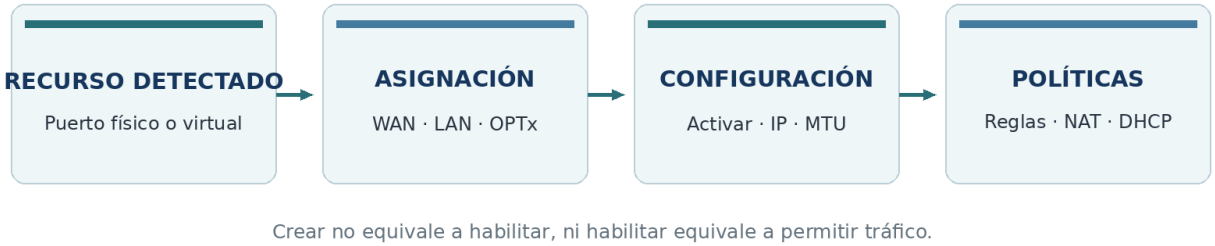


Figura 25.1. Secuencia funcional de una interfaz: recurso, asignación, configuración y política; representación íntegramente conceptual.

25.1. Objetivo y alcance operativo

La página Interface Assignments es el punto en el que pfSense Plus relaciona los dispositivos de red detectados por el sistema con interfaces lógicas utilizables por el firewall. Además de esta correspondencia, las pestañas de la página permiten administrar grupos de interfaces y definir recursos virtuales, como VLAN, enlaces agregados, puentes y túneles. No se trata de una sola operación: detectar, crear, asignar, habilitar, direccionar y autorizar tráfico son fases diferentes.

En la presente interfaz se observan once pestañas de administración. La vista principal muestra asignaciones existentes, selectores de puertos, botones Add, Delete y Save, y avisos contextualizados; las otras pestañas presentan listados por tipo con acciones de alta y, cuando hay entradas, edición o eliminación.

Criterio de lectura. Las tablas y los controles de listado se describen a partir de las pantallas de esta sección. Los campos de formularios Add/Edit que no aparecen en ellas se explican exclusivamente cuando están documentados por Netgate; no se presentan como si fueran visibles en la vista inicial.

25.2. Mapa de las once pestañas y su función

Pestaña	Función técnica	Resultado / diferencia
Interface Assignments	Relacionar puertos con WAN, LAN u OPTx.	Asignación lógica; la configuración se termina en Interfaces > [nombre].
Interface Groups	Aplicar reglas comunes a varias interfaces.	No crea un nuevo puerto ni un puente.
Wireless	Crear instancias inalámbricas compatibles.	Después deben asignarse y configurarse.
VLANs	Definir etiquetas IEEE 802.1Q sobre un padre.	Segmentos L2 lógicos sobre un mismo enlace.
QinQs	Crear doble etiquetado 802.1ad.	Transporte de VLAN con etiqueta exterior.
PPPs	Definir enlaces PPP y sus variantes.	Conexiones punto a punto, autenticación ISP.
GREs	Encapsulación GRE entre extremos.	Túnel L3 sin cifrado propio.
GIFs	Interfaz genérica de túnel.	Encapsulación, p. ej. IPv6 sobre IPv4.
VXLANs	Extender Ethernet L2 sobre UDP/IP.	Segmento identificado por VNI.

Pestaña	Función técnica	Resultado / diferencia
Bridges	Unir miembros en capa 2.	Un único dominio de difusión; riesgo de bucles.
LAGGs	Agrupar interfaces Ethernet físicas.	Redundancia y/o capacidad, según protocolo.

La ruta común para todas las pestañas es Interfaces → Assignments y, a continuación, el nombre de la pestaña. Los rótulos pueden presentarse en inglés aunque el resto del entorno tenga otro idioma. El detalle disponible depende del hardware, los paquetes instalados y la versión exacta de pfSense Plus.

25.3. Interface Assignments: asignación lógica de puertos

25.3.1. Lectura de las columnas y controles visibles

Elemento en pantalla	Interpretación y efecto
Interface	Nombre lógico asignado. Habitualmente WAN, LAN y OPTx, aunque los nombres visibles pueden personalizarse.
Nombre azul de la interfaz	Acceso a su configuración detallada (estado Enable, descripción, IPv4/IPv6 y parámetros particulares).
Network port	Selector que relaciona ese nombre lógico con una interfaz del sistema: física, VLAN o virtual compatible.
Lista de puertos disponibles	Muestra recursos no asignados; sus descriptores pueden incluir tipo, etiqueta, dispositivo o identificadores técnicos.
Add (icono +)	Incorpora el puerto seleccionado como una interfaz opcional nueva, normalmente OPT1, OPT2, etc.
Delete (papelera roja)	Elimina una asignación permitida, con efectos potenciales sobre reglas, direccionamiento y servicios ligados a ella.
Save (disquete azul)	Guarda los cambios realizados en los selectores de asignación existentes.
Aviso de LAGG	Los puertos que son miembros de un LAGG no aparecen como puertos libres asignables individualmente.
Aviso de Wireless	Es preciso crear previamente las instancias inalámbricas en Wireless para que aparezcan como asignables.

25.3.2. Qué ocurre al cambiar una asignación

Cambiar el puerto de una interfaz lógica no es una simple operación de etiquetado: se traslada la función lógica a otro dispositivo de red. El direccionamiento y las políticas asociados a WAN, LAN u OPT siguen vinculados al nombre lógico, pero el enlace físico o virtual que recibe el tráfico cambia. Si la gestión web entra por la interfaz afectada, la sesión puede perderse inmediatamente.

Los nombres WAN y LAN son convenciones. El tratamiento como interfaz de tipo WAN o LAN depende de la configuración del gateway, especialmente en interfaces con dirección estática; por ello no se debe deducir NAT, filtrado o confianza solo del nombre visible.

01. Identificar la función lógica que debe permanecer y el dispositivo de red destino; revisar el estado del enlace y la configuración del equipo adyacente.
02. Hacer copia de seguridad de la configuración y disponer de acceso alternativo por consola u otra interfaz no afectada.
03. Abrir Interfaces → Assignments y seleccionar el nuevo Network port de la fila correspondiente.
04. Confirmar que el resto de asignaciones conservan la correspondencia prevista; pulsar Save.
05. Comprobar acceso a la GUI, enlace físico, dirección IPv4/IPv6, rutas, reglas, NAT y servicios asociados antes de dar la modificación por válida.

Riesgo crítico. No cambiar la asignación de la interfaz desde la que se está administrando un firewall en producción sin una vía de recuperación independiente. Un selector incorrecto puede dejar sin acceso a la administración, al gateway o a una VPN.

25.3.3. Alta segura de una interfaz opcional

01. Crear primero el recurso virtual si se trata de una VLAN, túnel, bridge o LAGG. Una tarjeta física detectada puede estar disponible directamente.
02. Elegir el recurso en Available network ports y pulsar Add; identificar la nueva entrada OPTx.
03. Abrir Interfaces → OPTx y activar Enable si procede; asignar una descripción clara y configurar IPv4 e IPv6 apropiadamente.
04. Guardar y aplicar los cambios de interfaz cuando aparezca Apply Changes; configurar, según la necesidad, reglas en Firewall → Rules, servicios y rutas.
05. Verificar Status → Interfaces, probar tráfico autorizado y documentar únicamente la función de la nueva red.

Una interfaz creada y asignada puede no transportar tráfico útil: faltará habilitarla, direccionarla cuando corresponda, configurar el switch remoto si transporta VLAN y permitir explícitamente el tráfico requerido. La mera existencia de una fila no prueba que haya conectividad.

25.4. Interface Groups: reglas comunes entre interfaces

Columna / control	Qué informa o realiza
Name	Identifica el grupo de reglas.
Members	Muestra las interfaces incluidas en el grupo.
Description	Texto explicativo del propósito del grupo.
Actions: lápiz / papelera	Edita o elimina un grupo cuando la entrada lo permite.
Add (+)	Abre el formulario de creación.

Un grupo de interfaces es un mecanismo de organización del filtrado, no un bridge ni una interfaz encaminable. Desde la pestaña Firewall → Rules correspondiente al grupo es posible aplicar reglas comunes a sus miembros. Los grupos de interfaz no sustituyen el análisis de las reglas específicas de cada interfaz.

25.4.1. Campos del formulario de grupo, según Netgate

Campo documentado	Significado práctico
Group Name	Nombre del grupo; la documentación oficial de esta función indica solo letras, sin espacios, cifras ni símbolos.
Group Description	Anotación opcional del propósito.
Group Members	Lista de interfaces asignadas; admite selección múltiple con Ctrl o Cmd, según el sistema.
Save	Crea o actualiza el grupo de forma persistente.

25.4.2. Orden de evaluación y precauciones

Para reglas de usuario, el orden habitual es: reglas flotantes (según su comportamiento Quick) → reglas del grupo de interfaz → reglas propias de la interfaz. Una coincidencia en una regla de grupo puede impedir que se consulte una regla más específica de la interfaz; por ejemplo, un bloqueo general del grupo no se solventa con una regla posterior de permiso en la pestaña individual.

No es recomendable agrupar varias WAN para aplicarles reglas de entrada genéricas: las reglas en grupos no reciben el mismo comportamiento de reply-to que las reglas en pestañas WAN, lo que puede romper retornos en escenarios multi-WAN.

Grupos gestionados por paquetes. Si aparece un grupo creado para un paquete VPN, como WireGuard, no debe editarse ni eliminarse manualmente sin consultar las instrucciones del paquete. Su composición puede gestionarse desde los ajustes específicos de la VPN.

01. Crear un grupo solo si varias interfaces comparten realmente una misma política.

02. Definir nombre, descripción y miembros, y guardar.
03. Crear las reglas bajo Firewall → Rules → [grupo].
04. Comprobar orden y coincidencias con reglas flotantes y reglas particulares.
05. Validar los flujos permitidos y denegados desde cada interfaz del grupo.

25.5. Wireless: instancias inalámbricas

Columna / acción	Lectura de la lista
Interface	Instancia inalámbrica definida, si hay hardware y controladores compatibles.
Mode	Modo de funcionamiento de cada instancia.
Description	Anotación administrativa.
Actions / Add	Acciones de mantenimiento y creación de entradas; con lista vacía solo se observa Add.

La vista puede aparecer vacía sin que ello constituya un error: debe existir hardware inalámbrico compatible y un controlador que admita la función. Netgate documenta la creación de instancias Virtual Access Point (VAP), que permiten varias identidades inalámbricas sobre un mismo adaptador cuando este lo soporta.

25.5.1. Alta documentada de una instancia

Campo al pulsar Add	Uso y límites
Parent Interface	Adaptador inalámbrico compatible sobre el que se construye la instancia.
Mode	Access Point; Infrastructure (BSS, cliente); Ad-hoc (IBSS), según soporte.
Description	Identificación funcional de la instancia.
Save	Guarda la instancia para que posteriormente pueda asignarse en Interface Assignments.

Después de guardar, seleccionar la instancia en Available network ports, agregarla como OPTx, habilitarla y completar los ajustes inalámbricos de modo, SSID y seguridad desde su propia página. La modalidad usada tras la asignación debe ser coherente con el Mode definido al crearla.

Si el adaptador es incompatible, un intento de crear varias instancias puede fallar o provocar inestabilidad. En redes empresariales suele resultar más operativo utilizar puntos de acceso dedicados y limitar pfSense a enrutamiento y políticas, salvo necesidad específica.

Alcance. La pestaña mostrada es un listado; parámetros como SSID, canal, autenticación o clave no están presentes en esa pantalla y no deben confundirse con sus columnas.

25.6. VLANs: segmentación mediante etiquetado 802.1Q

Columna / acción	Significado
Interface	Dispositivo padre que transporta el etiquetado; puede ser físico o compatible con VLAN.
VLAN tag	Identificador numérico VLAN.
Priority	Prioridad 802.1p/PCP, si se establece.
Description	Nombre funcional de la VLAN, independiente del identificador numérico.
Actions / Add	Editar, eliminar o crear definiciones VLAN.

25.6.1. Campos confirmados por Netgate en Add/Edit VLAN

Campo	Uso, efecto y precaución
Parent Interface	Puerto o interfaz sobre la que viajarán las tramas etiquetadas. Debe estar coordinada con el equipo vecino.

Campo	Uso, efecto y precaución
VLAN Tag Type	C-Tag (0x8100) para 802.1Q habitual; S-Tag (0x88a8) cuando se requiere etiquetado de servicio.
VLAN Tag	VID 1–4094. Debe coincidir con la segmentación diseñada en ambos extremos.
VLAN Priority	PCP 0–7, si se especifica; afecta a la prioridad de marcado L2, no garantiza calidad de servicio extremo a extremo.
Description	Etiqueta documental de la función de red.
Save	Guarda la interfaz VLAN virtual; todavía puede requerir asignación en Interface Assignments.

La VLAN divide dominios de difusión sin requerir una tarjeta de red física para cada segmento. En el switch deben habilitarse las VLAN correspondientes en el puerto troncal, con etiquetado coherente y un criterio claro para tráfico sin etiqueta (untagged). En un escenario de ejemplo completamente genérico pueden crearse VLAN 100 y VLAN 200 sobre un puerto de laboratorio, sin que estos valores describan ningún sistema real.

El campo Priority no debe confundirse con el orden de reglas del firewall. PCP identifica prioridad de trama IEEE 802.1p y puede ser interpretado o descartado por switches del trayecto.

01. Crear la VLAN en Interfaces → Assignments → VLANs → Add.
02. Seleccionar el Parent Interface y C-Tag para una VLAN 802.1Q ordinaria.
03. Establecer VLAN Tag, definir Priority solo cuando el diseño QoS lo requiera y escribir Description.
04. Guardar; regresar a Interface Assignments y asignar la VLAN desde Available network ports.
05. Habilitar y configurar la nueva interfaz lógica; comprobar reglas, DHCP si procede y etiquetado del puerto del switch.
06. Verificar que dispositivos del segmento obtienen conectividad según política y que el aislamiento entre VLAN es el previsto.

Precaución de migración. Si una VLAN existente debe trasladarse a otro padre, la guía de Netgate para migración a LAGG recomienda crear primero otra VLAN sobre el nuevo padre, cambiar la asignación y retirar después la antigua, en lugar de editar el padre de una VLAN asignada en servicio.

25.7. QinQs: doble etiqueta de VLAN (802.1ad)

Columna / acción	Interpretación
Interface	Interfaz padre que transporta QinQ.
Tag	Etiqueta exterior del servicio.
QinQ members	VLAN internas que forman parte de la definición.
Description	Descripción funcional.
Actions / Add	Mantenimiento y alta de entradas QinQ.

QinQ añade una etiqueta exterior, normalmente S-Tag, a tramas que ya contienen una etiqueta interior C-Tag. Es útil cuando un operador o un entorno de transporte debe mover varias VLAN de un cliente o de distintas redes lógicas a través de una conexión común. Depende de que la infraestructura intermediaria preserve ambas etiquetas y soporte los tamaños de trama resultantes.

25.7.1. Opciones del formulario documentado

Campo	Cuándo utilizarlo y efecto
Parent Interface	Puerto o interfaz por donde saldrá el doble etiquetado.
VLAN Tag Type	C-Tag 0x8100 o S-Tag 0x88a8; en QinQ típico la etiqueta exterior es S-Tag.
First level tag	VID correspondiente al nivel exterior.

Campo	Cuándo utilizarlo y efecto
Adds interface to QinQ interface groups	Al activarlo, puede crearse un grupo de reglas QinQ para sus subinterfaces; su administración automática no debe alterarse manualmente.
Description	Propósito operativo, sin identificadores externos.
Member(s)	VLAN internas; Netgate admite IDs sueltos y rangos y ofrece Add Tag para añadir más líneas.

01. Confirmar con la contraparte el tipo TPID, etiqueta exterior, etiquetas interiores y MTU.
02. Abrir la pestaña QinQs y pulsar Add; seleccionar padre, TPID y First level tag.
03. Introducir las VLAN Member(s) permitidas; activar el grupo automático solo si se van a centralizar reglas.
04. Guardar, revisar interfaces resultantes y establecer la política de filtrado requerida.
05. Comprobar transmisión bidireccional de los segmentos esperados y ausencia de pérdida por MTU o filtrado de etiquetas.

La casilla de creación de grupo de QinQ no cifra ni aísla por sí misma el tráfico: únicamente facilita una política de filtrado común. Desactivar esta opción significa no generar esa agrupación automática desde la definición; no suprime el etiquetado QinQ por sí solo.

25.8. PPPs: enlaces punto a punto y autenticación de acceso

Columna / acción	Significado
Interface	Identificador del dispositivo PPP cuando existe una definición.
Interface(s)/Port(s)	Enlaces o puertos asociados al PPP.
Description	Explicación administrativa.
Actions / Add	Editar entradas existentes o crear nuevas.

La pestaña PPPs administra conexiones de tipo PPP, PPPoE, PPTP y L2TP cuando la conexión WAN o el proveedor lo requieren. No debe confundirse con la configuración de una VPN de acceso remoto de usuario: aquí se está definiendo fundamentalmente el enlace de acceso. Un router celular que expone Ethernet puede configurarse como una interfaz ordinaria sin utilizar PPP.

25.8.1. Link Type y campos dependientes

Tipo / campo documentado	Finalidad
Link Type = PPP	Acceso mediante dispositivo serie o módem; selecciona el equipo mediante Link Interface.
PPP: Country, Provider, Plan	Ayudan a obtener valores de operador y perfil cuando existe soporte.
PPP: APN, APN Number, Phone Number	Parámetros de acceso celular o marcado, según proveedor y dispositivo.
PPP: SIM PIN, SIM PIN Wait	Desbloqueo SIM opcional y tiempo de inicialización; no completar si la SIM no utiliza PIN.
PPP: Init String, Connection Timeout	Inicialización del módem y espera máxima de conexión.
PPP: Uptime Logging	Si se activa registra tiempo de actividad visible en Status → Interfaces; desactivado no presenta esa contabilización específica.
Link Type = PPPoE	Conexión PPP sobre Ethernet, incluso sobre una VLAN soportada.
PPPoE: Link Interface(s)	Interfaz portadora de la sesión; selección múltiple únicamente para enlaces MLPPP compatibles.
PPPoE: Username, Password	Credenciales suministradas por el operador; nunca deben publicarse en documentación general.
PPPoE: Service Name / NULL Service Name	Comportamiento de identificador de servicio exigido por determinados ISP.

Tipo / campo documentado	Finalidad
PPPoE: Periodic Reset	Reconecta periódicamente la sesión al programarse; normalmente no es necesario.
Link Type = PPTP / L2TP	Métodos heredados de acceso de ISP; L2TP añade Shared Secret cuando el extremo lo necesita.

MLPPP agrega varios enlaces PPP cuando el proveedor admite ese servicio. No equivale a multi-WAN con rutas y gateway groups; exige circuitos compatibles del mismo proveedor y no es compatible con el backend if_pppoe señalado por Netgate. No se debe activar por el mero hecho de disponer de dos WAN.

01. Determinar si el proveedor realmente utiliza PPPoE, PPP u otra variante y qué interfaz transporta la sesión.
02. Pulsar Add en PPPs y elegir Link Type; completar únicamente las opciones presentadas para ese tipo.
03. Guardar la entrada y configurar la WAN correspondiente, su dirección, gateway y las opciones de enlace.
04. Comprobar autenticación y establecimiento en Status → Interfaces y en los registros PPP, sin copiar secretos a informes.
05. Verificar tráfico, latencia, MTU/MSS y recuperación tras un corte controlado.

Seguridad. No incorporar contraseñas, PIN ni Shared Secret en figuras, manuales, capturas publicables o informes de soporte no autorizados. Los fallos de PPPoE pueden deberse tanto a las credenciales como a la VLAN portadora o a la selección del puerto.

25.9. GREs: túneles genéricos de capa 3

Columna / acción	Lectura
Interface	Identificador de túnel creado.
Tunnel to ...	Extremo remoto del túnel; se omite cualquier valor concreto por seguridad editorial.
Description	Propósito del túnel.
Actions / Add	Editar, retirar o crear túneles GRE.

GRE (Generic Routing Encapsulation) permite transportar tráfico IP entre extremos lógicos. La encapsulación GRE por sí sola NO proporciona cifrado ni autenticación criptográfica; cuando circula sobre redes no confiables debe protegerse con otra tecnología adecuada o emplearse otra solución VPN segura.

25.9.1. Campos de creación descritos por Netgate

Campo	Uso / efecto
Parent interface	Interfaz sobre la que termina el túnel exterior.
Remote Address	Extremo remoto alcanzable a través de la red de transporte.
Local IPv4/IPv6 Tunnel Address	Dirección de extremo interno del túnel en el firewall.
Remote IPv4/IPv6 Tunnel Address	Dirección de extremo interno en el peer remoto; puede utilizarse como próximo salto.
IPv4/IPv6 Tunnel Subnet	Tamaño del segmento del enlace virtual.
Add Static Route	Al activarlo, agrega una ruta estática explícita asociada a las direcciones internas, útil si otras rutas elegirían un camino incorrecto.
Description / Save	Anotación y persistencia de la definición.

01. Comprobar previamente que las direcciones exteriores de ambos extremos pueden comunicarse y que su política permite GRE.
02. Definir Parent interface, Remote Address y parámetros internos coherentes en ambos extremos; añadir ruta explícita solo si procede.
03. Guardar la definición y asignar el túnel desde Interface Assignments como OPTx.
04. Habilitar la nueva interfaz; configurar las reglas, rutas, gateway y NAT necesarios para el diseño.

05. Probar llegada a los dos extremos interiores, después a redes remotas autorizadas y finalmente las aplicaciones empresariales.

Un túnel existente en la lista no implica que el extremo remoto conteste. La prueba debe separar conectividad de transporte, presencia de ruta y reglas de entrada del túnel. Es una tecnología de encapsulación, no un reemplazo directo de un enlace cifrado.

25.10. GIFs: interfaz genérica de túnel

Columna / acción	Lectura
Interface	Identificador de GIF.
Tunnel to ...	Extremo remoto documentado en la definición.
Description	Texto funcional.
Actions / Add	Crear, editar o eliminar instancias.

GIF (Generic tunnel InterFace) es otra familia de encapsulación utilizada en pfSense para transportar protocolos entre extremos. Un uso habitual es IPv6 sobre una red de transporte IPv4. GRE y GIF comparten el concepto de túnel, pero difieren en mecanismos, opciones e interoperabilidad, por lo que no deben intercambiarse sin analizar lo que admite el proveedor o la contraparte.

25.10.1. Campos documentados en Add/Edit GIF

Campo	Interpretación funcional
Parent interface	Interfaz exterior portadora del túnel.
GIF Remote Address	Dirección del extremo remoto en la red de transporte.
GIF tunnel local address	Dirección del extremo local dentro del túnel.
GIF tunnel remote address	Dirección del extremo remoto dentro del túnel.
GIF Tunnel Subnet	Prefijo del enlace; consultar particularidades del modo IPv6, que puede tener prefijo interno impuesto por el kernel.
ECN Friendly Behavior	Controla copia de información de congestión/TOS; activarla exige acuerdo entre extremos y valoración de interoperabilidad.
Outer Source Filtering	Afecta al tratamiento/validación de tráfico exterior y entornos con enrutamiento asimétrico; cambio avanzado con implicaciones de seguridad.
Description / Save	Anotación administrativa y persistencia.

01. Obtener los parámetros del servicio de túnel y confirmar protocolos interior y exterior.
02. Crear la entrada GIF sobre el padre adecuado con extremos exterior e interiores y prefijo requerido.
03. Mantener las opciones avanzadas en sus valores comprobados salvo necesidad de interoperabilidad documentada.
04. Guardar, asignar el recurso como interfaz y habilitarlo; preparar rutas y reglas necesarias.
05. Probar accesibilidad al extremo remoto y tránsito de IPv6/IPv4 según diseño, además de la MTU.

Precaución. No cambiar opciones relacionadas con filtrado del origen exterior para corregir fallos de rutas sin estudiar el motivo: pueden ampliar la superficie de exposición del túnel.

25.11. VXLANs: extensión de Ethernet por redes IP

Columna / acción	Qué expresa
Interface	Instancia VXLAN definida.
Tunnel to	VTEP de destino configurado.
Description	Propósito.
Actions / Add	Operaciones sobre la lista.

VXLAN (RFC 7348) encapsula tramas Ethernet de capa 2 sobre UDP/IP para extender un segmento lógico a través de una red IP subyacente (underlay). Cada segmento se identifica mediante un VNI de 24 bits. Es útil en entornos virtualizados o conexiones L2 entre sistemas compatibles, pero exige especial disciplina de MTU, rutas, duplicación de redes y seguridad.

25.11.1. Opciones documentadas por Netgate

Campo	Finalidad y comportamiento
Parent Interface	Interfaz exterior por la que circula UDP/IP.
VXLAN Remote Address	Dirección del VTEP remoto.
VXLAN ID	Identificador VNI, único entre las instancias que comparten extremos.
VXLAN Local Port	Puerto UDP de escucha; valor habitual predeterminado 4789.
VXLAN Remote Port	Puerto UDP de destino; normalmente 4789, pero ciertos sistemas usan 8472.
VXLAN TTL	Tiempo de vida del encapsulado IP; Netgate documenta por defecto 64.
VXLAN Learn	Activado: aprende asociaciones entre IP de origen exterior y MAC de origen interior de tramas recibidas; desactivado: no realiza ese aprendizaje dinámico.
Description / Save	Describe y guarda la instancia.

01. Comprobar alcanzabilidad IP entre VTEP y acuerdo en VNI y puertos UDP.
02. Crear VXLAN mediante Add y definir Parent Interface, Remote Address, VNI y parámetros UDP.
03. Revisar el comportamiento Learn según el diseño y guardar.
04. Asignar y/o integrar el VXLAN en un bridge solo si el diseño requiere realmente extensión L2, y aplicar política de filtrado.
05. Validar conectividad L2, tamaño de trama, ausencia de bucles y alcance únicamente a los VTEP previstos.

Riesgo de confidencialidad del tráfico. VXLAN no cifra los datos encapsulados. Netgate desaconseja transportar VXLAN sin protección por redes no fiables. Debe aislarse o protegerse el underlay y filtrarse el tráfico UDP entre extremos.

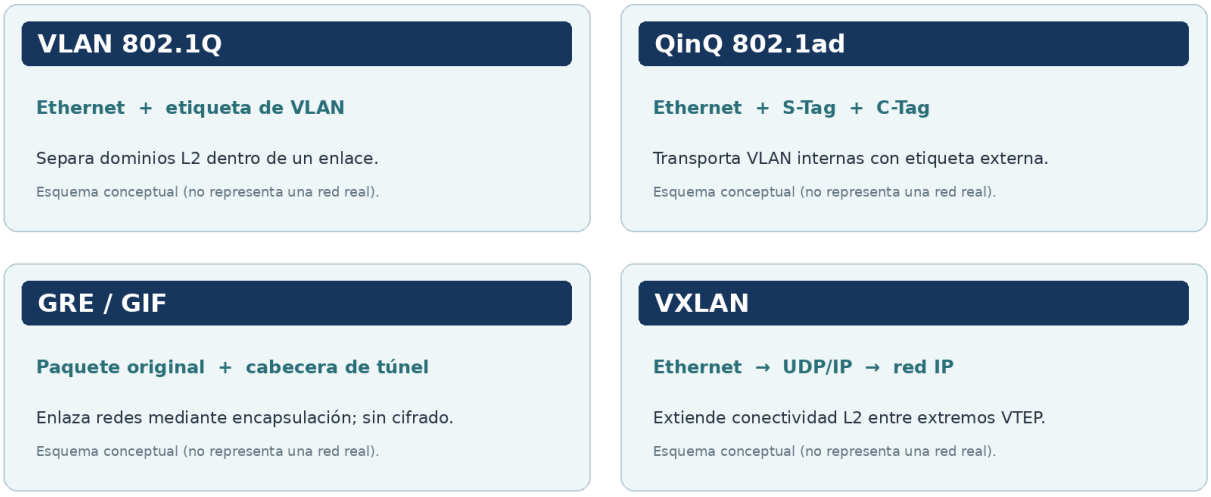


Figura 25.2. Comparación esquemática de VLAN, QinQ, GRE/GIF y VXLAN; ningún diagrama contiene configuraciones de producción.

25.12. Bridges: unión de interfaces en capa 2

Columna / acción	Interpretación
Interface	Bridge virtual generado por el sistema.

Columna / acción	Interpretación
Members	Puertos e interfaces que comparten el dominio L2.
Description	Finalidad de la unión.
Actions / Add	Editar o eliminar un bridge existente; crear uno nuevo.

Un bridge reenvía tramas entre miembros como un conmutador software. No equivale a añadir una ruta entre subredes: los miembros quedan en un dominio de difusión común. Esto puede resultar útil para determinados modos transparentes o para unir conexiones físicas e inalámbricas compatibles, pero introduce riesgos de bucles L2, interacciones con filtrado y pérdida de administración.

25.12.1. Crear un bridge según la documentación oficial

01. Abrir Interfaces → Assignments → Bridges y pulsar Add.
02. Seleccionar Member Interfaces, con al menos un miembro; la selección múltiple puede hacerse con Ctrl.
03. Añadir Description y revisar Show Advanced Options solamente si existe un requisito técnico.
04. Comprobar si se necesita STP o RSTP para prevenir bucles antes de guardar.
05. Guardar, asignar el propio bridge cuando deba tener IP y evaluar en qué interfaz se filtrará tráfico.

Opción avanzada documentada	Para qué sirve
Protocol: STP / RSTP	Protocolo de prevención de bucles; RSTP converge más rápidamente y suele preferirse en equipos compatibles.
STP Interfaces	Miembros sobre los que se aplica STP.
Bridge Priority / Port Priorities	Influyen en selección de raíz y puertos de forwarding/bloqueo.
Path Costs	Preferencias de camino de cada miembro; una mala elección cambia el tráfico utilizado.
Forward Time / Hello Time / Valid Time	Temporizaciones de convergencia; pueden introducir periodos sin tráfico durante cambios de topología.
Show Advanced Options	Despliega las opciones adicionales, no ejecuta una acción de red por sí mismo.

Netgate recomienda, en la mayoría de casos, colocar el direccionamiento IP en la interfaz del bridge asignada y no en uno de sus miembros. El filtrado se controla también mediante net.link.bridge.pfil_member y net.link.bridge.pfil_bridge: por defecto suele aplicarse a los miembros; al cambiarlo deben quedar reglas efectivas y al menos uno de estos mecanismos de filtrado habilitado.

Muy alto riesgo. Un bridge creado sobre puertos gestionados desde la misma sesión puede cortar el acceso web. Nunca modificar enlaces con posibilidad de bucle sin un plan de recuperación, acceso alternativo y protección STP/RSTP acorde con la red.

25.13. LAGGs: agregación y redundancia de enlaces

Columna / acción	Interpretación
Interface	Interfaz lógica agregada.
Members	Puertos físicos miembros del agregado.
Description	Etiqueta funcional.
Actions / Add	Alta y mantenimiento de definiciones LAGG.

LAGG combina varias NIC físicas en una interfaz lógica. Según el modo, permite redundancia ante un fallo de puerto, distribución de flujos y aumento de capacidad agregada. La suma de velocidades no asegura que una única conexión utilice todo el ancho de banda: en LACP un flujo habitual queda sujeto al rendimiento de uno de los miembros.

25.13.1. Campos y protocolos de LAGG documentados

Campo / modo	Efecto
Parent Interfaces	Interfaces físicas libres; una NIC ya asignada no suele poder añadirse directamente a un LAGG.
LAGG Protocol = LACP	Negocia 802.3ad con switch compatible; requiere configuración coincidente, velocidad/MTU y full duplex homogéneos.
LACP Timeout Mode	Slow usa mensajes menos frecuentes; Fast detecta antes pérdidas de negociación pero emite más PDUs.
LAGG Protocol = Failover	Transmite por el miembro principal y conmuta al siguiente disponible si falla.
Failover Primary Interface	Define miembro principal de Failover o auto.
LAGG Protocol = Load Balance	Reparte transmisiones sin negociación LACP; debe coordinarse cuidadosamente con el extremo.
LAGG Protocol = Round Robin	Distribuye paquetes secuencialmente entre miembros; puede causar reordenación y problemas de interoperabilidad.
LAGG Protocol = None	No transmite ni recibe tráfico por el grupo, aunque la interfaz siga apareciendo operativa a nivel del sistema.
Hash Algorithm	Criterios L2/L3/L4 usados para distribuir tráfico de salida; afecta al reparto por flujo.
Description / Save	Texto administrativo y persistencia.

25.13.2. Secuencia segura de implantación

01. Revisar compatibilidad del switch o stack y elegir LACP/Failover según el objetivo.
02. Disponer de puertos físicos sin asignación y respaldar la configuración antes de transformar un LAN o WAN en LAGG.
03. Crear LAGG mediante Add, seleccionar miembros y el protocolo; ajustar hash y parámetros solo cuando el entorno lo requiera.
04. Configurar la contraparte del switch en el mismo modo; guardar y crear las VLAN sobre LAGG si procede.
05. Asignar LAGG o sus VLAN en Interface Assignments; comprobar enlace, estados de agregación, tasa y conmutación ante fallo controlado.

Los puertos miembros de un LAGG no aparecen como puertos de red individuales disponibles en el selector principal. Esta restricción impide una doble asignación incompatible. Tampoco debe confundirse LAGG con un grupo de gateways: LAGG trabaja sobre puertos de un enlace o dominio L2 compatible, mientras que los gateway groups operan a nivel de selección de rutas WAN.

Precaución específica. Para migrar una LAN activa a LAGG existen procedimientos oficiales graduales; no liberar a ciegas el único puerto por el que se administra el firewall. En LACP, ambos extremos deben estar configurados de modo coordinado.



Figura 25.3. Diferencia entre grupo de interfaces, bridge y LAGG: reglas, conmutación de capa 2 y agregación de enlaces.

25.14. Dependencias entre pestañas: orden de trabajo

Necesidad	Secuencia adecuada	Verificación principal
Nueva red VLAN	VLANs → Interface Assignments → Interfaces/OPT → Rules/Services	Trunk, etiquetado, interfaz habilitada y aislamiento.
Conexión PPPoE	VLANs (si ISP la exige) → PPPs/ajustes WAN → reglas	Sesión PPP, gateway, MTU y tráfico.
Enlace LACP con VLAN	LAGGs → VLANs sobre LAGG → Assignments → reglas	Estado de miembros LACP y VLAN sobre agregado.
Túnel GRE o GIF	GREs/GIFs → Assignments → habilitar → rutas/reglas	Extremos, enrutamiento y paso de protocolos.
Tramo Ethernet extendido	VXLANs → Bridge si procede → reglas/MTU	VTEP, UDP, MAC y ausencia de bucles.
Política común	Interface Groups → Firewall > Rules	Orden reglas grupo/interfaz.
Instancia Wi-Fi	Wireless → Assignments → configuración individual	Modo, asociación y políticas.

El orden es determinante: un recurso virtual puede existir sin estar asignado, y una asignación puede existir sin estar habilitada o sin reglas. Del mismo modo, eliminar un objeto padre usado por otros objetos puede dejar referencias sin tráfico funcional. Conviene registrar antes de tocarlo la cadena de dependencias desde el puerto físico hasta las políticas del servicio.

25.15. Procedimientos empresariales ilustrativos

Caso A. Segmentar una red de usuarios y otra de dispositivos

Objetivo: impedir que dos colectivos compartan difusión L2 y permitir únicamente tráfico intersegmento explícitamente autorizado. Crear dos VLAN con identificadores ficticios de laboratorio sobre un puerto troncal previamente preparado; asignarlas como OPT, darles un direccionamiento apropiado a cada una y configurar DHCP y reglas independientes. La comprobación final debe realizarse desde un cliente de cada segmento y verificar tanto accesos permitidos como denegados. El funcionamiento no requiere un bridge.

Caso B. Aumentar disponibilidad de un enlace de acceso

Objetivo: tolerar la pérdida de un cable o un puerto sin modificar la identidad IP del enlace lógico. Si existe switch compatible, preparar un LAGG LACP con puertos equivalentes y conectividad alternativa de administración. Probar la caída controlada de un miembro y que el rendimiento total responde al reparto de flujos esperado; no prometer velocidad de un único flujo igual a la suma de enlaces.

Caso C. Concentrar reglas de varias interfaces internas

Objetivo: aplicar restricciones homogéneas a varias redes con funciones similares. Crear Interface Group, incluir únicamente las interfaces necesarias y colocar reglas comunes en su pestaña del firewall. Conservar reglas particulares solo para excepciones compatibles con el orden de evaluación y probar ambos sentidos de tráfico. No utilizar el grupo como sustituto del tratamiento multi-WAN.

Caso D. Extender una red L2 entre dos extremos controlados

Objetivo: transportar Ethernet entre dos sistemas usando una red IP subyacente. Diseñar VNI/puertos, seguridad y MTU de VXLAN; crear los VTEP, unir a un bridge solo los segmentos específicamente necesarios y verificar prevención de bucles. Una solución de extensión L2 exige justificar por qué no basta con enrutar redes independientes, habitualmente más sencillo y controlable.

25.16. Verificación sistemática y diagnóstico de incidencias

Síntoma	Posible causa	Comprobación segura
Interfaz virtual no aparece en Available network ports	Definición aún no creada; adaptador no soportado o puerto ya ocupado.	Revisar pestaña de origen, asignaciones y miembros LAGG.
OPT creada pero sin conectividad	Deshabilitada, sin IP, VLAN sin trunk o reglas insuficientes.	Interfaces > OPT; Status > Interfaces; Firewall > Rules.

Síntoma	Posible causa	Comprobación segura
VLAN sin tráfico	Etiqueta o interfaz padre discordante; switch no etiqueta el puerto.	Comparar ambos extremos y capturar tráfico autorizado.
PPP no establece sesión	Credenciales, servicio PPPoE, VLAN o medio físico erróneos.	Revisar estado de WAN y logs PPP sin mostrar claves.
GRE/GIF no llega al extremo	Ruta del underlay, permiso de encapsulado o datos de extremos.	Probar transporte, después direcciones del túnel y rutas.
VXLAN no aprende MAC	UDP filtrado, VNI dispar, Learn no adecuado o MTU.	Validar VTEP, puertos y pruebas de capa 2.
Bridge genera cortes	Bucle L2, STP/RSTP, ubicación de IP o filtrado.	Comprobar estados de puertos y reglas sin desactivar controles de seguridad.
LAGG presenta un solo enlace activo	Negociación o estado de miembro, switch, velocidad/MTU.	Verificar protocolos y puertos en ambos extremos.
Regla de interfaz no actúa	Regla flotante/grupo coincide antes.	Inspeccionar orden y los estados de firewall.
Se pierde acceso al panel	Cambio en puerto asignado o en LAN/bridge administrado.	Utilizar consola u otro canal aprobado para restaurar configuración.

25.16.1. Lista de comprobación mínima

01. Estado: Status → Interfaces confirma enlace y dirección cuando proceda; un enlace «up» por sí solo no garantiza conectividad.
02. Rutas: System → Routing y tabla de rutas efectiva incluyen el próximo salto adecuado.
03. Reglas: Firewall → Rules y los registros de filtrado muestran la política que ha permitido o bloqueado el flujo.
04. Servicios: DHCP, DNS, NAT, VPN o gateway monitoring solo si son necesarios para el propósito de la interfaz.
05. Capa 2: switch, VLAN, PCP, LACP, STP o transporte de encapsulado son coherentes con el extremo remoto.
06. Recuperación: existe copia verificable y procedimiento de vuelta atrás por consola o canal independiente.

25.17. Recomendaciones profesionales de operación y seguridad

Regla de administración	Aplicación práctica
Separar definición de activación	Crear objeto, asignarlo, habilitarlo y aplicar políticas en pasos verificables.
Preservar la vía de gestión	Mantener acceso alternativo al tocar LAN, bridge, VLAN de gestión o WAN.
Comprobar el extremo opuesto	Switch, ISP, peer de túnel y VTEP deben estar coordinados.
Cifrar cuando es necesario	GRE, GIF y VXLAN no sustituyen una VPN cifrada en redes no confiables.
Evitar puentes innecesarios	Preferir segmentación y enrutamiento cuando la extensión L2 no sea requisito.
No publicar identificadores	Usar diagramas genéricos y nunca copiar configuración ni valores de producción.
Cambios controlados	Guardar backup previo, registrar objetivo, validación y reversión.
Verificar dependencias	Antes de eliminar, buscar reglas, servicios, rutas, VLAN hijas y miembros afectados.

La gestión de interfaces afecta a todas las capas de red: un cambio aparentemente local en un selector puede alterar la conectividad del firewall y de sus clientes. La disciplina de cambios tiene tanto peso como la corrección técnica del formulario. Es esencial diferenciar observación (leer estados) de modificación (guardar cambios) y realizar primero pruebas no destructivas.

25.18. Glosario esencial

Término	Definición
Asignación	Vinculación entre interfaz lógica del firewall y recurso de red subyacente.
OPT / OPTx	Interfaz adicional con identificador ordinal y nombre configurable.
Parent Interface	Interfaz portadora o recurso sobre el que se crea otra interfaz.
Trunk	Enlace preparado para transportar varias VLAN etiquetadas.
VID / PCP	Identificador VLAN / prioridad 802.1p de la trama.
QinQ / TPID	Doble etiqueta de VLAN / indicador de protocolo de etiqueta.
PPP / PPPoE	Protocolo punto a punto / PPP encapsulado sobre Ethernet.
GRE / GIF	Mecanismos de encapsulación por túnel.
VTEP / VNI	Extremo de túnel VXLAN / identificador de segmento VXLAN.
Bridge / STP	Puente de capa 2 / prevención de bucles por spanning tree.
LAGG / LACP	Agregado de enlaces / negociación 802.3ad.
Underlay / Overlay	Red portadora IP / red lógica construida sobre ella.

25.19. Resumen operativo del capítulo

Interface Assignments conecta cada función lógica con su puerto. El resto de pestañas permiten definir tecnologías virtuales o grupos de reglas que luego se utilizan desde los menús de configuración, filtrado, rutas y servicios. Lo decisivo no es que una entrada aparezca en un listado, sino que toda su cadena de dependencias sea coherente, segura y comprobable.

Principio de cierre. Antes de guardar un cambio de asignación, responder cuatro preguntas: ¿qué recurso cambia?, ¿qué tráfico depende de él?, ¿cómo comprobaré el resultado?, ¿cómo recuperaré el acceso si falla?

Referencias técnicas oficiales de Netgate

Netgate. Interface Configuration: https://docs.netgate.com/pfsense/en/latest/config/interface-configuration.html
Netgate. Interface Types and Configuration: https://docs.netgate.com/pfsense/en/latest/interfaces/index.html
Netgate. Interface Configuration (General): https://docs.netgate.com/pfsense/en/latest/interfaces/configure.html
Netgate. WAN vs LAN Interfaces: https://docs.netgate.com/pfsense/en/latest/interfaces/wanvslan.html
Netgate. Interface Groups: https://docs.netgate.com/pfsense/en/latest/interfaces/groups.html
Netgate. Wireless VAP Instances: https://docs.netgate.com/pfsense/en/latest/wireless/vap.html
Netgate. VLAN Configuration: https://docs.netgate.com/pfsense/en/latest/vlan/configuration.html
Netgate. QinQ Configuration: https://docs.netgate.com/pfsense/en/latest/interfaces/qinq.html
Netgate. PPPs: https://docs.netgate.com/pfsense/en/latest/interfaces/ppp.html
Netgate. GRE: https://docs.netgate.com/pfsense/en/latest/interfaces/gre.html
Netgate. GIF: https://docs.netgate.com/pfsense/en/latest/interfaces/gif.html
Netgate. VXLAN Configuration: https://docs.netgate.com/pfsense/en/latest/interfaces/vxlan.html
Netgate. Creating a Bridge: https://docs.netgate.com/pfsense/en/latest/bridges/create.html
Netgate. Bridging and Interfaces: https://docs.netgate.com/pfsense/en/latest/bridges/interfaces.html

Netgate. Bridging and Firewall Rules: https://docs.netgate.com/pfsense/en/latest/bridges/firewall.html

Netgate. LAGG: https://docs.netgate.com/pfsense/en/latest/interfaces/lagg.html

Netgate. Migrating an Assigned LAN to LAGG: https://docs.netgate.com/pfsense/en/latest/recipes/migrate-assigned-lan-to-lagg.html

Netgate. WireGuard Settings: https://docs.netgate.com/pfsense/en/latest/vpn/wireguard/settings.html

Netgate. Status → Interfaces: https://docs.netgate.com/pfsense/en/latest/monitoring/status/interfaces.html

Documentación oficial consultada en noviembre de 2026. Los nombres, controles y opciones pueden variar en revisiones futuras; la versión exacta del producto deberá comprobarse antes de aplicar cambios sensibles.

26 Interfaces → Switch

Sistema, puertos físicos, pertenencia VLAN y transporte Ethernet en el switch integrado

Ruta principal: Interfaces → Switch | Pestañas: System · Ports · VLANs. El nombre del menú puede aparecer como «Switches» en determinadas versiones o plataformas.

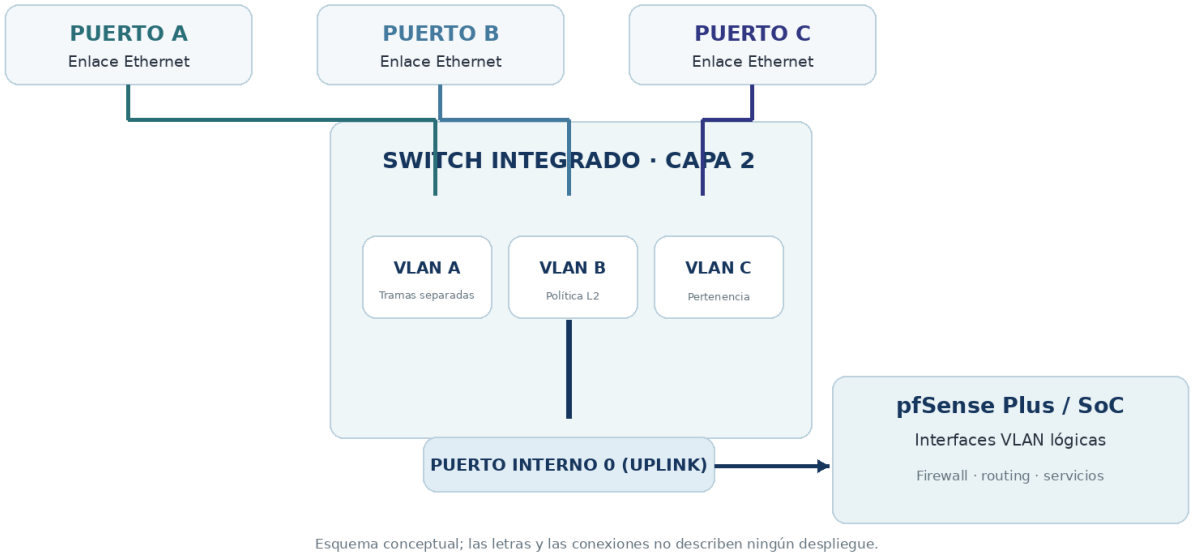


Figura 26.1. Arquitectura conceptual de un switch integrado y su conexión al sistema operativo; no muestra ninguna instalación real.

26.1. Objetivo y alcance del capítulo

La configuración de Switch en pfSense Plus administra el conmutador Ethernet integrado en determinadas plataformas Netgate. A diferencia de un equipo con tarjetas independientes por puerto, varios conectores de red pueden compartir un único enlace interno con el sistema operativo. La separación entre puertos se materializa mediante VLAN y su pertenencia en el chip de conmutación. Por ello, cambiar una VLAN en el switch no equivale a crear o modificar una interfaz en pfSense Plus.

La interfaz estudiada dispone de tres pestañas: System, que identifica las capacidades del componente; Ports, que presenta el estado y los parámetros de cada puerto; y VLANs, que activa el modo 802.1Q y gestiona los grupos VLAN. Las explicaciones distinguen controles visibles en estas vistas y principios adicionales verificados en la documentación oficial de Netgate. No se reproducen topologías, identificadores ni valores operativos particulares.

Punto de partida. Un switch integrado reúne puertos en capa 2; pfSense Plus aplica encaminamiento, reglas, NAT y servicios a los paquetes que atraviesan su interfaz con el sistema. El tráfico conmutado exclusivamente entre dos puertos del mismo dominio de capa 2 puede no pasar por el firewall.

26.2. Arquitectura: puerto externo, switch y enlace interno

En una plataforma de referencia como Netgate 1100, los puertos Ethernet externos están conectados al chip de switch. El chip dispone asimismo de un puerto interno, identificado habitualmente como puerto 0 (HOST o uplink), que enlaza con la interfaz del sistema operativo. Netgate documenta un enlace interno de 1 Gbit/s en esta familia: no debe confundirse la suma de velocidades nominales de los conectores con el caudal compartido disponible hacia la CPU.

Capa o elemento	Función	Qué puede observarse o modificarse
Conector Ethernet	Entrada y salida física de tramas.	Presencia de portadora, velocidad y dúplex; no implica una IP independiente.
Chip de switch	Conmutación Ethernet local y clasificación VLAN.	PVID, etiquetas, pertenencia y estado de puertos.

Capa o elemento	Función	Qué puede observarse o modificarse
Puerto interno / uplink	Camino entre switch y sistema operativo.	Membresías VLAN etiquetadas necesarias para que llegue tráfico a pfSense.
Interfaz padre	Dispositivo de red visible para el sistema.	Sobre ella se definen VLAN lógicas, según la plataforma.
Interfaz pfSense	Entidad WAN, LAN u OPT asignada.	IP, reglas, NAT, DHCP, gateways, servicios y supervisión.

26.2.1. Por qué pueden existir tres conectores pero una sola interfaz padre

El sistema operativo recibe las VLAN encaminadas desde el switch a través del enlace interno; cada VLAN puede presentarse como interfaz lógica independiente, aunque físicamente comparta el mismo soporte. La separación WAN/LAN/OPT puede mantenerse por pertenencia VLAN incluso cuando los conectores pertenecen a un único circuito integrado. Esta arquitectura exige coordinación entre la configuración de Switch y la de Interfaces → Assignments.

Limitación relevante. En la familia de referencia, el switch integrado no implementa STP (Spanning Tree Protocol). Conectar dos puertos a un mismo dominio capa 2 por rutas redundantes puede crear un bucle y paralizar el servicio. No debe tratarse como un switch de acceso empresarial con funciones completas de prevención de bucles.

26.3. Ruta, navegación y lectura segura de la pantalla

Elemento	Interpretación práctica
Interfaces → Switch	Ruta observada en la interfaz de usuario; Netgate puede denominar el menú «Interfaces → Switches».
System / Ports / VLANs	Pestañas del mismo dispositivo de conmutación, no tres interfaces independientes.
Icono ?	Ayuda contextual, según edición y disponibilidad.
Filas de información	Estado o definiciones que presenta el dispositivo; su existencia no constituye autorización para modificar.
Save	Guarda la sección correspondiente; el impacto puede ser inmediato sobre el tráfico.
Lápiz / papelera	Editar / eliminar una definición donde esté permitido; nunca borrar por ensayo un grupo base.
Add Tag	Accede al alta de un grupo de etiqueta 802.1Q, sujeto a las opciones disponibles en esa versión.

Es aconsejable revisar System, anotar de manera privada las capacidades, inspeccionar Ports y solo después evaluar VLANs. Este orden ayuda a comprender la relación entre el enlace interno, los puertos y los grupos existentes sin modificar la red.

26.4. System: inventario de capacidades del switch

La pestaña System es principalmente informativa. Resume el tipo de chip, límites y funciones anunciadas por el controlador. No debe confundirse con System → Advanced ni con la configuración general del firewall.

Columna visible	Interpretación técnica	Implicación para la administración
Type	Familia de switch integrada, p. ej. Marvell 6000 series switch.	Identifica el controlador; no es un nombre privado del equipo.
Ports	Capacidad total de puertos reconocidos por el chip/controlador.	No equivale necesariamente al número de tomas RJ-45 accesibles.
VLAN groups	Número máximo de entradas o grupos VLAN en ese chip.	Es un límite de hardware, no prueba de VLAN operativas.
LAGG groups	Capacidad declarada para agrupaciones de enlaces.	No significa que todas sean utilizables con conectores externos.
VLAN Mode	Modo vigente de tratamiento de VLAN, como DOT1Q.	Debe ser coherente con la pertenencia y los PVID.

Columna visible	Interpretación técnica	Implicación para la administración
Capabilities	Indicadores anunciados por el controlador.	Sirven para identificar prestaciones; no son controles activables.

26.4.1. Interpretación del campo Capabilities

Indicador técnico	Lectura orientativa
PORT	Funciones de gestión de puertos del switch.
DOT1Q	Soporte anunciado de operaciones de VLAN IEEE 802.1Q.
PORTS_MASK	Soporte de máscaras de pertenencia o agrupación de puertos a nivel del controlador.
LAGG	Funciones de agregación soportadas por el chip/controlador.
PSTATE	Información o control del estado de puertos expuesto por el controlador.

Estos identificadores son capacidades de bajo nivel; no equivalen a un menú de parámetros que deba configurarse directamente ni garantizan prestaciones ajenas al modelo. Los límites presentados por System describen el hardware y su controlador, mientras que los cambios operativos se ejecutan en Ports y VLANs.

26.5. Ports: inventario, estado y controles de puertos

La pestaña Ports combina datos descriptivos y parámetros administrables. La zona tabular suele permitir editar el Port VID y, cuando sea compatible, la pertenencia LAGG mediante interacción sobre la celda; el selector Media configura velocidad/dúplex cuando la plataforma lo admite. El botón Save confirma cambios. El comportamiento de edición depende del modelo y de la versión.

Columna visible	Qué representa	Cómo interpretarla
Port #	Índice interno que identifica el puerto en el chip.	Puede incluir un puerto interno distinto de los conectores físicos.
Port name	Designación funcional del puerto.	Etiqueta descriptiva; no asumir una identidad de interfaz IP.
Port VID	VLAN ID por defecto del tráfico entrante sin etiqueta.	PVID debe ser compatible con la membresía VLAN configurada.
LAGG	Grupo de agregación del switch, si existe.	Un guion puede indicar ausencia de pertenencia.
Flags	Atributos de funcionamiento, como HOST.	HOST identifica un puerto especial de conexión al sistema.
State	Estado de conmutación, por ejemplo FORWARDING.	No es sinónimo de enlace físico conectado.
Media	Medio y modo de negociación del enlace.	Normalmente se recomienda autonegociación.
Status	Presencia y situación del enlace físico.	Active y No Carrier describen portadora, no reglas firewall.

26.5.1. Diferencia esencial: State frente a Status

FORWARDING indica que el switch trata el puerto como habilitado para reenviar tramas dentro de su lógica de conmutación. Active describe una condición física de enlace existente. Un puerto puede aparecer en FORWARDING y simultáneamente en No Carrier cuando no se detecta conexión Ethernet: no hay contradicción, porque son dimensiones distintas.

State / Status	Lectura razonable	Siguiente comprobación
FORWARDING / Active	Conmutación permitida y portadora presente.	Revisar PVID, membresía, tráfico, IP y reglas.
FORWARDING / No Carrier	La lógica del switch permite reenviar, pero no hay enlace físico.	Revisar cable, equipo remoto y negociación.
Sin FORWARDING / Active	Existe señal física, pero el switch podría no reenviar.	Verificar configuración/estado del puerto y diagnósticos.

State / Status	Lectura razonable	Siguiente comprobación
Sin enlace / sin tráfico	No basta una etiqueta visual para atribuir una causa única.	Separar fallos físicos de VLAN y de políticas L3.

26.6. Port VID: PVID y clasificación de tráfico sin etiquetar

Port VID (PVID, Port VLAN Identifier) determina la VLAN que el switch asigna a las tramas entrantes por un puerto cuando llegan sin cabecera 802.1Q. Es una clasificación de entrada (ingress); no establece por sí sola el etiquetado de salida (egress). La salida tagged o untagged depende de la definición de miembros del grupo VLAN. Tampoco configura la dirección IP de pfSense.



Ejemplos didácticos: VLAN 110 y 220 son valores ficticios.

Figura 26.2. Comparación didáctica de puertos access y trunk, con VID de ejemplo completamente ficticios.

Concepto	Pregunta a resolver	Dónde se decide
PVID	¿A qué VLAN se asigna una trama entrante sin etiqueta?	Ports → Port VID.
VLAN Tag	¿Qué identificador de VLAN tiene este grupo?	VLANs → VLAN tag.
Member	¿Qué puertos participan de esta VLAN?	VLANs → Members.
Tagged / Untagged	¿Cómo sale por un puerto el tráfico de esta VLAN?	VLANs → pertenencia del miembro al editar.
IP / reglas	¿Qué tráfico se enruta o permite entre redes?	Interfaces → Assignments y Firewall → Rules.

No confundir. Modificar el PVID de un puerto no crea automáticamente un grupo VLAN ni añade el puerto a él. Si el PVID apunta a una VLAN inexistente o a un grupo del que el puerto no forma parte, el tráfico sin etiqueta puede dejar de llegar a su destino.

26.7. Media: velocidad, dúplex y negociación Ethernet

El selector Media permite elegir una preferencia de medio/negociación en los puertos donde aparece. En la configuración general, «Default (no preference, typically autoselect)» suele ser la selección recomendada, ya que ambos extremos negocian automáticamente velocidad y dúplex. La cadena de estado puede mostrar además «Ethernet autoselect (...)» como resultado negociado.

Ajuste o estado	Qué significa	Recomendación
Default / autoselect	Sin velocidad ni dúplex forzados; se negocian.	Preferible en la mayoría de enlaces Ethernet.
Velocidad fija	Solicitud de velocidad concreta, si el hardware la ofrece.	Solo ante una necesidad documentada y compatible.
Full-duplex	Transmisión y recepción simultáneas.	Debe concordar con el equipo conectado.

Ajuste o estado	Qué significa	Recomendación
No Carrier	El puerto no detecta portadora.	Diagnosticar cableado, energía, NIC y extremo remoto.
Active	La capa física mantiene enlace.	No garantiza VLAN correcta ni conectividad IP.

Forzar velocidad o dúplex unilateralmente puede ocasionar pérdidas, latencia, errores o pérdida completa de enlace. Si una de las partes está configurada con parámetros forzados, debe comprobarse la compatibilidad de la negociación en el otro extremo, en lugar de asumir que «más velocidad» mejora el rendimiento.

26.8. VLANs: activar y administrar 802.1Q en el switch

La pestaña VLANs es la pieza clave de la separación lógica en hardware. Cuando «Enable 802.1q VLAN mode» está activado, el switch opera con grupos VLAN y controla la admisión de etiquetas configuradas. La advertencia visible indica que las tramas etiquetadas con VLAN desconocidas se descartan, comportamiento importante tanto para seguridad como para diagnóstico.

Elemento visible	Función	Efecto o riesgo
Enable	Encabezado de la opción de conmutación de modo.	Agrupa la casilla de activación.
Enable 802.1q VLAN mode	Conmutar el modo IEEE 802.1Q.	Activado: grupos VLAN gestionan el aislamiento y las etiquetas reconocidas.
Aviso de VLAN desconocidas	Señala descarte de etiquetas no definidas.	Una etiqueta no configurada no llegará a la interfaz de destino.
VLAN(s) table	Inventario de grupos y membresías.	Base lógica del encaminamiento de VLAN en el chip.
Save	Guardar ajustes de la sección.	Puede alterar inmediatamente la conectividad de varios puertos.
Add Tag	Alta de una definición VLAN.	Después requiere miembros, PVID/trunk y configuración en pfSense cuando corresponda.

26.8.1. Qué ocurre al activar el modo

Con el modo 802.1Q habilitado, cada VLAN admitida se representa mediante una etiqueta y sus miembros. Un puerto de acceso puede recibir tráfico sin etiqueta y asignarlo al VID de entrada; el enlace interno suele participar como miembro etiquetado de las VLAN que se entregan al sistema. Este diseño permite mantener redes distintas sobre el enlace compartido.

26.8.2. Qué ocurre al desactivar el modo

La documentación de Netgate describe un modo alternativo denominado Port VLAN Mode, donde el comportamiento no es el de clasificación 802.1Q por grupos: las etiquetas pueden atravesar los puertos sin añadirse ni retirarse según el mecanismo de 802.1Q y se forman grupos físicos de puertos. Cambiar el modo en un firewall con WAN, LAN u OPT diferenciados por VLAN puede alterar radicalmente la separación de redes y provocar pérdida de administración o filtrado inesperado.

Riesgo crítico de aislamiento. No desactivar «Enable 802.1q VLAN mode» como prueba rápida para resolver una VLAN sin tráfico. En plataformas cuya arquitectura depende de etiquetas internas, esta acción afecta simultáneamente a las redes y servicios que usan el chip.

26.9. Tabla de VLANs: campos y acciones

Columna	Qué contiene	Precaución
VLAN group	Índice del grupo o entrada de la tabla del chip.	No es el VLAN ID; puede incluir entradas reservadas.
VLAN tag	Identificador IEEE 802.1Q asociado al grupo.	Debe concordar con el extremo remoto y con la VLAN lógica.
Members	Puertos participantes y, cuando se indica, sufijo «t».	«t» significa tráfico etiquetado en ese miembro.

Columna	Qué contiene	Precaución
Description	Descripción administrativa del grupo.	No determina PVID, conectividad ni reglas.
Action: lápiz	Abrir la edición de la pertenencia/definición.	Revisar todos los miembros antes de guardar.
Action: papelera	Eliminar una definición donde se permita.	Puede interrumpir redes, servicios, VPN y acceso a GUI.
Save / Add Tag	Confirmar o iniciar alta de grupos.	Crear el grupo no configura por sí solo interfaces ni permisos.

26.9.1. VLAN group no es igual a VLAN tag

Un grupo es una entrada del hardware; el tag es el valor de la cabecera 802.1Q (VID de 1 a 4094 en la configuración VLAN habitual). Un grupo con índice 4 no equivale a una VLAN con etiqueta 4. Confundir los dos campos puede terminar afectando al dominio de capa 2 equivocado.

26.9.2. Significado de los miembros y del sufijo t

La columna Members representa la pertenencia de puertos de switch a cada grupo. Un miembro escrito como «0t» indica que el puerto 0 participa con etiquetas en el tráfico de esa VLAN. El mismo número sin «t» indica salida sin etiqueta en esa VLAN. No equivale a que la VLAN sea de confianza ni a que tenga reglas permitidas en pfSense.

En el modelo de referencia, el puerto interno 0 enlaza con la CPU; Netgate advierte que la entrada de grupo base debe permanecer intacta y que los grupos base utilizados por las interfaces necesitan incluir el miembro interno etiquetado. Borrar ese miembro puede desconectar del sistema operativo una red físicamente activa.

Restricción documentada por Netgate. En el escenario de referencia Netgate 1100: conservar el grupo base 0 y la pertenencia «0t» de los grupos fundamentales. No copiar esta numeración como receta universal para otros equipos, pero sí respetar las entradas base y el uplink definidos por el fabricante.

26.10. Edición de grupos VLAN: secuencia y validaciones

La lista permite abrir un grupo con el icono del lápiz. La documentación oficial de Netgate para el equipo de referencia presenta un editor de miembros que permite agregar o quitar un puerto y marcarlo como Tagged. Los controles exactos del formulario de edición pueden variar; aquí se describen solo las operaciones demostradas documentalmente, no campos inexistentes en las tres vistas analizadas.

01. Confirmar la finalidad de la VLAN y los puertos que deben ser miembros. Identificar de manera privada la ruta de gestión del administrador.
02. Revisar la tabla existente y comprobar si el grupo es reservado o base: en ese caso no eliminarlo ni modificar la conexión interna a la CPU.
03. Abrir el lápiz de un grupo permitido. Revisar la lista de miembros y el estado Tagged de cada uno.
04. Agregar o retirar exclusivamente los miembros requeridos; diferenciar si la salida debe ser tagged o untagged para cada puerto.
05. Guardar la edición y, cuando corresponda, la página principal mediante Save. Evitar aplicar otras modificaciones simultáneas.
06. Comprobar el estado físico, pertenencia, tramas de entrada/salida, interfaz de pfSense y flujos permitidos antes de continuar.

La acción de la papelera no debe utilizarse mientras un grupo tenga dependencias. Antes de retirar una VLAN hay que identificar las interfaces lógicas que se apoyan en ella, el tráfico de servicios y las reglas, enrutamientos o políticas que la usan.

26.11. Access y trunk: comportamiento real en cada sentido

26.11.1. Puerto de acceso (access / untagged)

Está pensado para un dispositivo que envía tramas sin etiqueta, como una estación de trabajo o una impresora. El switch clasifica esas tramas entrantes con el PVID del puerto, y normalmente envía por ese

puerto las tramas de la VLAN correspondiente sin etiqueta. Que el puerto sea de acceso no implica que sea necesariamente LAN ni que pueda acceder a todas las redes.

26.11.2. Puerto troncal (trunk / tagged)

Transporta múltiples VLAN por un único enlace hacia otro conmutador o dispositivo compatible con IEEE 802.1Q. Cada VLAN autorizada se incorpora como miembro tagged del puerto troncal y el equipo remoto debe tener esos VID definidos de forma coherente. El PVID sigue determinando cómo tratar el tráfico no etiquetado que llegue a ese puerto; su elección debe ser deliberada, no casual.

Aspecto	Access	Trunk
Emisor típico	Equipo final sin 802.1Q.	Switch gestionable, hipervisor o host con 802.1Q.
Tramas de entrada	Usualmente untagged → PVID.	Etiquetadas, con los VID admitidos por membresía.
Tramas de salida	Generalmente untagged en su VLAN de acceso.	Tagged en las VLAN correspondientes.
Riesgo frecuente	PVID distinto de la VLAN de pertenencia.	VLAN omitida, tag incorrecto o mezcla accidental de tráfico sin etiqueta.
Validación	Obtiene servicio de la red prevista.	Se comprueban las VLAN autorizadas una por una.

26.12. Relación con Interfaces → Assignments y las reglas del firewall

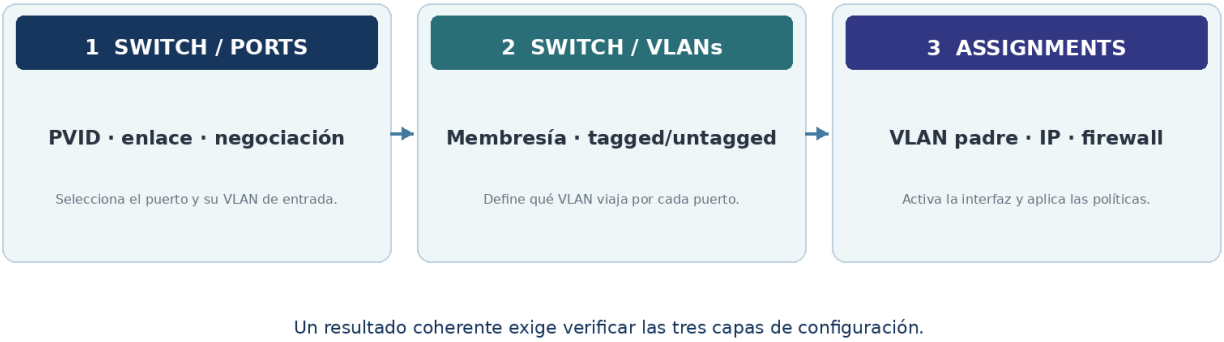


Figura 26.3. Tres planos que deben coordinarse al trabajar con VLAN de un switch integrado.

La pertenencia VLAN en el switch solo define por qué puertos circulan las tramas. Para que pfSense Plus las trate como una interfaz de red propia puede ser preciso definir una VLAN lógica sobre la interfaz padre, asignarla como WAN/LAN/OPTx, habilitarla y configurar su direccionamiento, servicios y reglas. Cuando la VLAN se utiliza únicamente para conmutación local entre puertos, el tráfico entre equipos de la misma VLAN puede no atravesar el firewall.

Acción	Se realiza en	Resultado
Definir miembros y etiquetado	Interfaces → Switch → VLANs	VLAN disponible en determinados puertos del chip.
Modificar la VLAN de entrada	Interfaces → Switch → Ports	Clasificación de tramas entrantes sin etiqueta.
Crear VLAN lógica del sistema	Interfaces → Assignments → VLANs	Subinterfaz sobre un padre compatible.
Asignar, habilitar y dar IP	Interfaces → Assignments; Interfaces → [nombre]	Interfaz L3 operativa si hay conectividad.
Permitir o impedir flujos	Firewall → Rules y otros menús pertinentes	Políticas de seguridad y, si procede, NAT/rutas/servicios.

Acción	Se realiza en	Resultado
Límite del filtrado. Dos dispositivos conectados al mismo dominio VLAN dentro del switch pueden intercambiar tráfico directamente en hardware. Para filtrar o registrar obligatoriamente ese tráfico se necesita que el diseño fuerce su paso por un dispositivo de seguridad; una regla de pfSense no inspecciona tramas que no llegan a su CPU.		

26.13. Procedimiento A: revisar el switch sin alterar servicios

01. Acceder por un canal autorizado y documentar únicamente el objetivo del análisis; evitar difundir detalles de la configuración operativa.

02. Entrar en Interfaces → Switch → System y verificar tipo de chip, capacidad y modo de funcionamiento.

03. Abrir Ports y revisar todos los índices visibles: localizar el puerto interno, observar Status y State, y comprobar que la negociación Media es razonable.

04. Abrir VLANs y verificar que el modo y los grupos existen y que el uplink interno conserva su membresía necesaria.

05. Comparar, de forma privada, esta vista con Interfaces → Assignments y las interfaces habilitadas.

06. No pulsar Save ni los iconos de edición si el objetivo era únicamente inventariar o supervisar.

Esta revisión es útil antes de migraciones, problemas de conectividad o auditorías de segmentación. El objetivo consiste en identificar relaciones entre puertos y dominios, no exportar ni reproducir configuraciones de producción.

26.14. Procedimiento B: configurar un puerto de acceso de ejemplo

Ejemplo didáctico: disponer un puerto libre en una VLAN ficticia 110 destinada a una red de pruebas. No se indican números de puerto reales ni una topología implementada. Este procedimiento requiere validar que el dispositivo de referencia permite crear y asignar el grupo de la forma descrita.

01. Asegurar conexión administrativa por un puerto diferente, no sujeto a la modificación, y preparar copia de seguridad y recuperación por consola.

02. En Switch → VLANs, comprobar si existe un grupo apropiado; crearlo mediante Add Tag solo cuando no exista y haya capacidad disponible.

03. Editar el grupo y añadir el puerto de pruebas como miembro untagged; conservar el miembro interno tagged si ese tráfico debe llegar a pfSense.

04. En Switch → Ports, cambiar el PVID de ese puerto a 110, coherente con la VLAN de pertenencia, y guardar.

05. Si la VLAN necesita direccionamiento o políticas en pfSense, definirla sobre el padre, asignarla, habilitarla y crear exclusivamente las reglas necesarias.

06. Conectar un cliente de prueba aislado y verificar enlace, direccionamiento y conectividad a los destinos expresamente autorizados.

Precaución. No asignar un PVID de una red aislada a un puerto que actualmente transporta la administración. Tampoco reutilizar una VLAN existente sin verificar que sus miembros y políticas coinciden con el objetivo.

26.15. Procedimiento C: configurar un puerto troncal de ejemplo

Ejemplo abstracto: un puerto enlaza con un switch gestionable que debe transportar únicamente dos segmentos ficticios, VLAN 110 y 220. La configuración del extremo remoto es tan importante como la del firewall.

01. Preparar acceso alternativo, respaldo y lista exacta de VLAN necesarias. No convertir el puerto de gestión principal en troncal sin plan de recuperación.

02. En Switch → VLANs, asegurar la existencia de los grupos de VLAN 110 y 220; incorporar el puerto elegido como miembro tagged de ambos.

03. Conservar la pertenencia adecuada del uplink interno etiquetado para las VLAN que deban alcanzar pfSense.

04. En Switch → Ports, definir deliberadamente el PVID para tráfico sin etiqueta; si no debe admitirse tráfico nativo, aplicar las salvaguardas compatibles con ambos equipos.
05. En el switch remoto, habilitar 802.1Q y permitir exclusivamente VLAN 110 y 220 por el enlace correspondiente; alinear el tratamiento de tramas sin etiqueta.
06. Crear/asignar VLAN lógicas en pfSense solo si el firewall debe ofrecer una interfaz L3 a esas redes, y verificar cada segmento separadamente.

Un enlace trunk no proporciona por sí mismo aislamiento completo: la seguridad depende de membresías acotadas, reglas de salida/entrada y de evitar VLAN nativa imprevista. Los protocolos de negociación automática de trunk no deben darse por disponibles en este switch.

26.16. Procedimiento D: unir dos puertos de acceso en una misma red

Netgate documenta un escenario en el que dos puertos externos se convierten en un pequeño switch de capa 2 dentro de un mismo grupo VLAN. El procedimiento real exige cambios coordinados de PVID y membresía. Aquí se presenta su lógica sin trasladar ni reproducir valores propios de ninguna instalación.

01. Determinar qué interfaz lógica debe prestar los servicios compartidos (por ejemplo, la LAN de pruebas) y seleccionar un puerto externo secundario que se incorporará a esa VLAN.
02. Verificar que la sesión de administración llega por un puerto ajeno al que se va a modificar; preparar consola y copia de seguridad.
03. Asignar al puerto adicional el PVID de la VLAN que se desea compartir.
04. Retirar ese puerto como miembro del grupo VLAN anterior cuando corresponda; agregarlo como miembro untagged del grupo VLAN compartido.
05. Conservar la pertenencia etiquetada del puerto interno hacia pfSense y no eliminar el grupo base protegido.
06. Revisar la opción Switch Port de la interfaz lógica que debe mantenerse disponible, porque ligar su estado al puerto original puede desactivar servicios cuando se desconecta ese conector.
07. Guardar de forma controlada y probar ambos puertos por separado, incluyendo DHCP/DNS si están configurados y tráfico hacia redes externas.

Observación documentada. En un grupo compartido, el tráfico entre los dos puertos se conmuta dentro del chip y puede no pasar por las reglas del firewall. La ampliación de bocas Ethernet no equivale a microsegmentación ni a filtrado entre los dispositivos conectados.

26.17. Escenarios empresariales y criterios de diseño

Necesidad	Diseño orientativo	Comprobación clave
Puesto de mantenimiento temporal	Puerto access con VLAN controlada y reglas mínimas.	Ningún acceso a redes ajenas a su función.
Conexión a switch gestionable	Trunk con VLAN expresamente autorizadas.	Coinciden VID, tagged/untagged y PVID en ambos extremos.
Dos conexiones en una misma LAN	Dos puertos untagged en la misma VLAN de switch.	Los servicios siguen disponibles al desconectar un puerto.
Segmentar redes de usuarios/servicios	Diferentes VLAN con interfaces L3 y reglas separadas.	Tráfico inter-VLAN atraviesa el firewall cuando se enruta.
Resolver fallo de enlace	Revisar No Carrier, autonegociación y estado remoto.	No modificar VLAN hasta descartar el nivel físico.
Necesidad de más caudal	Revisar arquitectura y límite de uplink compartido.	No confundir número de puertos con velocidad del camino CPU.
Red de switches redundante	Evitar bucles y elegir equipos con protecciones adecuadas.	El switch integrado de referencia carece de STP.

26.18. Seguridad, rendimiento y límites del switch

Riesgo o límite	Consecuencia	Práctica recomendada
Bucle capa 2, sin STP	Tormenta de broadcast y pérdida de servicio.	No construir conexiones redundantes L2 con este chip.
Uplink compartido hacia CPU	Posible cuello de botella para tráfico enrutado.	Dimensionar caudal agregado y cargas de inspección.
VLAN desconocida	Descartada en modo 802.1Q.	Crear grupo y membresía autorizada, no desactivar el modo.
Grupo base/uplink alterado	Pérdida de WAN/LAN o acceso al firewall.	Respetar grupo base y membresía tagged del puerto interno.
PVID y membresía incoherentes	Tramas sin etiqueta llegan a VLAN errónea o se pierden.	Validar ambas direcciones del tráfico.
Trunk demasiado permisivo	Segmentos llegan a donde no deben.	Permitir solo VLAN estrictamente necesarias.
Duplicación de red L2	Tráfico local elude inspección L3.	Revisar el modelo de amenaza y dónde se aplica el filtrado.
Configuración remota sin retorno	Administración interrumpida.	Consola, backup y acceso fuera del puerto afectado.

En equipos con recursos compartidos, el rendimiento no depende únicamente del estado Active de los conectores. Tráfico entre puertos en una misma VLAN puede quedar dentro del switch; tráfico entre VLAN diferentes o hacia WAN normalmente alcanza al sistema para ser enrutado y filtrado. Además del enlace interno, influyen CPU, reglas, NAT, inspección y características del tráfico.

26.19. Verificación técnica después de cada cambio

26.19.1. Pruebas progresivas en cinco capas

01. Capa física: confirmar portadora Active, negociación estable y ausencia de desconexiones intermitentes.
02. Capa switch: comprobar PVID, grupos VLAN y membresías tagged/untagged de los puertos afectados.
03. Capa interfaz: confirmar que la VLAN del sistema existe si se requiere, está asignada y habilitada, y su estado aparece correctamente.
04. Capa encaminamiento/seguridad: revisar rutas, reglas, NAT y servicios, sin introducir permisos globales para ocultar errores.
05. Capa de aplicación: probar únicamente los servicios previstos y verificar el retorno de las conexiones desde ambos extremos.

Prueba	Resultado esperado	Interpretación si falla
Cambio de estado al insertar cable	Status pasa a Active en el puerto correcto.	Cable, negociación, puerto o equipo remoto.
Trama sin etiqueta en access	La recibe la VLAN asociada al PVID.	Revisar Port VID y miembro untagged.
VLAN permitida en trunk	La etiqueta atraviesa el enlace hasta su destino.	Revisar membresía tagged y switch remoto.
VLAN no autorizada	No alcanza otros segmentos ni la CPU por error.	Revisar filtrado de grupos VLAN y política remota.
Interfaz asignada	Direccionamiento y servicios previstos funcionan.	Revisar Assignments, IP, DHCP, gateways y reglas.
Cambio reversible	Se conserva vía administrativa y respaldo.	Suspender intervención y usar procedimiento de recuperación.

Una prueba con ping no demuestra por sí sola que una VLAN esté correctamente aislada: debe verificarse también que el tráfico no autorizado no atraviesa la frontera. La inspección de paquetes o los diagnósticos deben realizarse solo en interfaces y equipos bajo administración legítima.

26.20. Resolución de incidencias frecuentes

Síntoma	Causa probable	Medida razonable
No Carrier con FORWARDING	Sin enlace físico pese a estado de conmutación.	Probar cable, energía y autonegociación.
Con enlace físico, sin dirección IP	VLAN mal clasificada, DHCP ausente o interfaz sin activar.	Revisar PVID y membresía antes de cambiar reglas.
Una VLAN no llega a pfSense	Falta membresía tagged del uplink interno.	Comprobar grupo VLAN y puerto interno según Netgate.
Trunk pasa una VLAN pero no otra	Membresía omitida o etiqueta discordante.	Comparar VID y tagging en ambos extremos.
Cliente aparece en red equivocada	PVID incorrecto o salida untagged en grupo erróneo.	Revisar VLAN de entrada y pertenencia del puerto.
Cortes al unir puertos	Bucle L2 o desconexión de estado Switch Port.	Separar bucles y revisar vínculo de estado de interfaz.
GUI inaccesible tras Save	Red de gestión dependía del puerto o grupo cambiado.	Acceso por consola y restauración del cambio aprobado.
Tráfico inter-puerto no aparece en firewall	Conmutación local dentro del chip.	Cambiar el diseño de aislamiento si se requiere filtrado.
Rendimiento menor del esperado	Uplink interno compartido o carga de CPU.	Medir tráfico real, rutas y límites físicos.

26.20.1. Método de diagnóstico no destructivo

Primero observar el estado; después comparar tres configuraciones (Ports, Switch VLANs y Assignments); luego ensayar conectividad con una fuente y destino de prueba autorizados. Evitar aplicar varios cambios simultáneos porque se perdería la trazabilidad de la causa. Mantener un registro privado de qué se modificó, cuál era el resultado esperado y cuál fue la verificación.

26.21. Gestión del cambio, copia de seguridad y recuperación

Antes de editar una red de gestión o un puerto que transporta servicios esenciales, generar una copia de seguridad desde Diagnostics → Backup & Restore, proteger el archivo y verificar que existe procedimiento de recuperación. Netgate documenta que las copias de configuración son sensibles y deben almacenarse de manera segura. En equipos con switch integrado, ciertas restauraciones ofrecen opciones específicas para conservar la configuración del switch: su utilización exige revisar la semántica exacta y las dependencias de VLAN.

Antes	Durante	Después
Confirmar ventana y alcance.	Cambiar una sola característica cada vez.	Repetir pruebas físicas y lógicas.
Copia de seguridad cifrada y protegida.	Mantener consola o camino independiente.	Verificar conexiones entrantes y salientes.
Inventario privado de dependencias.	Respetar grupos base y uplink.	Registrar resultado, impacto y retorno.
Plan de vuelta atrás verificable.	No ocultar errores abriendo reglas globales.	Guardar copia final tras validación.
Recuperación planificada. Si una operación impide acceder a la GUI, no repetir cambios a ciegas ni improvisar un reset de fábrica. Recuperar por la consola y el historial de configuración, o restaurar una copia compatible, conforme al procedimiento aprobado y a las opciones concretas del dispositivo.		

26.22. Glosario técnico del apartado Switch

Término	Definición
Switch integrado	Chip de conmutación Ethernet incorporado al dispositivo.
SoC	Sistema en chip que ejecuta pfSense y se comunica con el switch.
Puerto interno 0 / HOST	Enlace lógico del switch hacia el procesador en el modelo de referencia.

Término	Definición
PVID / Port VID	VLAN de entrada asignada a tramas sin etiqueta de un puerto.
VLAN tag / VID	Identificador 802.1Q contenido en la cabecera Ethernet.
VLAN group	Entrada de hardware que define una VLAN y sus miembros.
Tagged / t	Pertenencia con tráfico etiquetado en el puerto correspondiente.
Untagged	Pertenencia de VLAN con salida de tramas sin etiqueta.
Access / Trunk	Puerto de una VLAN para clientes / puerto que transporta varias VLAN etiquetadas.
Forwarding	Estado lógico del puerto apto para reenviar tramas.
Active / No Carrier	Indicadores de existencia o ausencia de portadora física.
Auto-negotiation	Acuerdo automático de velocidad y dúplex entre extremos.
STP	Protocolo para evitar bucles de capa 2; no implementado por el switch de referencia.
Switch Port (interfaz)	Opción de enlace del estado lógico al estado físico de un puerto en ciertos modelos.

26.23. Síntesis operativa

System indica qué es y qué soporta el chip. Ports muestra cómo está funcionando cada puerto y cómo clasifica sus tramas sin etiquetar. VLANs define los dominios de conmutación, los miembros y la forma en que las etiquetas atraviesan cada enlace. Finalmente, Interfaces → Assignments convierte los recursos de red que correspondan en interfaces pfSense con direccionamiento, filtrado y servicios. Una configuración correcta exige coherencia entre esos niveles y, especialmente, preservar el enlace interno y la red de gestión.

Regla profesional. No modificar una VLAN del switch sin responder: ¿qué puerto recibe la trama?, ¿qué PVID se aplica?, ¿por dónde sale etiquetada o sin etiqueta?, ¿llega a pfSense?, ¿quién permite o deniega después el tráfico?

Documentación oficial de Netgate

Netgate · Switch Overview	**Netgate · Configuring the Switch Ports**
Netgate · Configuring a Router on a Stick	Netgate · Input and Output Ports
Netgate · VLAN Configuration	Netgate · VLAN Terminology
Netgate · Interface Configuration	Netgate · Configuring Switches with VLANs
Netgate · Making Backups in the GUI	Netgate · Restoring from Backups
Netgate · Console Menu Basics	

Referencias oficiales con enlaces activos, verificadas el 17 de noviembre de 2026. Los menús y funciones varían según modelo, controlador y versión de pfSense Plus.

27 Interfaces → WAN

Identidad, direccionamiento, cliente DHCP, enlace y filtrado de redes reservadas

Ruta de administración: Interfaces → WAN. El identificador técnico del adaptador es dependiente del equipo y no es necesario para interpretar los controles de esta página.



Figura 27.1. Secuencia lógica de una interfaz WAN y sus dependencias entre capas, sin datos de instalaciones.

27.1. Propósito, alcance y contexto operativo

La interfaz WAN representa un punto de conexión externa del firewall. En pfSense Plus puede corresponder a una tarjeta física, una VLAN sobre un puerto físico, una interfaz virtual, o una interfaz de acceso de tipo PPP. Esta pantalla determina si la interfaz está habilitada, cómo obtiene parámetros IPv4 e IPv6 y cómo se comporta ante determinadas situaciones de capa 2 y de filtrado de orígenes. El nombre WAN es una designación administrativa, no una garantía de que el enlace tenga salida a Internet.

En una plataforma con switch integrado, el cable físico, su estado de portadora, la VLAN interna, la interfaz del sistema y la configuración IP constituyen elementos relacionados pero distintos. El diagnóstico correcto empieza por separar estas capas antes de atribuir el fallo a DHCP, NAT o reglas del firewall.

Alcance de interfaz. Los controles desarrollados en detalle están presentes en el formulario correspondiente. Los campos de IPv4 estática, DHCP6 y PPP descritos más adelante son opciones condicionales documentadas oficialmente: su presencia exacta cambia con la selección, la plataforma y la versión de pfSense Plus.

27.2. Localización de la página y estructura visible

Desde el menú Interfaces se selecciona WAN para abrir el formulario de configuración de esa interfaz. La página descrita se organiza en General Configuration, DHCP Client Configuration y Reserved Networks. Dependiendo de IPv4 Configuration Type y de IPv6 Configuration Type, pueden desplegarse bloques de campos adicionales. Los botones Save y, posteriormente, Apply Changes completan la secuencia habitual de guardar y aplicar, aunque su posición puede variar entre versiones.

Bloque visible	Qué administra	Efectos principales
General Configuration	Activación; nombre; modos IPv4/IPv6; MAC; MTU/MSS; promiscuo; enlace a puerto de switch.	Disponibilidad del enlace y definición de la interfaz lógica.
DHCP Client Configuration	Identificación del cliente; alias; servidores rechazados; prioridad 802.1p; controles avanzados.	Negociación y mantenimiento de la concesión IPv4 por DHCP.

Bloque visible	Qué administra	Efectos principales
Reserved Networks	Bloqueo de redes privadas/loopback y de redes bogon.	Reglas automáticas de filtrado del tráfico entrante.
Save / Apply Changes	Persistencia y aplicación operativa de las modificaciones.	Puede reiniciar el enlace o cambiar inmediatamente las rutas y servicios.

27.3. Enable interface: activación y consecuencias

Enable interface habilita administrativamente la interfaz. Activada, el sistema puede inicializarla conforme a su tipo de dirección, aceptar su estado de enlace y asociarle servicios, reglas y rutas. Desactivada, la interfaz permanece asignada en la configuración, pero deja de operar como conexión activa. La casilla no controla por sí sola que el equipo aguas arriba responda, que exista portadora física o que se obtenga una concesión DHCP.

Estado	Resultado esperado	Implicación administrativa
Activado	La interfaz puede configurar dirección, rutas y servicios según su modalidad.	Comprobar Status → Interfaces y pasarela.
Desactivado	No se usa normalmente para comunicar tráfico a través de esa asignación.	Puede detener Internet, VPN, NAT, rutas por defecto o acceso remoto.
Activado, sin carrier	Existe configuración, pero no hay enlace físico utilizable.	Revisar puertos, cableado y equipo remoto.
Activado, sin concesión	Hay enlace, pero falta direccionamiento dinámico.	Revisar DHCP, VLAN, identidad y operador.
Advertencia de continuidad. No deshabilitar la WAN desde una sesión remota que depende de ella. Antes de realizar cambios de impacto, confirmar acceso alternativo (consola local, conexión de gestión independiente o ruta secundaria realmente funcional).		

27.4. Description: nombre administrativo

Description es el nombre mostrado en el menú Interfaces y en múltiples selectores y apartados de la GUI: reglas, servicios, estados y gráficos. Netgate restringe estos nombres a letras, números y guion bajo como carácter especial. Una denominación breve y significativa facilita el diagnóstico y reduce los errores humanos al seleccionar interfaces en reglas, gateways o servicios.

Cambiar la descripción no modifica el cable, el puerto, la etiqueta VLAN ni transforma un enlace privado en público. Es prudente comprobar referencias visuales en documentación y procedimientos después de renombrar, especialmente cuando existen automatizaciones o inventarios ajenos a pfSense.

27.5. IPv4 Configuration Type: todas las opciones del selector

Este selector define la forma de obtener o establecer direcciones IPv4 en WAN. La elección correcta depende exclusivamente de lo que entregue el proveedor o el equipo intermedio. Seleccionar DHCP no significa que la dirección recibida deba ser necesariamente pública; algunos enlaces entregan direcciones privadas o de CGNAT.

Valor del selector	Modo operativo	Cuándo procede / riesgo
None	No se configura dirección IPv4 en esa interfaz.	Enlace solo IPv6 o interfaz con IP gestionada por otra tecnología; evita esperar DHCPv4.
Static IPv4	Dirección, prefijo y gateway introducidos manualmente.	Accesos con parámetros fijos; un gateway incorrecto provoca pérdida de salida.
DHCP	El cliente negocia IP, máscara, gateway y otros parámetros.	Acceso automático; requiere respuesta de servidor DHCP válido.
PPP	Enlace punto a punto de la familia PPP.	Casos de acceso específicos y heredados; comprobar medio físico.
PPPoE	Sesión PPP sobre Ethernet.	Proveedor que exige autenticación y encapsulado PPPoE.

Valor del selector	Modo operativo	Cuándo procede / riesgo
PPTP	Tipo de acceso PPP mediante túnel PPTP.	Tecnología heredada: no adoptarla para nuevas conexiones sin justificación.
L2TP	Tipo de acceso de enlace con L2TP.	Aplicaciones legadas; verificar requisitos y seguridad del servicio.

27.5.1. Campos condicionales de Static IPv4

La documentación de Netgate indica que Static IPv4 despliega IPv4 Address, CIDR Subnet Mask e IPv4 Upstream Gateway. La dirección y el prefijo deben corresponder al segmento definido para el enlace; el gateway debe ser alcanzable según la topología prevista. Para una interfaz interna no debe seleccionarse un gateway como si fuese una WAN, pues influye en su clasificación para NAT y otras funciones.

Ejemplo puramente documental: el espacio TEST-NET-1, 192.0.2.0/24, sirve para ilustrar formato de direcciones; no representa un circuito real y no es una configuración lista para aplicar. Los gateway y prefijos operativos los debe proporcionar el operador.

27.5.2. PPP, PPPoE, PPTP y L2TP

Los modos de la familia PPP remiten a interfaces que pueden necesitar credenciales, parámetros de sesión u opciones de transporte. Netgate documenta su configuración avanzada bajo Interfaces → Assignments → PPPs. PPPoE continúa siendo un modelo de acceso ISP habitual, mientras que PPTP y determinados usos de L2TP son legados y requieren una evaluación de seguridad y compatibilidad específica. No se deben rellenar valores por analogía con otra tecnología.

27.6. IPv6 Configuration Type: modos disponibles

El sistema IPv6 es independiente del modo IPv4. Puede existir WAN dual stack, WAN solo IPv4 o WAN solo IPv6. La documentación oficial indica que el operador determina cómo se anuncian direcciones, rutas y prefijos; una selección que funciona en otra conexión no constituye evidencia de que sea correcta.

Valor	Comportamiento principal	Observación práctica
None	Deshabilita la configuración IPv6 en la interfaz.	Adecuado cuando el acceso no ofrece IPv6.
Static IPv6	Configura manualmente dirección, prefijo y gateway ascendente.	Necesita datos de asignación y encaminamiento del proveedor.
DHCP6	Utiliza cliente DHCPv6 para dirección/opciones y, si corresponde, delegación de prefijos.	La ruta/gateway IPv6 procede de Router Advertisements, no de DHCPv6.
SLAAC	Genera dirección a partir de anuncios de router (RA).	DNS puede requerir RDNSS o DHCPv6 según proveedor.
6rd Tunnel	Transporta IPv6 por una infraestructura IPv4 del ISP.	Exige parámetros 6rd específicos; alternativa de transición.
6to4 Tunnel	Mecanismo histórico de encapsulación IPv6 en IPv4.	No es una elección preferible en despliegues actuales.
Track Interface	Utiliza prefijo delegado en otra interfaz ascendente.	Más habitual en LAN/DMZ dependiente de WAN, no en la WAN de acceso.

27.6.1. DHCP6 y delegación de prefijos

Si se elige DHCP6 pueden aparecer opciones adicionales: Request only an IPv6 Prefix, DHCPv6 Prefix Delegation Size, Send IPv6 Prefix Hint, Do not wait for a RA, Use IPv4 Connectivity as Parent Interface, ajustes avanzados y configuración de prioridad VLAN. Un prefijo delegado permite, por ejemplo, que interfaces internas con Track Interface utilicen bloques IPv6 del proveedor. Los tamaños y banderas dependen del ISP y no deben suponerse.

27.6.2. Precaución sobre IPv6 y filtros

IPv6 necesita determinados intercambios de control —como Neighbor Discovery y Router Advertisements — que no deben bloquearse de manera indiscriminada. Un problema de IPv6 puede ser independiente de

IPv4 y viceversa. Para comprobarlo, revisar direcciones, gateway IPv6 y registros con el mismo rigor que en IPv4.

27.7. MAC Address: identidad Ethernet y particularidad de las VLAN

La dirección MAC identifica una interfaz en el dominio Ethernet y, en determinados escenarios, puede ser utilizada por el equipo de acceso o por el proveedor para reconocer un dispositivo. En la página estudiada aparece una advertencia expresa: «The MAC address of a VLAN interface must be set on its parent interface». Es decir, para una interfaz VLAN la modificación de MAC, si procede, debe realizarse sobre su interfaz padre; no directamente en la subinterfaz virtual.

Netgate desaconseja forzar una MAC salvo necesidad concreta. Ante una sustitución de router puede ser suficiente renovar tablas ARP del equipo vecino, reiniciar el dispositivo de acceso o esperar a su caducidad. La clonación indiscriminada introduce el riesgo de MAC duplicada y de conflictos con el equipo sustituido.

Separación de funciones. Una MAC no determina la IP WAN, el VLAN ID, el gateway o el estado de reglas. No cambiarla por ensayo y error: comprobar primero qué mecanismo de identificación utiliza el proveedor.

27.8. MTU: tamaño de paquete y efectos operativos

MTU (Maximum Transmission Unit) fija el tamaño máximo de paquete de capa 3 que puede transportarse sin recurrir a mecanismos de fragmentación y adaptación. Si se deja en blanco, se usa el MTU por defecto del adaptador y de la modalidad, que en Ethernet convencional suele ser 1500 bytes. No obstante, el encapsulado, PPPoE, túneles y enlaces especiales pueden imponer un valor efectivo menor.

Situación	Interpretación	Decisión profesional
Campo MTU vacío	pfSense usa el valor adecuado por defecto para el tipo de enlace.	Opción normal cuando no hay requisito distinto.
Paquetes pequeños funcionan y grandes fallan	Posible Path MTU Discovery roto o encapsulado adicional.	Medir tamaño de paquetes/ICMP; no reducir por intuición.
Acceso con túnel superpuesto	Encabezados adicionales reducen el espacio útil.	Ajustar de acuerdo con la tecnología y sus extremos.
MTU demasiado alto	Paquetes pueden perderse o necesitar tratamiento no disponible.	Revisar red completa y limitaciones de dispositivo.
MTU demasiado bajo	Puede aumentar el número de paquetes por volumen de datos.	Evitar reducir sin fundamento técnico.

27.9. MSS: ajuste de segmentos TCP y PMTUD

MSS (Maximum Segment Size) es el tamaño máximo de datos TCP anunciado durante el establecimiento de conexiones. La pantalla estudiada explica que, al introducir un valor en su campo MSS, pfSense aplica limitación (clamping) utilizando ese valor menos 40 bytes en IPv4 y menos 60 bytes en IPv6, correspondientes a las cabeceras TCP/IP básicas señaladas por la ayuda. Por ello, el valor introducido no debe interpretarse sin más como tamaño neto del segmento TCP.

El MSS clamping puede mitigar fallos de Path MTU Discovery en sesiones TCP, especialmente con túneles o encapsulados. No arregla por sí mismo todos los problemas de UDP, ICMP, fragmentación, etiquetas VLAN o problemas físicos. Cuando el acceso funciona normalmente, conviene dejarlo en blanco y no imponer límites innecesarios.

Campo configurado	Consecuencia indicada por la ayuda	Nota de interpretación
MSS vacío	No se impone ajuste manual en este campo.	Pueden existir otras limitaciones por encapsulado/protocolos.
MSS con valor M	Clamping anunciado: M − 40 para IPv4 y M − 60 para IPv6.	La ayuda usa encabezados básicos; el tráfico real puede tener opciones.
MTU y MSS ajustados	Se modifican dos aspectos relacionados, pero diferentes.	Verificar resultados mediante pruebas y captura TCP.

27.10. Promiscuous Mode: recepción de tramas Ethernet

Enable Promiscuous Mode pone la interfaz en modo promiscuo permanentemente. En términos de capa 2, puede permitir que la pila de red observe tramas que no se dirigen a la MAC unicast de la interfaz, siempre que el hardware, el switch y el entorno permitan que lleguen. No convierte automáticamente a pfSense en un puente transparente, no desactiva el firewall y no garantiza que el switch entregue tráfico de otros puertos.

En una WAN convencional se suele mantener desactivado. Puede requerirse en configuraciones especiales de puente, autenticación o diagnóstico; Netgate describe casos específicos de paso de autenticación 802.1X que emplean este ajuste. Activarlo sin necesidad puede incrementar tráfico procesado y ampliar la visibilidad de tramas, por lo que su uso debe estar motivado y verificado.

27.11. Switch port: asociación entre interfaz virtual y portadora física

En equipos Netgate con switch integrado, el selector «Select the Switch port to monitor for media state changes» permite hacer que una interfaz lógica basada en VLAN refleje el estado de un puerto físico del switch. La lista exacta de puertos varía según la plataforma. Su función principal es observar los cambios de portadora para indicar si esa interfaz está operativamente conectada.

Sin asociación a un puerto físico, la interfaz VLAN puede aparecer como enlazada porque su enlace padre interno se mantiene activo, aun cuando el conector externo esté desconectado. Si se selecciona un puerto equivocado, los eventos de conexión/desconexión de una boca ajena podrían afectar a la lectura de estado de la interfaz y a servicios dependientes. Si una VLAN opera en más de un conector, no conviene hacer depender indebidamente toda la red de uno solo: Netgate advierte de ello en sus ejemplos de configuración del switch.

Precaución de plataforma. Este control solo existe en ciertos aparatos con switch integrado. No debe confundirse con «Interface Assignments», con la VLAN padre ni con el selector de velocidad y dúplex de Interfaces → Switch → Ports.

27.12. DHCP Client Configuration: funcionamiento general

La sección DHCP Client Configuration aparece en el contexto de una WAN con IPv4 Configuration Type = DHCP. La operación básica suele seguir el intercambio DISCOVER, OFFER, REQUEST y ACK. La concesión describe parámetros asignados temporalmente por un servidor: la renovación puede cambiar IP, gateway, DNS u otras opciones y es independiente de que el enlace Ethernet esté activo.

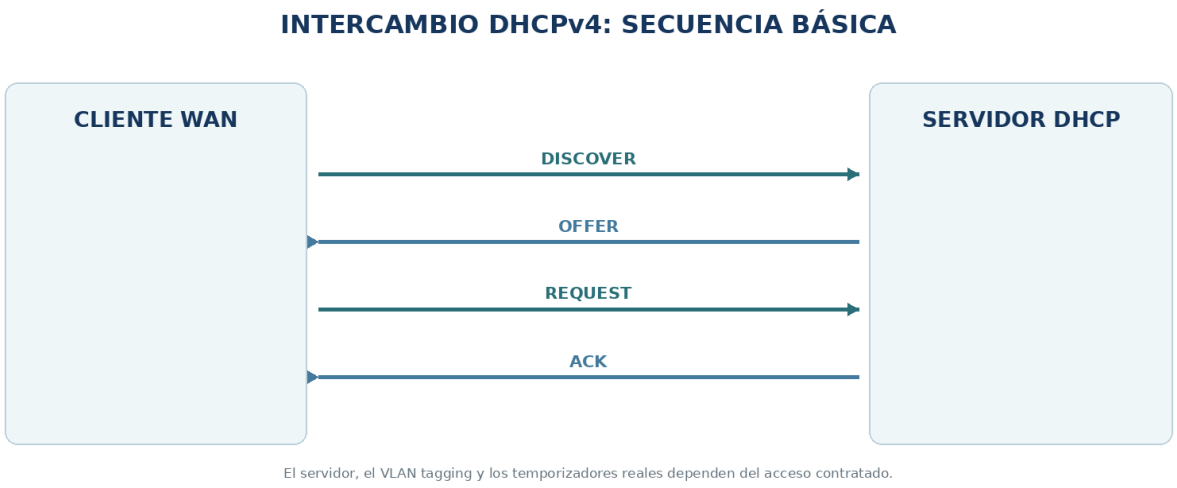


Figura 27.2. Diálogo conceptual DHCPv4, independiente de cualquier dirección, identificador o proveedor.

Una oferta recibida no demuestra por sí sola que exista conexión a Internet: tras obtener una dirección debe verificarse gateway, ruta por defecto, resolución DNS, NAT y reglas. Un firewall puede tener una concesión correcta y seguir sin acceso por políticas o rutas.

27.13. Options: Advanced Configuration y Configuration Override

Control	Desactivado	Activado / advertencia
Advanced Configuration	El cliente DHCP usa normalmente valores predeterminados de temporización.	Expone parámetros avanzados de tiempos y comportamiento de dhclient; cambiar solo por necesidad documentada.
Configuration Override	pfSense gestiona la configuración del cliente desde los campos estándar.	Permite usar un archivo completo alternativo de configuración dhclient; una ruta o sintaxis errónea puede impedir la concesión.

Netgate considera excepcionales ambos controles. Advanced Configuration puede desplegar campos de protocolo y presets, mientras que Configuration Override activa una ruta de archivo para una configuración personalizada. Esta última no es un botón de restauración ni significa ignorar un valor aislado: se trata de sustituir la configuración utilizada por el cliente DHCP, bajo control administrativo.

27.14. Hostname: identificación ante el servidor DHCP

El campo Hostname es enviado durante la solicitud DHCP como nombre de host y, según la documentación de Netgate, también se emplea en la identificación del cliente. Algunos proveedores vinculan la autorización a un identificador previsto; otros ignoran completamente ese dato. Dejarlo vacío cuando no se necesita reduce la posibilidad de que un valor inadecuado provoque rechazo de la concesión.

El valor es administrativo y puede revelar información de nomenclatura al extremo remoto. En un entorno empresarial no es aconsejable utilizar nombres internos sensibles en identificadores intercambiados con un tercero. No confundir Hostname del cliente DHCP con el hostname del propio firewall ni con un nombre DNS público.

27.15. Alias IPv4 address: dirección auxiliar fija junto a DHCP

Alias IPv4 address permite definir una dirección secundaria fija para el cliente DHCP, por ejemplo para administrar un equipo aguas arriba situado en una red de gestión separada de la concesión dinámica. El selector de prefijo que aparece a su lado especifica la longitud CIDR. Su utilización no sustituye la concesión IPv4 principal ni crea automáticamente la ruta adecuada si el diseño requiere medidas adicionales.

El prefijo ha de coincidir con el ámbito en que se necesite alcanzar ese dispositivo; un alias inadecuado puede causar colisiones de subred o introducir rutas conectadas inesperadas. Netgate lo documenta como alternativa frente a un VIP de tipo IP Alias convencional en una interfaz controlada por DHCP.

Ejemplos seguros. Si se necesita ilustrar una dirección de prueba, usar únicamente prefijos reservados para documentación como 192.0.2.0/24; no aplicarlos como si fueran valores válidos de producción. No se incluye en este capítulo ningún alias real.

27.16. Reject leases from: servidores DHCP no deseados

Reject leases from acepta una o varias direcciones IPv4 separadas por comas. El cliente descarta las ofertas emitidas por esos servidores. Netgate describe el caso de equipos de acceso que, cuando pierden sincronismo aguas arriba, responden con una concesión privada propia: el firewall podría aceptar esa oferta y aparentar que tiene IP aunque el circuito WAN real esté caído.

Este filtro no es un sustituto de DHCP Snooping en la red ni bloquea de modo universal todos los servidores DHCP maliciosos. Su utilidad consiste en impedir concesiones originadas por servidores concretos cuya dirección es conocida. No utilizarlo para bloquear por error al servidor legítimo del operador, ya que ello produciría ausencia de configuración IPv4.

27.17. DHCP VLAN Priority: prioridad 802.1p/PCP

Enable dhcpclient VLAN Priority tagging habilita el marcado de prioridad IEEE 802.1p del tráfico del cliente DHCP. Tras marcarlo, el desplegable permite escoger un PCP entre 0 y 7. Este ajuste solo debe habilitarse cuando el operador lo exija y haya especificado el valor. No equivale a elegir una VLAN ID ni garantiza priorización extremo a extremo del tráfico ordinario.

Etiqueta del desplegable	PCP	Uso semántico en la ayuda
Background (BK)	0	Tráfico de fondo.
Best Effort (BE)	1	Mejor esfuerzo; categoría que Netgate indica como predeterminada sin PCP explícito.
Excellent Effort (EE)	2	Mejor esfuerzo mejorado.
Critical Applications (CA)	3	Aplicaciones críticas.
Video (VI)	4	Tráfico de vídeo.
Voice (VO)	5	Tráfico de voz.
Internetwork Control (IC)	6	Control de interconexión.
Network Control (NC)	7	Control de red.

El selector define la semántica de las marcas PCP, no la prioridad efectiva acordada por una red pública: cada red puede tratar los valores de manera diferente. Como disciplina de troubleshooting, primero comprobar presencia de etiqueta y marcado solicitados por el operador; después comprobar la respuesta DHCP.

27.18. Reserved Networks: objetivo y ubicación de las reglas

Reserved Networks ofrece dos filtros independientes aplicados en la interfaz para tráfico entrante desde fuentes no esperadas en un enlace exterior. No deben confundirse con el NAT saliente, con una regla general de rechazo ni con el filtrado de puertos TCP/UDP. Su función debe evaluarse frente al tipo de conexión contratado y a los bloques de origen que realmente pueden circular por ella.



Figura 27.3. Criterio inicial para evaluar el bloqueo de direcciones privadas en la WAN.

27.19. Block private networks and loopback addresses

La casilla «Block private networks and loopback addresses» crea un filtro automático contra tráfico de origen procedente de rangos privados IPv4 RFC 1918 y de loopback. La ayuda de pantalla incluye también direcciones locales únicas IPv6 (ULA, RFC 4193) cuando corresponda. La finalidad es descartar fuentes que no deberían llegar desde una WAN pública directamente enrutada.

Rango / categoría	Concepto	Criterio operacional
10.0.0.0/8	Dirección IPv4 privada RFC 1918.	Puede ser legítima en accesos privados.
172.16.0.0/12	Dirección IPv4 privada RFC 1918.	Bloquearla en una WAN privada puede cortar servicios.
192.168.0.0/16	Dirección IPv4 privada RFC 1918.	Frecuente en equipos de acceso y router interpuesto.
127.0.0.0/8	Loopback IPv4.	No debería aparecer como origen externo normal.

Rango / categoría	Concepto	Criterio operacional
fc00::/7	Direcciones ULA IPv6 según ayuda visible.	No deshabilitar IPv6 válido indiscriminadamente.

En una WAN con IPv4 pública directa suele ser razonable dejar activo el bloqueo. En una WAN tras un router intermedio, en un acceso privado del operador, en ciertos túneles o en enlaces de tránsito internos, las fuentes privadas pueden ser legítimas y es necesario revisar su estado antes de habilitarlo. También el entorno CGNAT requiere estudiar qué tráfico entrante se espera: la dirección asignada al interfaz, por sí sola, no determina todos los orígenes que pueden llegar.

Precisión importante. Una casilla de bloqueo de orígenes privados actúa sobre tráfico recibido, no significa que pfSense prohíba por definición obtener mediante DHCP una IP WAN privada. La distinción entre dirección de interfaz y origen del paquete evita diagnósticos equivocados.

27.20. Block bogon networks

Block bogon networks utiliza listas de prefijos no asignados, reservados o impropios del encaminamiento público. pfSense mantiene tablas para IPv4 e IPv6, actualizables desde servidores de Netgate. Su valor es especialmente claro en interfaces externas expuestas a tráfico de Internet; en interfaces internas puede descartar paquetes necesarios, especialmente en IPv6.

La pantalla visible precisa que esta opción no sustituye el bloqueo RFC 1918 y recomienda reservarla para interfaces WAN. La frecuencia de actualización se configura en System → Advanced → Firewall & NAT (Update Frequency for bogons). Si la actualización falla, se puede investigar la resolución DNS y consultar Diagnostics → Tables; las rutas concretas deben confirmarse según versión.

Estado	Interpretación	Recomendación
Activado en WAN pública	Descarta fuentes incluidas en tablas bogon actualizadas.	Usarlo cuando no se esperan rangos especiales y esté verificada la lista.
Desactivado	No agrega ese filtro automático concreto.	Solo cuando el diseño requiera tráfico que el filtro eliminaría.
Activado en LAN/DMZ	Puede bloquear tráfico interno legítimo.	Evitar salvo justificación técnica excepcional.
Lista no actualizada	Puede no reflejar asignaciones recientes.	Comprobar DNS, conectividad y mantenimiento de tablas.

27.21. Save y Apply Changes: ciclo de aplicación seguro

En pfSense Plus, Save almacena los valores enviados desde el formulario. Cuando aparece un aviso de cambios pendientes, Apply Changes hace efectiva la nueva configuración. Algunas modificaciones pueden reiniciar el cliente DHCP, actualizar la interfaz, las rutas o las reglas. Un fallo de acceso a la GUI no implica necesariamente corrupción de configuración: puede haberse cambiado la ruta o el enlace desde el que se estaba conectado.

01. Registrar el objetivo del cambio, el valor actual y la condición verificable de éxito.
02. Realizar una copia XML completa desde Diagnostics → Backup & Restore y protegerla como información sensible.
03. Garantizar acceso de recuperación independiente del enlace modificado; establecer una ventana de mantenimiento.
04. Modificar solo los campos necesarios y revisar especialmente Enable, IPv4/IPv6, gateway, Switch port y filtros de origen.
05. Pulsar Save, comprobar el resumen y aplicar cambios cuando la GUI lo solicite.
06. Revisar Status → Interfaces, estados de gateway, DNS, rutas y registros; probar tráfico real.
07. Si el resultado es incorrecto, restaurar los valores previos o recuperar una versión válida desde historial/backup mediante acceso seguro.

27.22. Procedimiento práctico A: WAN que obtiene IPv4 por DHCP

01. Comprobar que el puerto y la VLAN del acceso están correctamente definidos en Interfaces → Switch y/o Interfaces → Assignments si el hardware lo requiere.

02. Ir a Interfaces → WAN y marcar Enable interface.
03. Revisar Description sin incorporar nombres de sistemas internos o de personas.
04. Establecer IPv4 Configuration Type = DHCP.
05. Elegir IPv6 Configuration Type según las especificaciones reales del operador; no suponer que DHCP6 es siempre correcto.
06. Dejar MTU, MSS, MAC y opciones DHCP avanzadas sin forzar si el operador no exige cambios.
07. Mantener desactivado DHCP VLAN Priority salvo instrucción expresa del proveedor.
08. Evaluar Reserved Networks según sea un acceso público directo o un tramo privado de tránsito.
09. Guardar, aplicar y validar dirección, gateway, rutas, DNS y acceso de servicio.

27.23. Procedimiento práctico B: WAN con IPv4 estática

01. Confirmar por escrito el bloque IPv4, máscara CIDR y gateway ascendente del enlace.
02. Seleccionar Static IPv4 y rellenar los campos condicionales que aparecen.
03. Comprobar que no se crea conflicto con ninguna red interna, alias o interfaz activa.
04. Configurar IPv6 de forma independiente, si está contratado.
05. Evaluar MTU, MSS y filtros de origen conforme al enlace, no por copiar otra WAN.
06. Guardar y aplicar desde un punto con acceso local o alternativo disponible.
07. Verificar ruta por defecto, monitorización de pasarela y conectividad tanto saliente como de servicios publicados autorizados.

27.24. Procedimiento práctico C: WAN con puerto físico monitorizado

01. En Interfaces → Switch → Ports, identificar en documentación propia el conector que realmente recibe el enlace externo, sin asumir numeraciones universales.
02. Comprobar que la VLAN lógica de esa WAN tiene la pertenencia y el etiquetado correctos.
03. Volver a Interfaces → WAN y seleccionar en Switch port el puerto físico cuya portadora deba gobernar el estado lógico.
04. Guardar y aplicar; validar comportamiento mediante una intervención controlada sobre el cable o el equipo remoto.
05. Comprobar que la desconexión del puerto supervisado se refleja correctamente sin activar o desactivar otras interfaces.
06. En configuraciones multipuerto, confirmar que no se introduce una dependencia inesperada de un solo conector.

27.25. Procedimiento práctico D: resolver incidencias de MTU/MSS

01. Reproducir un fallo concreto y anotar aplicación, protocolo y patrón: por ejemplo, conexiones TCP que establecen sesión pero fallan al transferir cargas mayores.
02. Comprobar primero si existe pérdida física, errores de interfaz, fallo DNS o rutas asimétricas.
03. Consultar MTU esperado para Ethernet, PPPoE y túneles empleados; revisar cabeceras adicionales.
04. Realizar pruebas de tamaño con tráfico de laboratorio que permitan observar ICMP y descubrimiento de MTU, cuando la red lo admita.
05. Aplicar un cambio mínimo y documentado en MTU o MSS, no ambos simultáneamente sin razón.
06. Verificar con captura TCP las opciones MSS en SYN y con pruebas reales las aplicaciones afectadas; revertir si no mejora.

27.26. Escenarios empresariales y criterios de decisión

Escenario genérico	Configuración razonable	Aspecto a verificar
Acceso empresarial con concesión IPv4 automática	WAN habilitada y DHCP, sin opciones de cliente especiales salvo requisitos expresos.	Validez de lease, gateway, DNS y monitorización.
Circuito con datos IPv4 fijos	Static IPv4 y gateway definido por el operador.	Ruta predeterminada, ARP y dirección/prefijo.
Tránsito por red privada antes de Internet	Revisar bloqueo RFC1918 y posibles excepciones.	Que no se descarten orígenes legítimos.
Conexión ISP con PPPoE	PPPoE con parámetros acreditados y MTU apropiada.	Sesión PPP y efecto sobre tamaño de paquetes.
Dual stack con prefijo IPv6 delegado	WAN DHCP6 según ISP; LANs con Track Interface cuando proceda.	RA, delegación, gateway IPv6 y reglas IPv6.
VLAN WAN sobre switch integrado	Consistencia entre switch, VLAN lógica, asignación y Switch port.	VLAN tag/membresía, carrier y reglas.

27.27. Métodos de comprobación y diagnóstico

Comprobación	Dónde / herramienta	Qué resuelve
Estado de interfaz	Status → Interfaces	Carrier, direcciones, concesiones, estado de enlace y renovaciones.
Monitorización del gateway	Status → Gateways y System → Routing	Latencia/pérdida y pasarelas predeterminadas o configuradas.
Registros de DHCP y sistema	Status → System Logs	Concesiones rechazadas, renovaciones y mensajes del enlace.
Tablas bogon	Diagnostics → Tables	Presencia de redes bogon y, según versión, actualización.
Captura de paquetes	Diagnostics → Packet Capture	DHCP, tráfico entrante, SYN/MSS, ICMP y etiquetado observado.
Resolución de nombres	Diagnostics → DNS Lookup	Separar fallo DNS de falla de transporte IP.
Pruebas de conectividad	Diagnostics → Ping y Traceroute	Rutas desde la propia interfaz y saltos de red.
Control de reglas	Firewall → Rules / Logs	Descartes explícitos/implícitos y políticas de interfaz.

Para DHCPv4, revisar que se observan DISCOVER y OFFER, y si no hay oferta, verificar primero VLAN, portadora, posibles filtros y servidor remoto. Para Internet parcial, comprobar si la WAN tiene IP y gateway y después DNS, rutas, NAT y firewall. En una sesión PPP, usar los controles Connect/Disconnect descritos en Status → Interfaces cuando correspondan al tipo de conexión. No iniciar Release o desconexión de una WAN de producción desde la única sesión remota.

27.28. Errores frecuentes y resolución sistemática

Síntoma	Causa posible	Verificación / corrección
WAN aparece habilitada, sin IP	Sin concesión, modo IPv4 incorrecto, VLAN no concordante.	Comprobar enlace, DHCP y requisitos del proveedor.
Se obtiene IP pero no hay navegación	Gateway, rutas, DNS, NAT o reglas.	Separar conectividad IP de resolución de nombres.
WAN parece activa sin cable	VLAN lógica sobre enlace padre interno.	Configurar Switch port adecuado si procede.
El enlace se cae al modificar Switch port	Se monitoriza el puerto equivocado.	Revisar asignación y revertir con consola.
Servicios de operador privado dejan de funcionar	Bloqueo automático de RFC1918/ULA o bogons.	Inspeccionar fuentes esperadas y reglas de filtrado.
DHCP ofrece parámetros erróneos	Servidor no deseado o tramo de acceso averiado.	Usar Reject leases from solo si se conoce el servidor rechazado.

Síntoma	Causa posible	Verificación / corrección
VPN funciona de forma intermitente	Cambio de gateway, IP dinámica, MTU o MSS.	Verificar rutas, DPD/túnel y tamaño efectivo de paquete.
TCP establece conexión pero se atasca	Path MTU Discovery o encapsulado.	Analizar con capturas y pruebas de paquetes grandes.
IPv4 correcto, IPv6 falla	Falta RA, DHCP6/PD incorrecto o reglas ICMPv6.	Verificar RA, prefijo, gateway y firewall IPv6.
Cambios en MAC no tienen efecto en VLAN	La MAC corresponde al interfaz padre.	No clonar en subinterfaz; revisar la interfaz principal.

27.29. Seguridad, disponibilidad y recomendaciones profesionales

La interfaz WAN es un componente de alta criticidad. El principio rector es cambiar una variable cada vez, documentar los valores anteriores y comprobar el resultado desde una ruta de administración controlada. Ningún filtro automático sustituye al principio de mínimo privilegio en reglas, a la segmentación de red ni a un diseño correcto de NAT y enrutamiento.

01. Mantener Enable solo en interfaces necesarias y monitorizar su estado de conexión.
02. Preferir parámetros de ISP documentados antes que configuraciones copiadas de otro acceso.
03. Dejar MTU, MSS y MAC sin forzar salvo necesidad comprobable y medible.
04. No activar Promiscuous Mode en conexiones ordinarias sin objetivo claro.
05. Confirmar si la WAN es pública, privada o CGNAT antes de habilitar bloqueos automáticos.
06. Aplicar las políticas IPv4 e IPv6 por separado, verificando cada pila.
07. Conservar acceso de consola y un backup XML fuera del firewall, cifrado y con control de accesos.
08. Registrar cambios de gateways, DHCP, VLAN y puertos en mantenimiento programado; comprobar VPN y servicios afectados después de aplicar.

27.30. Resumen de administración y lista de verificación

Punto de control	Pregunta de aceptación
Habilitación y nombre	¿La interfaz está activa y su descripción es inequívoca?
Modalidad IP	¿IPv4 e IPv6 coinciden con el servicio real contratado?
Capa 2 / VLAN	¿Portadora, switch, etiqueta y VLAN padre están coordinados?
Identificación DHCP	¿Hostname/cliente y opciones adicionales solo se definen cuando son necesarias?
Dirección / gateway	¿Hay concesión o configuración estática correcta y pasarela alcanzable?
MTU / MSS	¿Están vacíos salvo necesidad validada por prueba?
Promiscuous / Switch port	¿Se han empleado únicamente si el diseño los requiere?
Reservadas / bogons	¿No bloquean redes legítimas en el tipo de WAN implantada?
Diagnóstico y recuperación	¿Existen rutas de gestión, copia segura y pruebas tras cada cambio?

27.31. Glosario técnico

Término	Definición operativa
WAN	Interfaz de acceso o tránsito externo; no implica automáticamente IP pública.
Carrier	Detección de señal/enlace en el puerto físico Ethernet.
DHCP lease	Concesión de configuración IP por una duración y condiciones definidas.
DHCPv6-PD	Prefix Delegation: asignación dinámica de un prefijo IPv6 enrutable.

Término	Definición operativa
RA	Router Advertisement: anuncio que proporciona información de router IPv6.
MTU / MSS	Máximo paquete IP transportable / máximo bloque útil TCP anunciado.
802.1p PCP	Campo de prioridad de capa 2 con valores entre 0 y 7.
RFC1918 / ULA	Espacios privados de direcciones IPv4 / locales únicos IPv6.
Bogon	Prefijo reservado, no asignado o no adecuado como origen de Internet.
Promiscuous	Modo de interfaz que permite recibir tramas no dirigidas a su MAC, si llegan al adaptador.

27.32. Referencias oficiales de Netgate

Fuentes documentales de pfSense Plus y pfSense Software, consultadas el 17 de noviembre de 2026. La presentación de campos puede cambiar con la versión exacta y con el modelo de hardware. Estas fuentes describen las capacidades genéricas; cuando aparece un campo condicional se ha indicado expresamente en el capítulo.

Interface Configuration — https://docs.netgate.com/pfsense/en/latest/interfaces/configure.html

IPv4 Configuration Types — https://docs.netgate.com/pfsense/en/latest/interfaces/configure-ipv4.html

IPv6 Configuration Types — https://docs.netgate.com/pfsense/en/latest/interfaces/configure-ipv6.html

VLAN Priority — https://docs.netgate.com/pfsense/en/latest/vlan/priority.html

Interface Status — https://docs.netgate.com/pfsense/en/latest/monitoring/status/interfaces.html

Configuring the Switch Ports — https://docs.netgate.com/pfsense/en/latest/solutions/sg-1100/configuring-the-switch-ports.html

WAN Connectivity with 802.1X Authentication Bridging — https://docs.netgate.com/pfsense/en/latest/recipes/authbridge.html

Block Bogon Networks / Rule Methodology — https://docs.netgate.com/pfsense/en/latest/firewall/rule-methodology.html

Bogon Network List Updates — https://docs.netgate.com/pfsense/en/latest/general/netgate-servers.html

Packet Capture GUI — https://docs.netgate.com/pfsense/en/latest/diagnostics/packetcapture/webgui.html

Making Backups in the GUI — https://docs.netgate.com/pfsense/en/latest/backup/configuration.html

28 Interfaces → LAN

Dirección local, gateway, delegación IPv6 y controles de seguridad

Ruta: Interfaces → LAN. Los nombres técnicos de los controles se mantienen en inglés, tal como figuran en pfSense Plus. Los identificadores físicos y las direcciones concretas dependen del dispositivo y no forman parte de esta explicación.

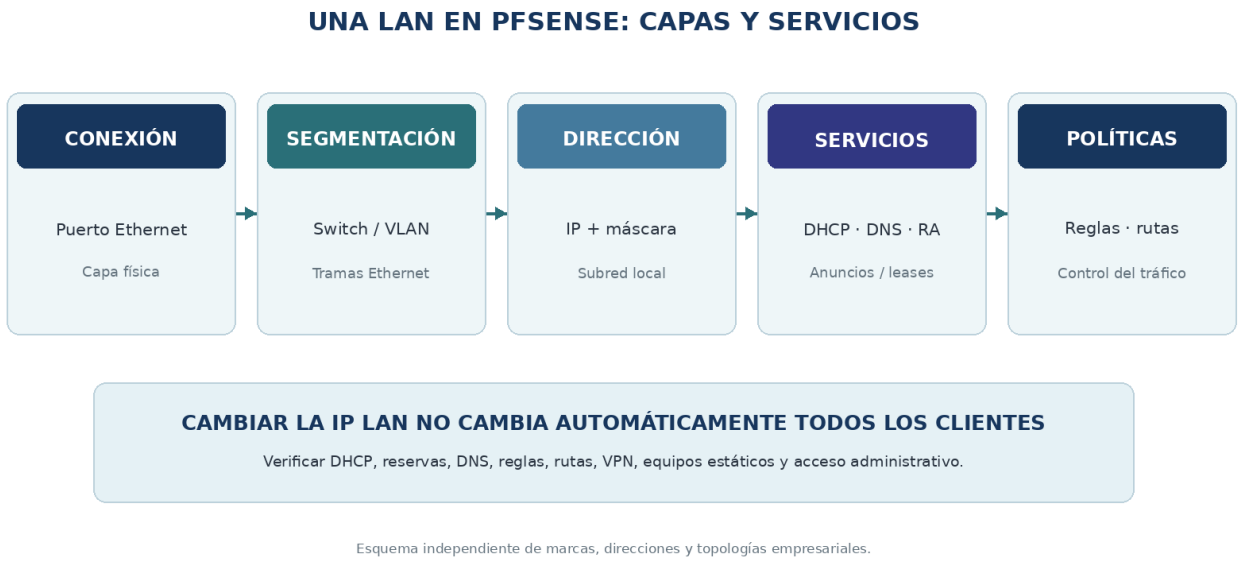


Figura 28.1. Relación entre conectividad, segmento lógico, direccionamiento y servicios de una LAN.

28.1. Propósito de la interfaz LAN y alcance del capítulo

Una interfaz LAN conecta pfSense Plus con una red interior y suele alojar la dirección utilizada por los equipos del segmento como siguiente salto, puerta de enlace y punto de acceso a determinados servicios locales. «LAN» es una denominación administrativa: el comportamiento efectivo depende del direccionamiento, de la existencia o no de un gateway ascendente y de las reglas que controlan los paquetes.

Este capítulo estudia el formulario de Interfaces → LAN: General Configuration, Static IPv4 Configuration, Track IPv6 Interface y Reserved Networks. También explica los servicios y controles dependientes necesarios para usar la LAN de forma segura; sus pantallas se administran en otros menús.

Disponibilidad de los campos. La visibilidad de las opciones de IPv4 e IPv6 depende del tipo de configuración seleccionado, de la edición y de la versión de pfSense Plus. Los formularios asociados deben comprobarse en el sistema administrado.

28.2. Localización y lectura de los cuatro bloques

Sección	Controles visibles	Responsabilidad
General Configuration	Enable, Description, IPv4/IPv6 Configuration Type, MAC Address, MTU, MSS, Promiscuous Mode, Switch port.	Identidad, direccionamiento seleccionado y comportamiento del enlace.
Static IPv4 Configuration	IPv4 Address / prefijo y IPv4 Upstream gateway.	Definir la red IPv4 local y evitar clasificación WAN accidental.
Track IPv6 Interface	IPv6 Interface e IPv6 Prefix ID.	Asignar automáticamente a LAN un /64 derivado de un prefijo externo.
Reserved Networks	Block private networks and loopback addresses; Block bogon networks.	Reglas automáticas de filtrado de orígenes entrantes.

Las secciones Static IPv4 Configuration y Track IPv6 Interface corresponden respectivamente a los modos elegidos en los selectores IPv4 e IPv6. Su visibilidad depende del modo seleccionado; no aparecen necesariamente para cualquier configuración.

28.3. Enable interface: activar, desactivar y consecuencias

Enable interface habilita administrativamente la interfaz. Si está marcada, pfSense puede aplicar su configuración IPv4/IPv6, utilizar sus direcciones, registrar tráfico y ejecutar los servicios asociados cuando esos servicios estén configurados. Si se desmarca, el segmento puede dejar de tener conectividad o punto de acceso al firewall; las reglas y los servicios vinculados no constituyen por sí solos una vía de recuperación.

La LAN suele ser la vía de administración de emergencia y el origen de DHCP, DNS y tráfico interno. Deshabilitarla durante una sesión remota puede impedir aplicar correcciones, afectar rutas hacia otros segmentos y desconectar a usuarios, switches gestionados o servidores.

RIESGO ALTO — pérdida de administración. No desactivar una LAN de producción ni cambiar su dirección o asociación de enlace sin una consola local, un canal de administración alternativo o un mecanismo de recuperación probado.

28.4. Description: nombre lógico y buenas prácticas

Description permite asignar un nombre reconocible a la interfaz. El texto se emplea en los listados, reglas y pantallas donde se seleccionan interfaces. Una descripción funcional como LAN, GESTIÓN o USUARIOS es más útil que términos temporales; debe documentarse cualquier cambio porque puede alterar la identificación de la interfaz en tareas de administración y automatizaciones.

No debe confundirse la descripción visible con el nombre del controlador, del puerto Ethernet o de la VLAN sobre la que se transporta el tráfico. Renombrar no mueve cables, no crea una subred y no establece reglas de firewall.

28.5. IPv4 Configuration Type: selector y efectos

Valor disponible	Uso / significado	Criterio para red interna
None	Sin configuración IPv4 en la interfaz.	Solo cuando LAN no necesita IPv4 o la dirección se gestiona de otro modo.
Static IPv4	Dirección y máscara definidas manualmente.	Opción habitual para una LAN que actúa como gateway de clientes.
DHCP	Obtiene dirección y otros parámetros por cliente DHCPv4.	Poco habitual para una LAN principal; evalúese el diseño.
PPP	Interfaz basada en protocolo PPP.	No es el modo ordinario de un segmento Ethernet local.
PPPoE	Sesión PPP sobre Ethernet, normalmente de acceso externo.	Raro en LAN; puede cambiar su función de encaminamiento.
PPTP / L2TP	Modos de conexión heredados dependientes de tecnología.	Evitar como elección por defecto; revisar soporte y seguridad.

El menú combina modalidades de configuración IPv4 para diferentes tipos de conexión. Elegir un valor no sustituye la necesidad de asignar correctamente el puerto en Interfaces → Assignments ni de mantener el switch y las VLAN coherentes. Los campos y procedimientos adicionales de los modos dinámicos o PPP dependen de la selección y se documentan en las secciones específicas de Netgate.

28.6. IPv6 Configuration Type: opciones y diferencias con IPv4

Selección	Comportamiento	Aplicación típica / precaución
None	Deshabilita configuración IPv6 para esta interfaz.	LAN solo IPv4; comprobar si se necesita dual stack.
Static IPv6	Dirección IPv6 y longitud de prefijo fijas.	Prefijo propio o rutas IPv6 estables; sin gateway ascendente en LAN.
DHCP6	Cliente DHCPv6 en la interfaz.	Más propio de uplink: no es servidor DHCPv6 de la LAN.
SLAAC	Autoconfiguración IPv6 a partir de Router Advertisements recibidos.	Principalmente como cliente de una red existente.

Selección	Comportamiento	Aplicación típica / precaución
6rd Tunnel / 6to4 Tunnel	Mecanismos de transición IPv6 sobre infraestructura IPv4.	No sustituyen un prefijo LAN delegado; dependientes del escenario.
Track Interface	Aprovecha prefijo delegado recibido por interfaz ascendente.	Opción común para redes internas con delegación dinámica del ISP.

La configuración de una dirección IPv6 en LAN no habilita automáticamente en todos los clientes un router por defecto ni asegura resolución DNS. La distribución a dispositivos suele requerir Router Advertisements (RA) y, cuando corresponda, DHCPv6 Server. En IPv6 el gateway de los clientes se anuncia mediante RA: DHCPv6 no transporta la opción equivalente de puerta de enlace.

28.7. MAC Address: comportamiento específico de una interfaz VLAN

La ayuda visible establece que la dirección MAC de una interfaz VLAN se modifica, cuando es necesario, en su interfaz padre. El campo no debe utilizarse para intentar cambiar la identidad Ethernet de una subinterfaz VLAN de forma aislada. La clonación de MAC se reserva para supuestos justificados; puede producir duplicados, conflictos de aprendizaje Ethernet o problemas en equipos vecinos.

En la LAN, antes de modificar la MAC debe verificarse si el problema procede realmente de un conflicto ARP, del switch o de una asignación incorrecta. Las direcciones IP y los identificadores de VLAN se configuran por vías diferentes.

28.8. MTU: tamaño máximo de paquete en el segmento local

MTU representa el tamaño máximo de paquete de la interfaz. En blanco, se conserva el valor predeterminado del adaptador, habitualmente 1500 bytes en Ethernet convencional. Las VLAN Ethernet 802.1Q agregan una etiqueta de capa 2 que el hardware debe soportar; esto no implica que el administrador deba reducir siempre a mano la MTU IP de la interfaz VLAN.

Situación	Resultado esperado	Recomendación
Campo vacío	El sistema adopta el valor por defecto adecuado.	Mantener salvo requerimiento medido.
Jumbo frames en el segmento	Posible mayor tamaño por paquete cuando todos los equipos lo soportan.	Alinear switches, NIC, hosts y rutas; comprobar fragmentación.
VPN o encapsulado	Cabeceras adicionales pueden reducir MTU efectiva de extremo a extremo.	Medir Path MTU antes de ajustar.
Valor muy bajo o muy alto	Más paquetes o pérdida de tramas/paquetes.	Cambiar una variable cada vez y registrar la prueba.

28.9. MSS: limitación del tamaño de segmentos TCP

MSS permite efectuar TCP MSS clamping. Según la ayuda de esta versión de pantalla, el valor introducido se interpreta como referencia de la que se restan 40 bytes para IPv4 o 60 bytes para IPv6 por cabeceras básicas. No debe confundirse el dato ingresado con el contenido útil resultante de TCP. La opción puede ayudar en rutas con túneles o fallos de descubrimiento de MTU, pero no corrige por sí sola errores de UDP o de conmutación.

En una LAN ordinaria, el MSS se deja en blanco salvo evidencia: por ejemplo, sesiones TCP establecidas que dejan de progresar con paquetes grandes y para las que ya se han descartado pérdidas físicas, rutas incorrectas, filtros ICMP y encapsulados. Comprobar el efecto sobre SYN TCP mediante Packet Capture.

28.10. Promiscuous Mode: observación de tramas y límites

Enable Promiscuous Mode mantiene el adaptador en modo promiscuo, de modo que puede aceptar tramas que no coincidan con su dirección MAC unicast, siempre que el dispositivo o la topología permitan que esas tramas le lleguen. No convierte automáticamente la LAN en un bridge, no modifica las reglas y no permite ver tráfico entre otros puertos conmutados si el switch no lo entrega.

De forma predeterminada permanece desactivado. Solo habilitarlo para casos particulares de captura, puente o mecanismos documentados, con una finalidad comprobable y sin aumentar innecesariamente la carga de procesamiento.

28.11. Switch port: seguimiento de la portadora física

En determinadas plataformas con switch interno, «Select the Switch port to monitor for media state changes» ofrece una lista de puertos para asociar el estado de enlace de la interfaz lógica LAN a un conector físico. El número mostrado no indica por sí solo la VLAN, el PVID, el dispositivo WAN ni la velocidad del puerto.

Si se asocia el estado de la LAN a un puerto que pierde portadora, servicios que dependen de la interfaz podrían quedar sin disponibilidad incluso si hay otros conectores que siguen transportando la misma VLAN. La documentación oficial de Netgate indica expresamente que, al usar varios puertos como miembros de una única LAN conmutada, puede ser conveniente dejar sin seleccionar un puerto de monitorización para no convertir la conexión de un solo cable en dependencia de toda la LAN.

Distinción clave. Interfaces → Switch → Ports administra características del conmutador. Interfaces → LAN → Switch port solo supervisa eventos de portadora de un puerto seleccionado en los modelos que exponen ese control; no sustituye una configuración de VLAN o de asignación.

28.12. Static IPv4 Configuration: papel de la dirección del firewall

Con Static IPv4, IPv4 Address define la dirección que tendrá pfSense en la red LAN y la lista de prefijos define el tamaño de su subred. Por ejemplo, un /24 corresponde a 255.255.255.0, 256 direcciones en total y, en una red IPv4 ordinaria, 254 direcciones de host utilizables. La longitud de prefijo no mide los equipos conectados; delimita las direcciones que se consideran locales para ese segmento.

A efectos puramente didácticos, la red ficticia 10.77.50.0/24 y la dirección del firewall 10.77.50.1/24 ilustran un segmento privado. No proceden de ninguna instalación y no son una configuración que deba copiarse sin estudio de redes, VPN, DHCP y solapamientos.

Concepto de ejemplo	Valor ilustrativo	Consecuencia
Dirección de interfaz	10.77.50.1/24	pfSense tiene una dirección en el segmento 10.77.50.0/24.
Máscara equivalente	255.255.255.0	Determina qué destinos pertenecen a la red conectada.
Red / difusión	10.77.50.0 / 10.77.50.255	No deben usarse como direcciones de host ordinarias.
Hosts de ejemplo	10.77.50.2 a 10.77.50.254	Antes de asignar hay que excluir equipos fijos, VIP y reservas.
Gateway de los clientes	10.77.50.1	Los clientes usan la IP LAN del firewall como siguiente salto, si es su router.

Prohibición operativa. No elegir nunca la misma subred para LAN y WAN u otra interfaz activa, ni una dirección ya ocupada. Una LAN que se solapa con una VPN o red remota puede romper rutas y acceso aun cuando los cables estén correctos.

28.13. IPv4 Address: campo y máscara, controles visibles

El cuadro IPv4 Address exige una dirección IPv4 adecuada a la red interior. A su derecha, la longitud de prefijo CIDR permite elegir valores entre /1 y /32 según los controles del equipo. No todos los prefijos son apropiados para una LAN de usuarios: la selección debe responder a la capacidad del segmento, a las rutas y al plan de direccionamiento.

La red local que el firewall considera directamente conectada cambia al modificar dirección o máscara, con efectos inmediatos sobre ARP, rutas conectadas, servidores locales y clientes. Una dirección de firewall en otra red obliga a los administradores a cambiar su propia conectividad para volver a abrir la GUI.

28.14. IPv4 Upstream gateway: dejar None en una LAN normal

El control muestra normalmente None y, opcionalmente, gateways existentes o un botón para crear otro. La propia ayuda de pfSense advierte de que el gateway ascendente se configura cuando la interfaz actúa como enlace hacia una red externa; en interfaces locales debe mantenerse None. Seleccionar un gateway hace que pfSense trate esa interfaz como tipo WAN, con implicaciones en NAT y otros comportamientos vinculados a la clasificación de interfaces.

No confundir «IPv4 Upstream gateway» con «gateway que reciben los clientes». En el primer caso se define hacia dónde sale el propio firewall por esa interfaz; en el segundo los clientes reciben la dirección LAN del firewall o de otro router por DHCP o configuración manual. Son sentidos y roles de encaminamiento diferentes.

Elemento	En LAN habitual	Si se configura incorrectamente
IPv4 Upstream gateway (pfSense)	None.	La interfaz puede ser clasificada como WAN; cambia la lógica de NAT y otras funciones.
Gateway del PC cliente	IP LAN de pfSense cuando es su router.	El cliente no alcanzará otras redes o tomará un salto inadecuado.
Ruta estática hacia un router interior	Crear gateway/ruta en System → Routing cuando corresponda, sin escogerlo como upstream LAN.	Riesgo de rutas erróneas o de política NAT indeseada.

28.15. Track IPv6 Interface: finalidad y requisito de delegación

Track Interface permite asignar a una LAN una subred IPv6 procedente de un prefijo delegado dinámicamente a una interfaz ascendente. El modelo común es: la WAN recibe del operador un bloque mediante DHCPv6 Prefix Delegation, mientras que una o varias LAN utilizan subredes de ese bloque sin que el administrador tenga que escribir direcciones globales rígidas.

Track IPv6 Interface requiere que la interfaz elegida como origen tenga una delegación adecuada. No crea por sí misma una delegación, no garantiza IPv6 público operativo ni anuncia automáticamente a los clientes todos los parámetros necesarios. Hay que contrastar Status → Interfaces, delegaciones obtenidas y los Router Advertisements pertinentes.

28.16. IPv6 Interface: seleccionar la interfaz ascendente correcta

IPv6 Interface enumera interfaces que disponen de un modo IPv6 dinámico adecuado para aportar la delegación. Hay que elegir el enlace ascendente que realmente recibe el prefijo destinado a las LAN. Si se escoge otra conexión, se pierde la delegación o el operador renumera el bloque, las direcciones de LAN pueden cambiar o dejar de estar disponibles.

En entornos con múltiples WAN se debe prever cómo actúan los cambios de prefijo ante la conmutación de proveedor: direcciones de clientes, reglas IPv6, DNS, publicación de servicios y rutas pueden necesitar una política más amplia que un simple cambio de selector.

28.17. IPv6 Prefix ID: formato hexadecimal y cálculo

IPv6 Prefix ID selecciona qué subred /64 dentro del prefijo delegado se utilizará en esta LAN. El valor se expresa en hexadecimal y su rango depende del tamaño del bloque recibido. La ayuda indica un valor predeterminado 0; el máximo debe comprobarse en el formulario, que lo calcula según la delegación.



Figura 28.2. Ejemplo documental de un bloque /60 dividido en 16 subredes /64 con IDs 0–f.

Un prefijo delegado /60 contiene 16 subredes /64 y admite IDs 0…f. Un /56 contiene 256 /64 (0…ff). Una delegación /64 ofrece una única subred /64: no admite repartir múltiples LAN independientes con distintos /64 dentro de ese mismo bloque. Cada red interna que utilice la delegación debe tener un Prefix ID exclusivo para evitar solapamientos.

Bloque delegado	/64 disponibles	Prefix ID posibles
/64	1	0
/60	16	0 a f
/56	256	0 a ff
/48	65.536	0 a ffff

28.18. Qué sucede si cambia el prefijo IPv6 delegado

Cuando el proveedor renumera la delegación, una LAN con Track Interface puede recibir un nuevo prefijo. Los clientes pueden conservar temporalmente direcciones anteriores según sus temporizadores de validez y preferencia; por ello conviene comprobar las reglas y los anuncios RA y la resolución DNS externa e interna. Este comportamiento no equivale necesariamente a un fallo de configuración.

En redes con aplicaciones que exigen direccionamiento estable, estudiar las opciones de prefijo propio, ULA, direccionamiento IPv6 fijo ofrecido por operador y mecanismos de alta disponibilidad. No asumir que un prefijo obtenido dinámicamente es inmutable.

28.19. Relación con DHCPv4 Server, DHCPv6 Server y RA

La dirección IPv4 estática de LAN hace posible que pfSense aloje un servidor DHCPv4 para esa subred, pero el servidor se configura por separado en Services → DHCP Server. Un cambio de IPv4 LAN puede exigir modificar rango DHCP, reservas, DNS entregados y gateway anunciado. El motor DHCP configurado y el formato de la pantalla pueden variar según la edición y la versión.

Para IPv6, el reparto de direcciones y la elección del router requieren analizar Services → DHCPv6 Server y Services → Router Advertisement. La definición de Track Interface no sustituye la política de RA. Por ejemplo, determinados equipos solo utilizan SLAAC para obtener dirección, aunque otros acepten DHCPv6; elegir Managed sin estudiar clientes puede dejar dispositivos sin dirección IPv6 global.

Necesidad en clientes	Menú responsable	Punto esencial
Dirección IPv4 automática	Services → DHCP Server	El rango debe pertenecer a la LAN estática, con reservas y exclusiones coherentes.
Gateway IPv4 de clientes	DHCPv4 o configuración manual	Normalmente IP LAN del firewall, no IPv4 Upstream gateway de la página LAN.

Necesidad en clientes	Menú responsable	Punto esencial
Router IPv6 predeterminado	Services → Router Advertisement	RA anuncia la presencia del router; DHCPv6 no lo sustituye.
Dirección IPv6 / parámetros	RA (SLAAC) y/o DHCPv6 Server	Escoger modo considerando sistemas operativos y requisitos.
DNS local	DNS Resolver/Forwarder y DHCP/RA	Verificar escucha, accesos y direcciones ofrecidas.

28.20. Reserved Networks: interpretación en una LAN

Esta sección ofrece las mismas opciones que otras interfaces, pero su conveniencia cambia radicalmente por tratarse de una red interna. Las reglas automáticas se refieren al origen del tráfico que entra por la interfaz. Bloquear fuentes que legítimamente pertenecen a la LAN puede equivaler a bloquear los propios clientes.

28.21. Block private networks and loopback addresses

Al activar esta opción, pfSense crea restricciones automáticas para orígenes RFC1918 (10/8, 172.16/12 y 192.168/16), loopback IPv4 y los rangos IPv6 únicos locales relevantes según lo indicado por la ayuda. En una LAN basada en direccionamiento privado, esos orígenes son precisamente los normales. Por ello, normalmente debe permanecer DESACTIVADA en LAN; activarla puede cortar la navegación, el acceso a GUI o servicios internos dependiendo de reglas y rutas.

Desactivarla no significa permitir libremente todo el tráfico: las reglas de Firewall → Rules → LAN y otras políticas continúan siendo responsables de autorizar o denegar comunicaciones. Para limitar segmentos internos se prefieren reglas explícitas y documentadas por origen/destino, no el filtrado masivo pensado para WAN.

28.22. Block bogon networks

Block bogon networks bloquea tráfico con direcciones de origen incluidas en tablas de prefijos no asignados, reservados o impropios de la red pública. Netgate advierte expresamente de que ese filtrado no es apropiado para redes locales y puede impedir tráfico imprescindible, especialmente IPv6. En LAN ordinaria debe permanecer DESACTIVADO salvo un diseño excepcional fundamentado y validado.

Las listas bogon se actualizan por la plataforma; su frecuencia se administra en System → Advanced → Firewall & NAT. La actualización de una tabla no reemplaza la revisión de reglas, la prevención de suplantación de IP en redes internas ni un diseño de segmentación.

Control en LAN	Normalmente	Motivo
Block private networks and loopback addresses	Desactivado	Los clientes usan legítimamente direcciones privadas o ULA.
Block bogon networks	Desactivado	Puede descartar tráfico local, incluidos protocolos IPv6 necesarios.
Firewall → Rules → LAN	Reglas explícitas, mínimo privilegio	Separa el acceso por redes, protocolos y destinos.
Anti-lockout / gestión	Evaluación específica del acceso de administración	Cambiar reglas sin acceso alternativo puede provocar bloqueo.

28.23. Save, Apply Changes y validación de la operación

Save guarda la configuración que se ha editado; cuando la interfaz web informa de cambios pendientes, Apply Changes los hace efectivos. Las operaciones que cambian LAN pueden alterar la dirección de la propia GUI, renovar servicios o provocar cortes instantáneos de tráfico. No asumir que una sesión web que deja de cargar revela una avería: puede seguir disponible en la nueva red.

01. Registrar valores anteriores, motivo del cambio, dependencias y criterio de aceptación.
02. Hacer copia segura de la configuración y disponer de acceso físico/serie o de una vía alternativa probada.
03. Comprobar que el cliente de administración podrá usar la nueva subred y alcanzar la nueva dirección.
04. Revisar IPv4 Upstream gateway = None y las opciones de bloqueo privado/bogon.

05. Pulsar Save y luego Apply Changes cuando se solicite.
06. Renovar dirección del cliente o adaptar temporalmente su IP, máscara y gateway según el nuevo escenario.
07. Comprobar GUI, DHCPv4, DNS, IPv6/RA, rutas, reglas y conectividad a redes remotas.
08. Documentar el resultado; si falla, revertir desde la consola o mediante copia verificada.

28.24. Procedimiento A: configurar una LAN con IPv4 fija

01. Identificar el puerto o VLAN lógico asignado a LAN y comprobar que existe un segmento Ethernet aislado según el diseño.
02. Establecer Enable interface y una descripción funcional.
03. Elegir IPv4 Configuration Type = Static IPv4.
04. Asignar IPv4 Address y longitud de prefijo que no coincidan ni se solapen con otras redes conectadas o remotas.
05. Mantener IPv4 Upstream gateway en None.
06. Elegir el modo IPv6 que proceda; no activar automáticamente servicios de cliente IPv6 si no existe una justificación.
07. Mantener MAC, MTU, MSS y Promiscuous Mode sin forzar cuando no sea necesario.
08. Revisar Switch port si el modelo lo ofrece; evitar depender de un único puerto si LAN tiene varios conectores.
09. No habilitar Block private networks ni Block bogon networks en una LAN privada ordinaria.
10. Guardar/aplicar, adaptar DHCPv4 si existe y verificar conectividad desde clientes y firewall.

28.25. Procedimiento B: activar IPv6 mediante Track Interface

01. Comprobar que un enlace ascendente recibe un prefijo IPv6 delegado utilizable y conocer su longitud.
02. Elegir LAN → IPv6 Configuration Type = Track Interface.
03. En IPv6 Interface seleccionar la interfaz ascendente que recibe el prefijo.
04. Asignar un IPv6 Prefix ID hexadecimal permitido y no usado por otra red interna.
05. Guardar/aplicar y verificar que LAN obtiene una subred /64 válida en Status → Interfaces.
06. Configurar Router Advertisements en Services → Router Advertisement según los clientes previstos.
07. Configurar DHCPv6 Server si se requiere y el modo RA lo admite; recordar que DHCPv6 no proporciona gateway.
08. Probar autoconfiguración de clientes, rutas IPv6, DNS, ICMPv6 necesario y políticas de firewall.
09. Validar comportamiento al renovar el prefijo, documentando servicios que requieren direcciones estables.

28.26. Procedimiento C: cambiar la IP LAN sin perder la administración



Figura 28.3. Flujo de cambio controlado: preparación, aplicación, comprobación y recuperación.

01. Preparar backup XML protegido, consola y plan de rollback.
02. Inventariar dependencias: DHCP, DNS, servidores estáticos, NAT, reglas, VPN, monitorización y gestión de switches.
03. Verificar que la nueva red no se solapa con WAN, otras LAN, VPN, VTI, redes de terceros o rutas existentes.
04. Planear la adaptación de los clientes: reservas, leases y direccionamiento manual.
05. Editar IPv4 Address y máscara en Interfaces → LAN, manteniendo gateway upstream = None.
06. Aplicar cambio desde mantenimiento; reconfigurar el equipo administrador para acceder a la nueva IP LAN.
07. Corregir rango DHCP, reservas, DNS y accesos administrativos según proceda.
08. Verificar conectividad y servicios; revertir por consola si falla antes de que expire la ventana de mantenimiento.

Consola de recuperación. Netgate documenta la opción 2 del menú de consola («Set interface(s) IP address») para cambiar la dirección LAN y, cuando corresponde, recuperar conectividad administrativa. El procedimiento exacto depende del equipo y no reemplaza una copia de seguridad.

28.27. Escenarios empresariales de referencia

Escenario genérico	Configuración orientativa	Validación prioritaria
Red local de puestos	IPv4 estática en LAN, gateway ascendente None; DHCPv4 separado si procede.	Clientes reciben IP y usan firewall como router.
LAN de gestión restringida	Interfaz dedicada o VLAN lógica y reglas de origen/destino estrictas.	Solo gestores autorizados alcanzan GUI/SSH.
Varias redes locales	Una interfaz/VLAN por red, sin redes superpuestas; reglas entre segmentos.	Rutas, DNS, DHCP y políticas entre VLANs.
IPv6 con ISP dinámico	LAN Track Interface, Prefix ID exclusivo, RA y DHCPv6 cuando corresponda.	Prefijo /64 y conectividad IPv6 extremo a extremo.
LAN con dos conectores conmutados	VLAN compartida y seguimiento Switch port valorado cuidadosamente.	Desenchufar un puerto no tumba servicios al otro.
Rutas hacia redes tras router interior	Gateway/ruta estática en System → Routing, sin cambiar el upstream gateway LAN.	Rutas de ida/vuelta y firewall sin NAT no deseado.

28.28. Comprobación funcional y herramientas de diagnóstico

Prueba	Herramienta / ruta	Qué determina
Dirección y estado	Status → Interfaces	Dirección LAN, enlace, IPv6 delegado y presencia operativa.
Prueba local desde cliente	Ping/ARP/NDP en puesto o Diagnósticos	Conectividad del host con su puerta de enlace.
Configuración de clientes	ipconfig/ifconfig/ip; DHCP leases	Dirección/máscara, router y DNS correctos.
Rutas del firewall	Diagnostics → Routes / System → Routing	Red LAN conectada y rutas internas y externas.
Reglas y bloqueos	Firewall → Rules, Status → System Logs	Política efectiva, descartes y causas de bloqueo.
Captura real	Diagnostics → Packet Capture	DHCP, ARP, ND, RA, ICMP y datos TCP de prueba.
DNS	Diagnostics → DNS Lookup; Services → DNS Resolver	Separación entre fallo DNS y fallo de encaminamiento.
Delegación IPv6	Status → Interfaces y servicios IPv6	Prefijo delegado, ID elegido, RA y respuesta de clientes.

Orden práctico: comprobar link físico, membership VLAN, IPv4/v6 del firewall, configuración del cliente, ruta hasta LAN, DNS, reglas y rutas hacia fuera. Si IPv4 funciona e IPv6 no, estudiar RA/PD, Neighbor Discovery e ICMPv6 sin atribuir automáticamente la incidencia al DHCPv4.

28.29. Errores frecuentes, síntomas y correcciones

Síntoma	Causas plausibles	Resolución ordenada
GUI inaccesible tras cambiar LAN	PC conserva IP anterior, subnet nueva o puerto/VLAN modificados.	Ajustar cliente, verificar nuevo URL y conectar por consola si es preciso.
Clientes sin dirección DHCP	Servidor sin rango válido, servicio deshabilitado, VLAN o puerto incorrectos.	Revisar Services → DHCP Server y captura DORA.
Acceso local sí, salida no	Gateway de cliente/DNS/rutas o reglas incorrectas.	Separar LAN–firewall, firewall–WAN y DNS.
LAN se trata como WAN	IPv4 Upstream gateway configurado.	Volver a None; revisar NAT y rutas impactadas.
No llegan paquetes a la LAN	PVID, miembros VLAN o enlace físico incorrecto.	Revisar Interfaces → Switch y Assignments.
LAN desaparece al desconectar un puerto	Switch port monitoriza un conector de un grupo compartido.	Revisar seguimiento de portadora según diseño.
IPv6 sin dirección global	No hay delegación, upstream incorrecto o Prefix ID fuera de rango.	Comprobar WAN PD y Track Interface.
IPv6 tiene dirección pero no salida	RA, reglas ICMPv6 o rutas IPv6 incorrectas.	Validar gateway mediante RA y firewall IPv6.
Tráfico de clientes privados bloqueado	Block private networks activo en LAN.	Deshabilitar ese filtro y usar reglas explícitas.
Inestabilidad IPv6 local	Block bogon networks o RA mal configurados.	Deshabilitar bogon en LAN y estudiar capturas IPv6.

28.30. Seguridad, continuidad y buenas prácticas

01. Mantener la LAN de administración protegida por reglas explícitas y acceso restringido a la GUI, preferentemente en red de gestión dedicada.
02. No suponer que un nombre «LAN» permite automáticamente tráfico: examinar políticas efectivas y reglas anti-lockout.
03. No elegir un IPv4 Upstream gateway en LAN para forzar una salida por router interior; administrar rutas estáticas correctamente.

04. Evitar superposición de redes internas, VPN y WAN, especialmente en migraciones de direccionamiento.
05. Mantener DHCP/RA separados de la edición de IP LAN, verificando coherencia del servicio tras cada cambio.
06. Reservar MTU/MSS/MAC/modo promiscuo para requisitos contrastados y medibles.
07. No activar filtrados RFC1918 ni bogon en LAN ordinaria.
08. Garantizar consola, copia XML cifrada y ventana de mantenimiento para cambios de interfaz de gestión.
09. Comprobar IPv4 e IPv6 por separado; no bloquear ND/RA/ICMPv6 necesarios por políticas demasiado amplias.
10. Anotar cada cambio y sus pruebas de aceptación para facilitar mantenimiento y auditoría.

28.31. Lista de comprobación de una LAN bien configurada

Control	Condición de aceptación
Enable / Description	Interfaz activa y nombre funcional inequívoco.
IPv4 + máscara	IP LAN única, prefijo correcto, sin solapamientos.
IPv4 Upstream gateway	None en una LAN interna que no sea un uplink.
IPv6	None, Static IPv6 o Track Interface conforme al diseño.
Track IPv6	Interfaz fuente con PD válida y Prefix ID no duplicado.
Capa 2 / switch	VLAN/PVID, portadora y seguimiento físico coherentes.
DHCP / RA / DNS	Servicios separados configurados, probados y coherentes con la subred.
Reserved Networks	Filtros RFC1918 y bogon desactivados para LAN privada ordinaria.
Seguridad	Reglas explícitas y acceso a la administración controlado.
Recuperación	Backup, consola y prueba de clientes tras los cambios.

28.32. Glosario de términos usados

Concepto	Definición
LAN	Segmento local conectado a una interfaz lógica del firewall.
CIDR	Notación /n que determina longitud del prefijo IP.
Upstream gateway	Pasarela ascendente para el propio firewall en esa interfaz; distinta de la IP LAN que reciben clientes.
Track Interface	Modo que deriva un prefijo IPv6 de una delegación recibida por otra interfaz.
Prefix ID	Selector hexadecimal del /64 dentro del prefijo delegado.
DHCPv4 / DHCPv6	Protocolos de configuración automática; DHCPv6 no anuncia el router por defecto.
RA / SLAAC	Anuncios de router y autoconfiguración IPv6 de hosts.
MTU / MSS	Tamaño máximo de paquete y tamaño máximo de carga TCP anunciado.
Bogon	Prefijo reservado/no asignado, filtrado habitualmente en WAN pública.
PVID / VLAN	Identificador VLAN asignado a tramas sin etiqueta / segmentación 802.1Q.
Anti-lockout	Regla/protección administrativa que puede afectar al acceso a GUI desde LAN.

28.33. Referencias oficiales de Netgate

Documentación de Netgate para pfSense Plus y pfSense Software. La disponibilidad exacta de los controles depende del equipo y de la versión. Los detalles de otras pantallas aportan contexto técnico y no son campos del formulario LAN.

Interface Configuration — https://docs.netgate.com/pfsense/en/latest/interfaces/configure.html

IPv4 Configuration Types — https://docs.netgate.com/pfsense/en/latest/interfaces/configure-ipv4.html

IPv6 Configuration Types y Track Interface — https://docs.netgate.com/pfsense/en/latest/interfaces/configure-ipv6.html

WAN vs LAN Interfaces — https://docs.netgate.com/pfsense/en/latest/interfaces/wanvslan.html

pfSense Configuration y cambio de IP LAN desde consola — https://docs.netgate.com/pfsense/en/latest/config/index.html

DHCPv4 Server — https://docs.netgate.com/pfsense/en/latest/services/dhcp/ipv4.html

DHCPv6 Server — https://docs.netgate.com/pfsense/en/latest/services/dhcp/ipv6.html

IPv6 Router Advertisements — https://docs.netgate.com/pfsense/en/latest/services/dhcp/ipv6-ra.html

Switch Ports - equipos con switch integrado — https://docs.netgate.com/pfsense/en/latest/solutions/sg-1100/configuring-the-switch-ports.html

Rule Methodology y Block Bogon Networks — https://docs.netgate.com/pfsense/en/latest/firewall/rule-methodology.html

Configuration Backup — https://docs.netgate.com/pfsense/en/latest/backup/configuration.html

29 Interfaces → WAN secundaria

Conectividad 4G/LTE, cliente DHCP, filtrado y conmutación de respaldo

Ruta de acceso: Interfaces → interfaz opcional asignada como salida secundaria. La denominación exacta del menú y el adaptador físico dependen del sistema. Este capítulo explica los controles de la página y sus consecuencias de operación; no describe ningún equipo o conexión particular.



Figura 29.1. Cadena de dependencias desde el acceso móvil hasta el enrutamiento efectivo de usuarios.

29.1. Función, alcance y relación con otras interfaces

pfSense Plus permite utilizar interfaces opcionales como conexiones de acceso exterior. En un diseño con una conexión fija principal y una línea móvil de respaldo, la interfaz secundaria puede obtener su IPv4 por DHCP desde un router 4G/LTE o 5G conectado por Ethernet. Que el nombre de la interfaz sugiera 4G no determina por sí mismo la tecnología ni convierte el firewall en un módem celular: el radioenlace, la SIM, el APN y la calidad de señal se administran generalmente en el equipo de acceso, salvo soluciones con módem compatible integrado.

El formulario examinado comprende General Configuration, DHCP Client Configuration y Reserved Networks. La configuración presentada expone un cliente DHCPv4 y controles generales que también existen en otras interfaces; su misión operativa, sin embargo, difiere: mantener una vía exterior preparada, monitorizarla y utilizarla cuando la política lo permita. El vínculo entre esta página y System → Routing / Firewall → Rules / Firewall → NAT es fundamental.

Las opciones de IPv4 e IPv6 condicionan los campos que presenta la interfaz. Las funciones Multi-WAN, los gateways y la monitorización se explican en sus apartados correspondientes. El orden y la presentación pueden variar con la versión de pfSense Plus y el hardware.

29.2. ¿Cuándo conviene habilitar una WAN de respaldo móvil?

Aplicación práctica	Ventaja	Precaución
Oficinas con acceso de fibra único	Continuidad para aplicaciones críticas.	Cobertura, energía y consumo de datos.
Instalación temporal / puesta en marcha	Conectividad rápida sin obra civil.	Latencia y velocidad variables.
Comercio con servicios de pago remotos	Mantener transacciones básicas si falla la principal.	Validar terminales y DNS tras el cambio de IP.
Telemetría y soporte remoto	Ruta alternativa para supervisión.	CGNAT y túneles pueden limitar el acceso entrante.
Plan de contingencia empresarial	Reducción del punto único de fallo.	Un router móvil comparte energía o switch si no se diseña redundancia física.

Una WAN secundaria no elimina la necesidad de redundancia eléctrica, cobertura suficiente ni configuración correcta de DNS, NAT, VPN y firewall. Debe existir un umbral de servicio aceptable y un ensayo de conmutación previo a considerarla disponible para producción.

29.3. Arquitectura funcional: interfaz, gateway y tráfico

Conviene separar cuatro conceptos: (1) portadora Ethernet del puerto/switch; (2) concesión IPv4 y parámetros recibidos por DHCP; (3) disponibilidad del gateway evaluada por el monitor; (4) decisión de salida por las reglas o por la ruta predeterminada. Cada etapa puede funcionar mientras otra falla. Por ejemplo, un router móvil puede responder al enlace y entregar DHCP aunque el operador haya perdido acceso a Internet.

Diferencia crítica. Habilitar una interfaz OPT y obtener una concesión DHCP NO activa automáticamente el failover de todo el tráfico. Es necesario integrar los gateways en un grupo apropiado, configurar la ruta predeterminada y/o las reglas de policy routing, y verificar NAT y DNS.

29.4. Ruta exacta y organización del formulario

Abrir Interfaces → [nombre administrativo de la interfaz secundaria]. Los nombres WAN, LAN y OPTn son asignaciones lógicas: pueden renombrarse y su papel efectivo depende del tipo de configuración, enrutamiento y reglas. El uso de DHCP clasifica dinámicamente la interfaz como tipo WAN para funciones como NAT. No se necesita mostrar el nombre interno del adaptador ni la URL de administración para explicar ninguna opción.

Sección visible	Contenido	Finalidad
General Configuration	Enable, Description, IPv4/IPv6 Configuration Type, MAC Address, MTU, MSS, Promiscuous Mode y Switch port.	Definir estado y comportamiento del interfaz.
DHCP Client Configuration	Advanced Configuration, Configuration Override, Hostname, Alias IPv4 address, Reject leases from y DHCP VLAN Priority.	Gestionar la concesión y particularidades del proveedor.
Reserved Networks	Block private networks and loopback addresses; Block bogon networks.	Bloquear orígenes no esperados según el tipo de enlace.

29.5. Enable: habilitación y retirada de servicio

Enable interface determina si pfSense mantiene operativa la asignación. Activarla permite que se procese la configuración IP y que puedan crearse/monitorizarse servicios asociados. Desactivarla retira esa interfaz de las operaciones previstas, interrumpe concesiones y puede dejar sin ruta a conexiones que la utilizaban; el efecto exacto depende de la configuración del firewall y de los gateways.

En una WAN de reserva suele permanecer habilitada aun cuando no deba transportar tráfico ordinario: así puede mantenerse la concesión DHCP y medirse su disponibilidad antes de un fallo. Deshabilitarla como mecanismo de ahorro de datos impide comprobarla y puede retrasar la conmutación. Es preferible controlar la elección de camino con grupos de gateways y reglas, valorando los costes de las sondas y del equipo de acceso.

Riesgo de desconexión. No deshabilitar la única salida disponible ni modificar interfaces desde una sesión remota sin consola o acceso alternativo. Preparar copia de la configuración y ventana de mantenimiento si la conexión soporta VPN, telefonía u otros servicios críticos.

29.6. Description: nomenclatura sin exponer la infraestructura

Description es el nombre que aparece en menús y pestañas de reglas, servicios y monitorización. Según Netgate admite letras, números y el carácter de subrayado. Conviene indicar la función, no el proveedor, la ubicación, el número de SIM ni detalles contractuales. Un nombre genérico como ENLACE_RESPALDO es suficiente para un ejemplo didáctico.

Renombrar no convierte una interfaz LAN en WAN ni cambia físicamente puertos o VLAN. Después de renombrar, verificar que administradores y procedimientos identifiquen la interfaz correcta antes de aplicar acciones de riesgo.

29.7. IPv4 Configuration Type: siete modalidades disponibles

Opción exacta	Comportamiento	Uso en una línea móvil / advertencia
None	No se configura IPv4 en la interfaz.	Solo si no se utiliza IPv4 o se gestiona mediante otra técnica.
Static IPv4	Dirección y prefijo definidos manualmente; requiere gateway apropiado para salida.	Posible con router/operador que proporcionen parámetros fijos.
DHCP	Solicita dirección, prefijo y opciones al servidor de aguas arriba.	Típico cuando el router celular presenta Ethernet con DHCP.
PPP	Acceso a través de interfaz de protocolo punto a punto.	Solo cuando el acceso y hardware requieren este modo.
PPPoE	Sesión PPP encapsulada sobre Ethernet.	No asumirlo por el hecho de ser 4G.
PPTP	Modo histórico de conexión; se configura según parámetros externos.	No recomendable como solución nueva de acceso sin justificación.
L2TP	Conexión mediante protocolo de túnel de capa 2.	Depende del servicio y del extremo proveedor.

Al seleccionar DHCP se muestra la sección DHCP Client Configuration recogida en el material de origen. Otras elecciones revelan controles específicos que no forman parte del formulario visible y que se describen en la documentación Netgate de IPv4 y PPP. Cambiar el tipo de configuración puede eliminar la dirección y la pasarela actuales; no debe realizarse sin verificar cómo se entregan las direcciones en el acceso real.

29.8. IPv6 Configuration Type: siete alternativas

Opción exacta	Significado	Criterio práctico
None	Sin configuración IPv6 para esa interfaz.	Válido si el proveedor no ofrece IPv6 y no se requiere.
Static IPv6	IPv6/prefijo definidos manualmente.	Solo con parámetros de acceso acordados.
DHCP6	Cliente DHCPv6 con opciones de dirección y/o delegación.	Comprobar si el operador realmente ofrece DHCPv6 y PD.
SLAAC	Autoconfiguración con anuncios de router IPv6.	Depende de RA válidos en ese enlace.
6rd Tunnel	Transición IPv6 sobre red de acceso IPv4.	Uso específico bajo parámetros de proveedor.
6to4 Tunnel	Mecanismo de transición legado.	No recomendación genérica para una red nueva.
Track Interface	Seguimiento de un prefijo delegado por otra interfaz.	Suele corresponder a redes internas, no a una WAN celular nueva.

La lista visible en la interfaz incluye siete opciones: None, Static IPv6, DHCP6, SLAAC, 6rd Tunnel, 6to4 Tunnel y Track Interface. Los mecanismos de transición y seguimiento requieren parámetros distintos. IPv4 e IPv6 se administran por separado: una conexión IPv4 funcional no acredita automáticamente salida IPv6 ni delegación de prefijos.

29.9. MAC Address: identificación en la capa Ethernet

El campo MAC Address permite cambiar la dirección de enlace en adaptadores que lo admiten, por ejemplo para mantener un identificador conocido por un equipo aguas arriba. La ayuda del formulario aclara que la MAC de una interfaz VLAN debe configurarse en su interfaz padre. No es una opción de identificación de la SIM ni sustituye APN, IMEI u otros parámetros del router celular.

La práctica recomendada es dejarla sin forzar. Cuando existen bloqueos por MAC, revisar primero el registro del operador, reiniciar el equipo de acceso o esperar a la actualización de ARP. Clonar MAC sin retirar el equipo anterior puede originar duplicados y pérdida intermitente de conectividad.

29.10. MTU: paquete máximo en Ethernet y accesos encapsulados

MTU (Maximum Transmission Unit) determina el tamaño máximo de paquete IP que puede circular por la interfaz sin exceder su capacidad de transporte. La ayuda indica que, cuando se deja vacío, se utiliza el valor predeterminado del adaptador, normalmente 1500 bytes en Ethernet clásico, aunque el acceso real puede imponer otro valor por encapsulado o tecnología intermedia.

Una conexión celular puede presentar MTU efectiva inferior a la de Ethernet por políticas de proveedor, túneles o adaptadores virtuales. Sin embargo, no procede establecer un valor universal de 4G o reducirlo por intuición. Primero verificar fallo concreto, negociación física, Path MTU Discovery y comportamiento de las aplicaciones. Un MTU demasiado alto puede producir pérdida de paquetes grandes; uno innecesariamente bajo añade sobrecarga.

29.11. MSS: limitación de segmentos TCP

MSS (Maximum Segment Size) describe la carga de datos TCP anunciada en el establecimiento de la conexión. La ayuda visible indica que pfSense calcula clamping restando 40 bytes para IPv4 o 60 bytes para IPv6 al valor introducido en este campo. Esta distinción entre el valor del campo y la carga TCP efectiva evita un ajuste accidental excesivo.

Situación	Recomendación
MTU y MSS vacíos; servicios correctos	Mantener la negociación automática.
Sesiones TCP conectan pero se bloquean en transferencias	Investigar PMTUD, ICMP, encapsulado y TCP SYN antes de ajustar.
VPN sobre la WAN celular	Comprobar overhead real de túnel, extremo remoto y aplicación.
Fallo de UDP o ICMP	MSS TCP por sí solo no resuelve el problema.

29.12. Promiscuous Mode: recepción de tramas no dirigidas a la MAC

Enable Promiscuous Mode mantiene la interfaz en modo promiscuo. En este estado el sistema puede procesar tramas que llegan al adaptador y que no estén destinadas a su dirección MAC, si el switch y el controlador realmente las entregan. No significa permitir libremente tráfico por el firewall ni equivale a capturar todo el tráfico de la red.

En una WAN de respaldo normal se recomienda desactivarlo. Puede tener utilidad en diseños específicos de puente o pruebas avanzadas, pero sin requisito demostrable aumenta complejidad y puede alterar el comportamiento esperado del controlador o la visibilidad del tráfico.

29.13. Switch port: seguimiento del estado de un puerto físico

En determinados equipos Netgate con switch integrado, el selector Switch port permite asociar el estado de una interfaz VLAN lógica a la portadora de un puerto físico del switch. La lista de puertos depende del modelo; no se interpreta como un mapa universal de conectores. Es especialmente útil cuando la interfaz VLAN se encuentra sobre un enlace interno siempre activo: sin seguimiento físico, puede aparentar que está conectada aun cuando su puerto exterior esté desconectado.

Debe elegirse únicamente el puerto que efectivamente determina la disponibilidad de esa conexión. Seleccionar uno ajeno puede provocar falsas caídas o estados erróneos; y asociar una VLAN compartida a un solo conector sin estudiar el diseño puede introducir dependencias inesperadas. No confundir este selector con Interfaces → Switch → Ports, con Interface Assignments ni con la configuración del tagged/untagged VLAN.

Coherencia por capas. El estado del switch físico y la pérdida de salida a Internet son incidencias distintas. Para detectar una avería del operador aunque el cable siga conectado se requiere monitorizar el gateway y, cuando proceda, una dirección de prueba situada más allá del router local.

29.14. DHCP Client Configuration: propósito y secuencia DORA

Cuando IPv4 Configuration Type es DHCP, pfSense solicita su configuración a un servidor DHCP situado en el tramo aguas arriba. El proceso habitual IPv4 emplea DISCOVER → OFFER → REQUEST → ACK y entrega dirección, prefijo, puerta de enlace y posibles servidores DNS. Un router celular puede responder

por DHCP mientras el acceso a la red móvil está desconectado; por eso una concesión válida no garantiza salida externa.

Al diagnosticar, hay que separar (a) ausencia de DHCP (capa 2, VLAN, bloqueo o servidor), (b) concesión válida sin gateway alcanzable y (c) acceso hasta el router pero sin tránsito por el operador. La duración y renovación del lease pueden producir cambios en gateway, IP y estados de conexiones.

29.15. Options: Advanced Configuration

La casilla Advanced Configuration expande ajustes de funcionamiento del cliente DHCP, principalmente temporizadores y opciones de protocolo. Desactivada, pfSense utiliza sus valores normales. Activada, la documentación oficial describe controles adicionales de timing y presets que deben mantenerse sin cambios salvo que exista una necesidad documentada por el operador o un diagnóstico reproducible.

Enlaces móviles pueden tardar en recuperar señal o cambiar la concesión cuando el CPE se reinicia; esto no justifica por sí mismo manipular los tiempos de DHCP. Primero se deben revisar los registros y el estado del equipo de acceso. Temporizaciones excesivamente agresivas pueden incrementar tráfico de control; tiempos demasiado conservadores pueden ralentizar la recuperación.

29.16. Options: Configuration Override

Configuration Override habilita el uso de un archivo de configuración DHCP alternativo, indicando su ruta completa. No se limita a cambiar una opción aislada ni restaura la concesión; puede reemplazar el comportamiento generado por la GUI. Netgate lo contempla para proveedores con requerimientos no cubiertos por los campos ordinarios.

De forma predeterminada debe permanecer desactivado. Una ruta inexistente, permisos incorrectos o sintaxis inválida pueden impedir recibir IPv4, con pérdida de conectividad en la WAN secundaria. Debe comprobarse, antes de su aplicación, dónde se mantiene el archivo, quién lo modifica y cómo será respaldado en restauraciones.

29.17. Hostname: identificador enviado en solicitudes DHCP

Hostname envía al servidor DHCP un valor de identificación y nombre de host, conforme a la ayuda del formulario y a la referencia oficial Netgate. Puede ser necesario cuando el operador asigna la concesión a un cliente conocido, pero muchas implementaciones Ethernet de routers 4G/LTE no lo requieren.

Si no existe requisito, dejarlo vacío. Si se emplea, debe ser un identificador aprobado y no revelar el nombre interno de una organización, dominio privado, ubicación, persona o dispositivo; los mensajes DHCP pueden observarse en el segmento de acceso. No confundirlo con la configuración de hostname general del firewall.

29.18. Alias IPv4 address: dirección auxiliar y longitud CIDR

Alias IPv4 address permite mantener una dirección IPv4 fija adicional asociada al cliente DHCP, acompañada de su prefijo CIDR. Es útil para alcanzar un dispositivo de gestión aguas arriba que está en otra red distinta de la dirección obtenida en el lease. El alias no reemplaza la dirección principal ni constituye una segunda conexión a Internet.

No debe elegirse una dirección arbitraria. Una máscara inadecuada puede causar solapamiento de subredes, rutas conectadas imprevistas o conflicto con otros elementos. Únicamente configurar el alias cuando el diseño lo justifique, con parámetros suministrados para ese tramo. Para documentación, los prefijos TEST-NET reservados a ejemplos no son valores de despliegue.

29.19. Reject leases from: rechazo selectivo de servidores DHCP

Reject leases from acepta direcciones IPv4 de servidores DHCP que no deben suministrar concesiones a esta interfaz, separadas por comas. La finalidad descrita por Netgate es evitar ofertas de un equipo aguas arriba que, al perder la conexión con el proveedor, entrega una IP de emergencia y aparenta mantener la WAN disponible.

En una instalación móvil, el router local puede ser precisamente el servidor DHCP legítimo incluso cuando la red celular funciona. Rechazarlo sin verificar qué dispositivo responde dejaría el enlace sin dirección. No usar este campo para rechazar una subred entera ni como sustituto de las políticas de seguridad DHCP de un switch; filtra emisores concretos identificados por IP.

Advertencia específica. No asumir que toda dirección IPv4 privada ofrecida por DHCP es errónea: en un enlace con router celular, doble NAT o CGNAT puede ser el diseño normal. Configurar un rechazo solo después de capturar y atribuir las ofertas a un servidor no autorizado.

29.20. DHCP VLAN Priority: habilitación y alcance 802.1p

Enable dhcpclient VLAN Priority tagging permite marcar mensajes del cliente DHCP con una prioridad de capa 2 conforme a 802.1p. Está normalmente desactivado y solo conviene emplearlo cuando lo exige el operador y la plataforma admite la correspondiente etiqueta 802.1Q. No es un selector de prioridad del tráfico LTE por radio ni sirve para garantizar más ancho de banda a aplicaciones.

Valor visible	Código	Significado en la GUI
0	BK	Background
1	BE	Best Effort
2	EE	Excellent Effort
3	CA	Critical Applications
4	VI	Video
5	VO	Voice
6	IC	Internetwork Control
7	NC	Network Control

Las denominaciones y los números se corresponden con los ocho elementos visibles y la tabla de Netgate. El orden mostrado expresa niveles de prioridad en el esquema pfSense; no debe interpretarse como autorización para elevar indiscriminadamente el tráfico. Primero conocer el requisito exacto del proveedor y comprobar mediante captura, si procede, que el tráfico DHCP sale con el etiquetado esperado.

29.21. Reserved Networks: reglas automáticas en la entrada

Las opciones de Reserved Networks añaden protecciones automáticas frente a determinadas direcciones de origen que no deberían iniciar conexiones por una WAN pública convencional. Estos bloqueos se aplican al tráfico entrante según la lógica de reglas de la interfaz; no son ajustes de DHCP, NAT saliente, filtrado de destino ni un sustituto de reglas de mínimo privilegio.

Su idoneidad cambia en enlaces con CPE privado, agregación, rutas de operadores o segmentos de tránsito. Es imprescindible conocer qué origen se está filtrando: la dirección IP asignada a la propia interfaz no equivale necesariamente a la dirección de origen de las tramas que llegan a esa WAN.

29.22. Block private networks and loopback addresses

Block private networks and loopback addresses bloquea orígenes de redes privadas y loopback; la propia ayuda de la pantalla cita RFC 1918 (10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16), direcciones ULA IPv6 (fc00::/7) y loopback IPv4 (127.0.0.0/8). En una WAN pública directa es una protección habitual ante tráfico entrante con direcciones de origen inesperadas.

En una WAN detrás de un router móvil que utiliza direccionamiento privado, determinados mensajes entrantes legítimos del CPE o del proveedor pueden depender de esos orígenes. Por ello, en accesos privados debe revisarse el bloqueo antes de habilitarlo. No se debe confundir recibir una concesión DHCP privada con filtrar paquetes originados en redes privadas. La configuración exacta de filtrado debe validarse en el firewall, especialmente para IPv6 y según versión.

29.23. Block bogon networks: listas de prefijos no adecuados en Internet

Block bogon networks impide que entren paquetes con origen en bloques no asignados, reservados o clasificados como bogon por las listas mantenidas por pfSense. La ayuda visible excluye RFC 1918 de esa descripción concreta; los controles de privado y bogon deben evaluarse por separado. El contenido de la lista puede variar a medida que IANA asigna nuevos bloques o se actualiza el sistema.

Netgate desaconseja este bloqueo en LAN y redes internas. En una WAN con tránsito de operador o particularidades de direccionamiento móvil, hay que revisar que la lista no descarte tráfico requerido. La frecuencia de actualización de las listas se configura en System → Advanced → Firewall & NAT, de

acuerdo con la ayuda de esta página. La excepción de una red debe implementarse con conocimiento del origen y del orden de las reglas, no desactivando filtros sin investigación.

29.24. CGNAT, direccionamiento privado y accesibilidad remota

En redes móviles es frecuente que la IP de la conexión no sea una dirección pública alcanzable desde Internet, por el uso de NAT en el router del abonado, en el operador o en ambos. CGNAT hace que varios abonados compartan direcciones públicas aguas arriba. El espacio 100.64.0.0/10 (RFC 6598) es de uso compartido de operadores, distinto de los rangos RFC 1918; su presencia puede ser una pista, no una demostración por sí sola del punto exacto de traducción.

Es posible que aplicaciones salientes funcionen y que, sin embargo, no sea viable publicar puertos entrantes directamente. Para asistencia remota y VPN, priorizar arquitecturas donde el extremo local inicie un túnel saliente hacia un punto alcanzable, o contratar un servicio de IP pública cuando el caso lo requiera. Un cambio de WAN puede alterar la IP pública efectiva, romper sesiones o exigir actualización DNS y reconexión de túneles.

29.25. Preparación Multi-WAN: gateways, monitorización y grupo de reserva

Una segunda WAN operativa necesita un gateway válido, normalmente descubierto mediante DHCP, y monitorización de disponibilidad. En System → Routing → Gateways se revisa el gateway y se puede indicar una Monitor IP adecuada. Si la monitorización verifica solo el CPE local, puede seguir marcando «Online» aunque la red móvil carezca de acceso a Internet. Siempre que sea viable, elegir un objetivo externo estable, accesible y representativo, con monitor IP distinta para cada gateway cuando Netgate lo requiera.

El grupo de conmutación se define en System → Routing → Gateway Groups. Situar la vía prioritaria en Tier 1 y la móvil en Tier 2 significa preferir el primer gateway cuando se considera disponible, utilizando el segundo en las condiciones de caída definidas. El grupo por sí solo no modifica el tráfico: hay que seleccionar el grupo como gateway predeterminado para tráfico del propio firewall y/o en reglas aplicables a clientes, respetando los requerimientos de la configuración.

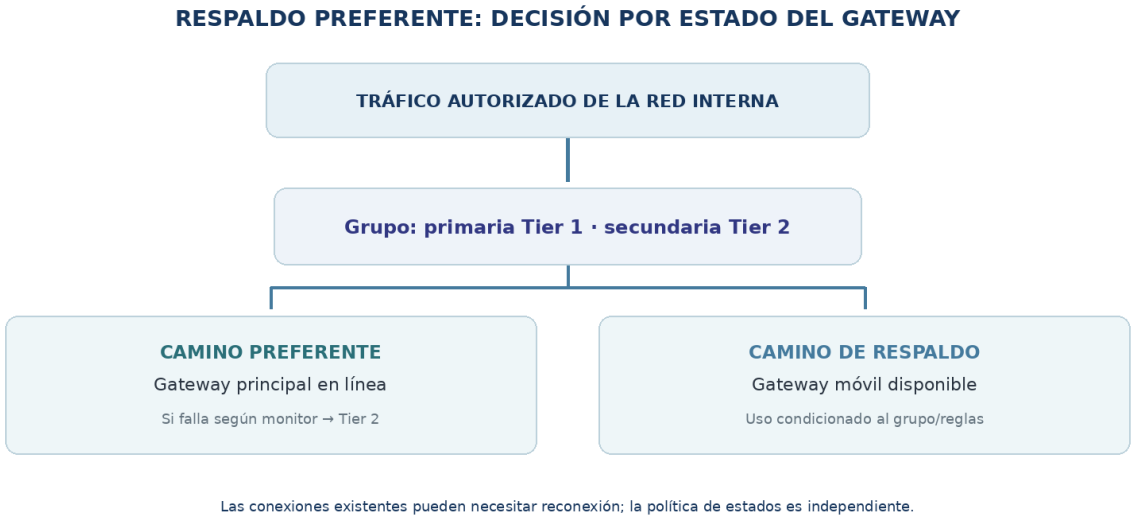


Figura 29.2. Priorización conceptual de salida principal y secundaria; el grupo debe utilizarse en la configuración real.

29.26. Monitorización de disponibilidad: qué constituye un fallo

El proceso de monitorización evalúa conectividad hacia un destino de prueba y dispone de parámetros de latencia, pérdida y umbrales de activación. Una interfaz Ethernet «Active» no implica que el operador móvil pueda enrutar tráfico a Internet, y un gateway «Online» solo significa que el monitor responde bajo las condiciones configuradas; pueden seguir existiendo errores de DNS, congestión o incidencias de una aplicación concreta.

No conviene elegir destinos de monitorización que ignoren ICMP o que funcionen exclusivamente por la conexión principal; tampoco se deben fijar parámetros de pérdida excesivamente sensibles en líneas

celulares variables, porque pueden producir oscilación repetida entre enlaces. Documentar umbrales y comprobarlos con pruebas de conmutación controladas.



Figura 29.3. Comprobaciones independientes para evitar diagnósticos falsos en conexiones de respaldo.

29.27. Reglas, NAT y DNS: completar la continuidad de servicio

El tráfico de los clientes suele seguir las reglas de entrada de las interfaces locales. Cuando una regla usa un gateway o gateway group, aplica policy routing al tráfico que coincide con ella. El orden de las reglas importa: la primera coincidencia determina el resultado. El grupo de failover también puede ser elegido como default gateway para servicios originados por el propio firewall, pero esa elección no reemplaza las reglas necesarias en las LAN.

El NAT automático de salida suele crear traducciones para interfaces de tipo WAN, incluida la secundaria. En modo NAT manual deben existir reglas expresas para esa salida; en modo híbrido deben revisarse las excepciones. NAT traduce direcciones, no selecciona la ruta. DNS requiere una configuración coherente para multi-WAN: resolución del firewall, forwarding y servidores asociados a gateways según la modalidad. Revisar además VPN, VoIP y servicios ligados a una dirección específica.

Precaución sobre las sesiones. Durante la conmutación, conexiones ya establecidas pueden permanecer asociadas al enlace anterior y requerir reconexión o política de eliminación de estados. La eliminación indiscriminada de estados es disruptiva; no debe considerarse obligatoria sin analizar servicios de voz, ERP, VPN y teletrabajo.

29.28. Procedimiento A: habilitar y validar la interfaz secundaria con DHCP

01. Antes de intervenir, realizar copia segura de la configuración y confirmar una vía de acceso a consola o administración alternativa.
02. Verificar físicamente la conexión Ethernet del equipo de acceso, su alimentación, el puerto de switch y, cuando exista, la coherencia de VLAN y asignación.
03. Entrar en Interfaces → interfaz opcional seleccionada y marcar Enable interface. Introducir una descripción genérica funcional.
04. Elegir IPv4 Configuration Type = DHCP solo cuando el dispositivo de acceso entregue concesiones mediante DHCP. Ajustar IPv6 según servicio disponible, sin presuponer delegación.
05. Mantener MAC Address, MTU y MSS sin cambios, salvo requisito acreditado; dejar Promiscuous Mode desactivado.
06. Configurar Switch port únicamente si el hardware permite el seguimiento y se ha identificado con certeza el puerto de esa salida.
07. Dejar Advanced Configuration y Configuration Override desactivados si no hay requisitos del operador; no filtrar ningún servidor DHCP legítimo.
08. Revisar Block private networks y Block bogon networks en función del tipo real de tránsito, no por el nombre «WAN». Guardar y aplicar cambios.

09. En Status → Interfaces verificar concesión IPv4, máscara y estado; en Status → Gateways verificar pasarela y monitorización.
10. Hacer pruebas salientes acotadas por la WAN secundaria sin alterar aún todo el tráfico y registrar el resultado.

29.29. Procedimiento B: configurar failover con datos móviles limitados

01. En System → Routing → Gateways comprobar la existencia de la pasarela principal y la secundaria. Revisar que cada una tiene un destino de monitorización válido y diferenciado.
02. En System → Routing → Gateway Groups crear un grupo de conmutación con gateway principal Tier 1 y móvil Tier 2; establecer un Trigger Level apropiado para los umbrales admitidos.
03. Considerar el grupo como pasarela predeterminada en System → Routing → Gateways, de acuerdo con las necesidades de tráfico originado en el propio firewall.
04. En Firewall → Rules, sobre las interfaces internas que deben tener continuidad, usar el gateway group en las reglas de salida pertinentes, sin redirigir sin necesidad tráfico de gestión local o redes internas.
05. Revisar Firewall → NAT → Outbound: en modo automático verificar traducción esperada; en modo híbrido/manual comprobar reglas específicas hacia la WAN móvil.
06. Revisar DNS Resolver/Forwarder y servidores DNS asociados a gateways, especialmente si el modo de resolución depende de salidas concretas.
07. Definir qué aplicaciones se permiten durante el respaldo: servicios esenciales antes que grandes transferencias, copias masivas o actualizaciones automáticas.
08. Simular la caída de la principal de forma programada, observar Status → Gateways y probar el restablecimiento de nuevas conexiones, DNS y servicios de negocio.
09. Devolver la conexión principal al servicio y comprobar recuperación, estados, VPN y ausencia de oscilaciones; documentar política de estados y consumo de datos.

29.30. Procedimiento C: comprobar DHCP, VLAN, MTU y portadora

01. Confirmar si el enlace físico se negocia: portadora y velocidad/dúplex, sin asumir que un estado lógico VLAN implica cable conectado.
02. Si el enlace se mantiene activo pero no llega DHCP, capturar el intercambio DISCOVER/OFFER y revisar switch, etiquetado, DHCP legítimo y puertos.
03. Cuando DHCP responde, confirmar lease, gateway, vigencia y que el servidor no figure accidentalmente en Reject leases from.
04. Si el gateway del router local responde pero falla Internet, comprobar conectividad exterior mediante el mismo enlace y revisar estado de red móvil/APN en el equipo de acceso.
05. Para errores con ficheros grandes o VPN, investigar PMTUD y medir la MTU real antes de modificar MSS; realizar una variación controlada por vez.
06. Si se sospechan cortes de enlace no detectados, examinar el selector Switch port cuando exista en el equipo y correlacionar sus eventos con los logs.

29.31. Escenarios empresariales orientativos

Escenario neutro	Decisión de diseño	Pruebas mínimas
Conexión de respaldo de bajo consumo	Failover Tier 2 y restricciones de aplicaciones no críticas.	Consumo, tiempo de recuperación y transacciones.
Router móvil detrás de NAT privado	DHCP, revisar filtros de orígenes privados y acceso a CPE.	Gateway, gestión local y llegada a Internet.
Servicios VPN en ambas WAN	Diseñar endpoints, DDNS, IP pública o túnel saliente.	Negociación y reconexión desde salida secundaria.
Enlace móvil con latencia variable	Monitorización con umbrales tolerantes y evidencia de calidad.	Pérdida, RTT, jitter, falsos failover.
VLAN sobre switch integrado	Separar puerto portadora, VLAN y asignación.	Carrier, DHCP y camino efectivo sin bucles.

29.32. Comprobación operativa: herramientas y evidencias

Herramienta / ruta	Qué observar	Interpretación
Status → Interfaces	IP/prefijo, gateway DHCP, enlace y estadísticas.	Acredita estado local, no Internet por sí mismo.
Status → Gateways	Online/Offline/Warning, pérdida y latencia.	Evalúa el objetivo monitorizado y el grupo.
System → Routing	Pasarela por defecto y grupos.	Determina rutas del firewall y prioridades de failover.
Diagnostics → Routes	Ruta predeterminada y rutas específicas.	Identifica salidas inesperadas o rutas persistentes.
Firewall → Rules / NAT	Policy routing y NAT de salida.	Comprueba qué tráfico se dirige y traduce.
Diagnostics → Packet Capture	DHCP, ICMP, TCP SYN/MSS y pruebas de puertos.	Aísla errores de cada capa.
Status → System Logs	Eventos DHCP, gateways, interfaces y firewall.	Detecta renovaciones, oscilaciones y descartes.
Diagnostics → DNS Lookup / Ping	Consultas DNS y pruebas de conectividad.	Distingue DNS de fallo de ruta.
Status → Traffic Graph	Tráfico saliente durante un ensayo.	Detecta consumo inesperado en la WAN móvil.

29.33. Errores frecuentes y ruta de resolución

Síntoma	Origen probable	Diagnóstico/corrección
Carrier activo, sin IP	Servidor DHCP inaccesible o VLAN/puerto incorrectos.	Captura DHCP y verificación de switch.
IP válida, sin Internet	Equipo celular sin servicio, rutas o DNS incorrectos.	Probar gateway y monitor remoto por interfaz.
No cambia a respaldo	Gateway group no aplicado o monitor principal sigue Online.	Revisar Tier, trigger, reglas y Default Gateway.
Conmuta repetidamente	Latencia/pérdida variable y umbrales sensibles.	Revisar monitor, temporización y cobertura.
VPN no conecta tras el cambio	CGNAT, IP distinta, túnel ligado a WAN o rutas.	Comprobar endpoint, DDNS y reconexión.
Se consume el bono de datos	Actualizaciones o flujos no críticos pasan por backup.	Policy routing, reglas de tráfico y consumo.
Se pierden sesiones activas	Estados permanecen en gateway anterior.	Evaluar política de estados antes de borrarlos.
No hay acceso al router móvil	Reglas de privados o ruta de gestión.	Distinguir IP propia, orígenes y destinos.
No se detecta cable retirado	Interfaz VLAN sobre puerto padre interno.	Verificar Switch port y monitorización real.
Solo falla tráfico grande	MTU/PMTUD o encapsulación.	Analizar ICMP, SYN/MSS y túneles.
IPv6 falla pero IPv4 funciona	DHCP6, RA, delegación o política IPv6.	Revisar pila IPv6 independientemente.

29.34. Riesgos de administración y medidas de seguridad

En redes empresariales, las operaciones sobre esta pantalla pueden afectar simultáneamente al acceso remoto, la telefonía IP, el filtrado de orígenes, las VPN y el comportamiento de tráfico entrante. Antes de guardar, registrar modo IP, estado de la interfaz, configuración de filtros, versión del firmware y condiciones de monitorización; después verificar la continuidad del servicio.

01. Mantener un medio de gestión fuera de banda o consola local para cambios de interfaz, VLAN y gateway.
02. No copiar identificadores del proveedor, direcciones internas ni información de dispositivos a manuales o tickets abiertos.

03. Evitar valores de DHCP avanzado, MAC fija y ajustes MTU/MSS sin evidencia de necesidad.
04. Tratar la red móvil como no confiable; aplicar política de mínimo privilegio y comprobar IPv6 además de IPv4.
05. Diseñar reglas para impedir que copias, parches o descargas masivas agoten el plan de datos en respaldo.
06. Vigilar que las sondas y los servicios del firewall no generen consumo excesivo en el circuito celular.
07. Conservar copia cifrada de configuración y plan de recuperación verificable.
08. Registrar impacto sobre VPN, publicaciones de puertos, IP pública y DNS dinámico después de conmutar.

29.35. Lista de verificación para puesta en producción

Control de aceptación	Evidencia exigible
Interfaz habilitada y descripción comprensible	Nombre funcional y estado en Status → Interfaces.
Selección IPv4/IPv6 correcta	Concesión/parametrización verificadas de forma independiente.
Capa 2 y puerto correctos	Portadora, switch/VLAN y estado coincidentes.
DHCP normal sin filtros innecesarios	Concesión estable y servidor legítimo reconocido.
Filtros de privados/bogons justificados	No se bloquean orígenes válidos para ese acceso.
Gateway monitorizado externamente cuando procede	Monitor con respuesta y umbrales realistas.
Grupo de failover integrado en tráfico	Tier correcto, default gateway/reglas revisadas.
NAT, DNS y VPN preparados	Pruebas exitosas con secundaria como salida.
Consumo móvil y política de sesiones definidos	Controles, responsables y plan de reversión.
Conmutación ensayada y documentada	Acta de ensayo con caída y recuperación.

29.36. Glosario especializado

Término	Definición aplicada
OPT	Interfaz opcional; puede ser WAN, LAN, DMZ u otra función según configuración.
CPE	Equipo de acceso del operador o situado aguas arriba de pfSense.
DHCP lease	Concesión temporal de parámetros IPv4.
Carrier	Portadora física del enlace Ethernet.
Gateway	Siguiente salto hacia otra red o hacia el exterior.
Failover	Cambio a otra ruta cuando la preferida falla conforme a una política.
Tier	Prioridad de gateways dentro de un grupo de conmutación.
dpinger	Proceso empleado por pfSense para monitorizar gateways.
CGNAT	NAT de operador que puede impedir acceso directo entrante.
PMTUD	Path MTU Discovery: detección de tamaño de paquete viable en la ruta.
802.1p PCP	Prioridad de tramas en capa 2, separada de la QoS radio LTE.
State table	Tabla de estados de conexiones del firewall.

29.37. Referencias oficiales y notas de versión

Referencias oficiales de Netgate consultadas el 17 de noviembre de 2026. La versión exacta de pfSense Plus no está especificada; por tanto, las diferencias de controles y funciones condicionadas por tipo de

interfaz o hardware deben contrastarse con el sistema administrado. Los enlaces siguientes son públicos y no contienen información de ninguna instalación.

Interface Configuration — https://docs.netgate.com/pfsense/en/latest/interfaces/configure.html

IPv4 Configuration Types / DHCP — https://docs.netgate.com/pfsense/en/latest/interfaces/configure-ipv4.html

IPv6 Configuration Types — https://docs.netgate.com/pfsense/en/latest/interfaces/configure-ipv6.html

Interface Naming Terminology — https://docs.netgate.com/pfsense/en/latest/general/interface-names.html

WAN vs LAN Interfaces — https://docs.netgate.com/pfsense/en/latest/interfaces/wanvslan.html

VLAN Priority — https://docs.netgate.com/pfsense/en/latest/vlan/priority.html

Multi-WAN Terminology and Concepts — https://docs.netgate.com/pfsense/en/latest/multiwan/concepts.html

Load Balancing and Failover with Gateway Groups — https://docs.netgate.com/pfsense/en/latest/multiwan/load-balance-and-failover.html

Summary of Multi-WAN Requirements — https://docs.netgate.com/pfsense/en/latest/multiwan/requirements.html

Gateway Settings — https://docs.netgate.com/pfsense/en/latest/routing/gateway-configure.html

Managing the Default Gateway — https://docs.netgate.com/pfsense/en/latest/routing/gateways.html

Multi-WAN and NAT — https://docs.netgate.com/pfsense/en/latest/multiwan/nat.html

Multi-WAN Caveats and Considerations — https://docs.netgate.com/pfsense/en/latest/multiwan/considerations.html

Verifying Functionality — https://docs.netgate.com/pfsense/en/latest/multiwan/test.html

Gateway Status — https://docs.netgate.com/pfsense/en/latest/monitoring/status/gateways.html

Troubleshooting Multi-WAN — https://docs.netgate.com/pfsense/en/latest/troubleshooting/multi-wan.html

Gateway Monitoring – Miscellaneous — https://docs.netgate.com/pfsense/en/latest/config/advanced-misc.html

ANEXO 29.A / REGISTRO DE PRUEBAS DE CONMUTACIÓN

Ficha reutilizable para validar la operatividad del respaldo. Los resultados deben archivarse en un sistema interno con acceso controlado; no introducir en copias públicas IP, identificadores de acceso, números de SIM ni datos de clientes.

Prueba de aceptación	Evidencia esperada
A. Estado previo	Dos gateways conocidos; la conexión preferida cursa nuevas sesiones.
B. Pérdida controlada de primaria	Se detecta fallo en el monitor y el Tier 2 pasa a ser elegible.
C. Navegación y DNS	Nuevas conexiones y resolución DNS funcionan por la vía de respaldo.
D. Servicio crítico elegido	La aplicación funcional priorizada supera una transacción de prueba.
E. Restricción de tráfico	El acceso móvil no transporta descargas o flujos no autorizados.
F. VPN o enlace remoto	Se verifica reconexión; se documentan límites de CGNAT si aplican.
G. Recuperación de primaria	Los gateways regresan al estado previsto, sin flapping persistente.
H. Registro y reversión	Se conservan resultados, incidencias y procedimiento de recuperación.

Criterio de aceptación: la WAN secundaria se considera lista para contingencia únicamente cuando la prueba confirma conectividad real de los servicios previstos, no solo el estado físico y la concesión DHCP.

Parte III Firewall

30 Firewall → Introducción general

Políticas de acceso, traducción de direcciones, estados y calidad de servicio

Ruta de acceso: Firewall (menú principal de pfSense Plus). Este capítulo establece el marco conceptual para administrar sus siete apartados, comprender las dependencias entre funciones y reducir el riesgo operativo de las modificaciones. No presupone una versión exacta ni reproduce configuraciones de terceros.



Figura 30.1. Relación funcional entre los siete apartados del menú Firewall.

30.1. El firewall como punto de decisión de la red

En una red con varias zonas, el firewall es el elemento que decide qué comunicaciones pueden atravesar sus interfaces. pfSense Plus utiliza el motor Packet Filter (PF) y combina filtrado con estado, traducción de direcciones, enrutamiento, monitorización y herramientas de priorización. Su función no es únicamente bloquear accesos desde Internet: también delimita la comunicación entre segmentos internos, hacia servicios remotos y a través de túneles VPN.

La pantalla de navegación ofrece siete opciones: Aliases, NAT, Packet Flow Data, Rules, Schedules, Traffic Shaper y Virtual IPs. Son mecanismos relacionados, pero cada uno responde a una pregunta diferente: qué identificar, qué traducir, qué observar, qué permitir, cuándo aplicarlo, cómo distribuir capacidad y con qué direcciones adicionales trabajar.

Este capítulo presenta la arquitectura del firewall. Las pantallas de edición de reglas, NAT y otros módulos tienen pestañas y campos que se desarrollan en sus capítulos correspondientes. Los menús y las funciones pueden incorporar cambios según la versión instalada.

30.2. Mapa del menú y responsabilidad de cada apartado

Opción exacta	Ruta	Finalidad principal
Aliases	Firewall → Aliases	Definir conjuntos reutilizables de hosts, redes y puertos.
NAT	Firewall → NAT	Gestionar redirecciones y traducciones de direcciones.
Packet Flow Data	Firewall → Packet Flow Data	Exportar metadatos de flujos NetFlow/IPFIX desde estados PF.
Rules	Firewall → Rules	Definir políticas de paso, bloqueo y rechazo.
Schedules	Firewall → Schedules	Definir calendarios utilizados por reglas horarias.

Opción exacta	Ruta	Finalidad principal
Traffic Shaper	Firewall → Traffic Shaper	Priorizar o limitar tráfico mediante colas y limitadores.
Virtual IPs	Firewall → Virtual IPs	Asignar direcciones adicionales y recursos de alta disponibilidad.
Lectura correcta del menú. Los apartados son accesos administrativos, no etapas ejecutadas en ese mismo orden. El procesamiento real depende de PF, del sentido del paquete, NAT, estados y reglas automáticas.		

30.3. Fundamento: filtrado con estado (stateful)

Una regla de paso puede crear un estado que asocia una comunicación con su origen, destino, protocolo y puertos. Los paquetes de respuesta de una comunicación ya autorizada suelen atravesar el firewall al coincidir con su estado, sin necesitar una regla simétrica de paso en la interfaz de retorno. Este comportamiento simplifica las políticas y mejora la eficiencia, pero exige revisar los estados cuando se investiga un cambio de permisos.

Un bloqueo añadido después del establecimiento de una conexión no garantiza cortar inmediatamente esa sesión: el estado existente puede seguir permitiéndola. La eliminación selectiva de estados puede ser necesaria, pero interrumpe comunicaciones; conviene realizarla con criterio y después de registrar el impacto. Existen excepciones, como reglas sin estado y filtrado Ethernet de capa 2.

30.4. Dirección de evaluación: la interfaz de entrada

Las reglas normales de pestañas de interfaz se evalúan cuando el tráfico entra en el firewall por esa interfaz. Una conexión iniciada desde una LAN hacia Internet se controla normalmente con reglas de entrada en esa LAN, no con una regla WAN para el paquete de ida. En cambio, una conexión iniciada desde el exterior hacia un servicio publicado se evalúa en la WAN de entrada tras las traducciones de destino que correspondan.

Existen también reglas Floating, que pueden actuar en direcciones de entrada o salida, y reglas de grupos de interfaces o pestañas VPN. Las reglas de los grupos y las Floating pueden preceder a las de una interfaz y afectar a lo que parecía permitido localmente.

30.5. Orden de reglas, prioridad y política por defecto

En las reglas ordinarias de interfaz rige, en general, la primera coincidencia de arriba abajo: se ejecuta la acción y se detiene la evaluación. Las reglas Floating sin Quick son una excepción importante porque admiten un comportamiento en el que puede prevalecer una coincidencia posterior. Se deben consultar el sentido, el indicador Quick y el tipo de regla antes de interpretar conflictos.

La estrategia recomendada es denegar por defecto y permitir expresamente los flujos justificados. En configuraciones iniciales habituales pfSense permite salidas amplias desde LAN y bloquea nuevas entradas WAN, pero esa condición inicial no constituye una política empresarial definitiva ni se debe extrapolar a todas las interfaces OPT, grupos o VPN.

30.6. Procesamiento conceptual: NAT, reglas y estados

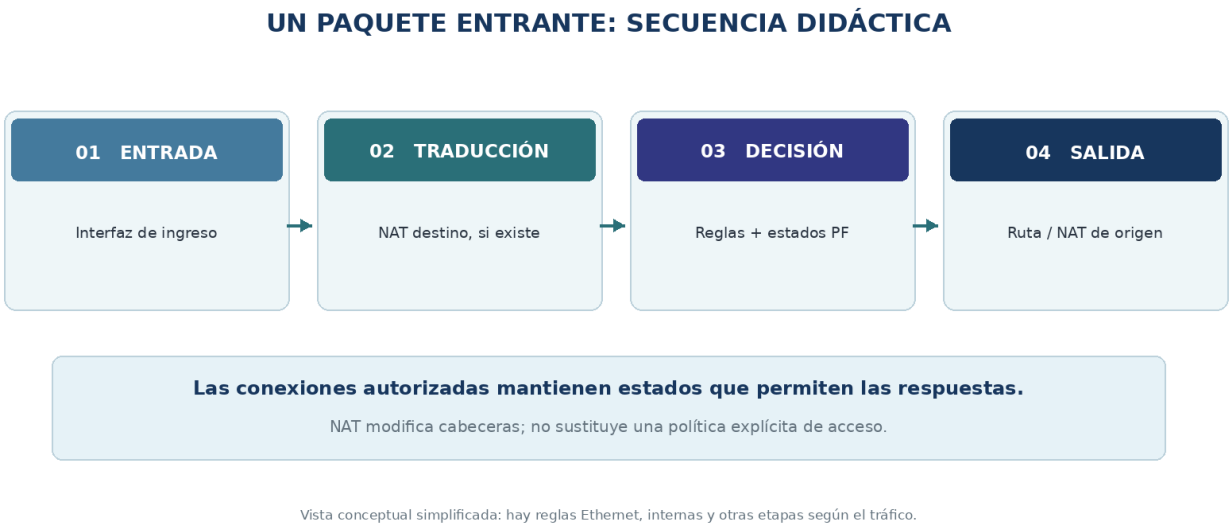


Figura 30.2. Visión resumida de la inspección de un paquete que atraviesa pfSense Plus.

NAT y firewall no son sinónimos. NAT cambia una dirección o puerto según reglas de traducción; Rules decide si el paquete puede atravesar el sistema. En una publicación habitual, el DNAT/port forward se realiza antes de evaluar la regla de filtrado de entrada, por lo que la regla suele referirse al destino interno ya traducido. En el tráfico saliente, SNAT/Outbound NAT se aplica cuando corresponde a la salida seleccionada.

El orden completo incluye reglas Ethernet opcionales, reglas internas automáticas, controles dinámicos y reglas de usuario. Puede variar con opciones avanzadas, reglas Floating y escenarios bidireccionales. El diagrama resume la lógica básica de flujo, no sustituye el orden documentado por Netgate.

30.7. Aliases: política legible y mantenible

Aliases permite agrupar hosts, redes o puertos bajo un nombre técnico reutilizable. Una misma lista puede emplearse en múltiples reglas y, al actualizar sus elementos, simplificar el mantenimiento de la política. Son especialmente útiles cuando diferentes equipos comparten un permiso o una restricción y cuando la legibilidad es importante para auditorías.

La documentación diferencia alias de IP, Ports, URLs y vistas generales. Un alias no es una regla por sí mismo: necesita ser referenciado. Tampoco equivale a una dirección virtual de tipo IP Alias. Un alias con hostnames puede depender de resolución DNS; las tablas dinámicas deben comprobarse en Diagnostics → Tables si existe incertidumbre sobre sus miembros actuales.

30.8. NAT: traducir no implica autorizar

NAT (Network Address Translation) gestiona transformaciones de direcciones y, cuando procede, puertos. Port Forward redirige tráfico entrante hacia un servicio; 1:1 NAT relaciona direcciones en ambos sentidos bajo su alcance configurado; Outbound NAT traduce salidas de redes hacia otras interfaces. Existen modalidades automáticas, híbridas y manuales para el NAT de salida.

Una redirección no debería publicarse sin evaluar reglas, superficies expuestas, cifrado de la aplicación y restricciones de origen. Asimismo, NAT de salida no sustituye la ruta correcta: traducir hacia una dirección no obliga al sistema a seleccionar esa interfaz. En redes IPv6 se privilegia el direccionamiento y filtrado explícitos, sin asumir que el NAT44 sea el modelo de referencia para todo el tráfico.

30.9. Packet Flow Data: telemetría de flujos en pfSense Plus

Packet Flow Data es una prestación específica de pfSense Plus desde la versión 24.03. Usa pflow(4) de PF para exportar datos de flujo desde los estados del firewall a colectores mediante NetFlow v5 o IPFIX, sin depender de un daemon adicional. Puede configurarse exportación global o selectiva por reglas y admitirse varias configuraciones de destino. Su disponibilidad exige comprobar la versión; no debe presuponerse en pfSense CE.

NetFlow v5 tiene limitaciones de representación y no incluye flujos IPv6; IPFIX ofrece más flexibilidad e información IPv6. La exportación está ligada a la creación de estados, de modo que los cambios de activación no convierten automáticamente sesiones antiguas en flujos nuevos. También es distinta de una captura PCAP: describe metadatos de tráfico, no el contenido íntegro de los paquetes.

Privacidad y seguridad. Los registros de flujos pueden revelar patrones de comunicación, destinos y volúmenes. Deben enviarse únicamente a colectores autorizados, proteger su transporte, limitar la conservación y aplicar el marco de privacidad de la organización. Restablecer todos los estados para obtener datos inmediatos puede cortar servicios.

30.10. Rules: el corazón de la política de acceso

En Firewall → Rules se organizan reglas por interfaces, grupos y otros contextos disponibles. Cada regla expresa una acción (Pass, Block o Reject, según corresponda), protocolo, origen, destino y parámetros adicionales. Se pueden utilizar alias, descripciones, registro de coincidencias, horarios, gateways y opciones avanzadas para modelar decisiones operativas con trazabilidad.

Antes de crear una regla conviene responder seis preguntas: ¿quién inicia?, ¿desde qué interfaz?, ¿a qué destino?, ¿mediante qué servicio o protocolo?, ¿en qué horario?, ¿qué debe ocurrir con el resto del tráfico? El objetivo es evitar permisos ambiguos y excepciones más amplias que la necesidad técnica.

30.11. Block, Reject y Pass: diferencia operacional

Acción	Comportamiento conceptual	Elección habitual
Pass	Permite el tráfico que cumple la condición; normalmente crea estados.	Flujos expresamente autorizados.
Block	Descarta sin responder expresamente al origen.	Denegación silenciosa, especialmente en perímetros.
Reject	Deniega y devuelve una respuesta compatible con el protocolo cuando procede.	Denegaciones donde se desea notificar rápidamente al cliente.

El comportamiento preciso de Reject depende del protocolo y del contexto. No debe confundirse registrar un evento con enviar respuesta, ni considerarse que una regla Block es suficiente para evitar que un servicio expuesto acepte conexiones por otra regla previa.

30.12. Schedules: horarios vinculados a las reglas

Schedules define calendarios que se asocian a reglas. Durante un periodo activo, la regla puede evaluarse conforme a su acción; fuera del horario, la regla se comporta como si no estuviese en el conjunto efectivo. No se transforma automáticamente un Pass en Block ni un Block en Pass. Por ello hay que revisar las reglas siguientes y las condiciones de acceso fuera de horario.

Los cambios de calendario y de reloj deben revisarse con la zona horaria/NTP. Las conexiones existentes pueden requerir políticas de estados para que la restricción temporal surta efecto exactamente cuando cambia el horario. El uso más seguro es crear una regla horaria específica dentro de una política por defecto restrictiva.

30.13. Traffic Shaper: priorizar y limitar, no aumentar capacidad

Traffic Shaper configura mecanismos de calidad de servicio (QoS) para administrar congestión. ALTQ organiza colas y prioridades, pero depende de compatibilidad con controladores y puede reducir el rendimiento máximo. Los Limiters permiten límites de velocidad y políticas de reparto sobre una dirección, usuario o grupo, según su configuración.

Su valor aparece especialmente en enlaces saturados: priorizar aplicaciones sensibles a la latencia, evitar que transferencias masivas ocupen toda la línea y repartir recursos. La aplicación exige conocer el ancho de banda efectivo y medir latencia, pérdidas y utilización antes y después. El shaper no crea ancho de banda ni corrige pérdida física de señal.

30.14. Virtual IPs: direcciones adicionales y HA

Virtual IPs permite a pfSense utilizar o anunciar direcciones IP adicionales para NAT, publicación, servicios locales o alta disponibilidad. Netgate distingue cuatro tipos principales: IP Alias, CARP, Proxy ARP y Other. No todas las variantes se asignan a servicios locales ni responden al ping del mismo modo.

Tipo de VIP	Uso típico	Consideración esencial
IP Alias	Dirección adicional con servicios locales y NAT.	Puede responder a ARP y usarse para binding.
CARP	Dirección compartida en diseños de alta disponibilidad.	Exige coordinación entre miembros y conectividad L2 adecuada.
Proxy ARP	Responder ARP por direcciones usadas para NAT.	La dirección no se configura como IP local para servicios.
Other	Hacer utilizable una dirección ya encaminada al firewall.	No anuncia ARP ni sirve como dirección local de servicio.

Un alias de objetos y un VIP IP Alias son conceptos distintos. Añadir una VIP tampoco equivale a crear una redirección o a autorizar un puerto; cada aspecto requiere su propia configuración. En entornos de alta disponibilidad deben comprobarse dependencias del switch, sincronización y retorno de tráfico.

30.15. Dependencias entre las siete funciones

Necesidad de negocio	Elemento principal	Complementos a revisar
Permitir acceso concreto entre zonas	Rules	Aliases, rutas, estados, DNS, horarios.
Publicar un servicio interno	NAT + Rules	Virtual IPs si hay direcciones adicionales, TLS, logs.
Auditar patrones de conectividad	Packet Flow Data	Colector, estados, políticas de registro y retención.
Permitir acceso solo en horario	Schedules + Rules	Reloj, reglas posteriores y estados activos.
Controlar saturación	Traffic Shaper	Tipo de limitador/cola, métricas, capacidades WAN.
Configurar IP adicional	Virtual IPs	NAT, rutas, ARP, alta disponibilidad y reglas.

30.16. Un modelo de seguridad para varias zonas

Un diseño empresarial sencillo puede separar usuarios, servidores, servicios publicados y administración en distintas interfaces o VLAN. El firewall decide qué flujos cruzan cada frontera: por ejemplo, permitir desde los usuarios solo los puertos necesarios para una aplicación alojada en una zona de servidores, y denegar la iniciativa desde la zona publicada hacia la administración salvo una excepción documentada.

La segmentación no se logra únicamente creando VLAN; requiere políticas entre ellas, reglas coherentes en la interfaz de ingreso y control de rutas alternativas. Un dispositivo que comparta segmento de capa 2 con otro puede comunicarse localmente sin pasar por el firewall; deben considerarse las fronteras reales de tráfico.

30.17. IPv4, IPv6 y políticas equivalentes

pfSense evalúa las familias IPv4 e IPv6 de manera diferenciada cuando así se especifica en las reglas. Es frecuente definir controles restrictivos para IPv4 y olvidar que una red IPv6 puede disponer de salida independiente. Se debe inventariar qué familias están habilitadas en cada interfaz y autorizar ambas solo cuando la aplicación lo requiere.

Las traducciones NAT de IPv4 no reemplazan las reglas de entrada/salida de IPv6. Además, registros de flujos en formato NetFlow v5 no cubren IPv6, por lo que el formato IPFIX puede ser necesario para observabilidad completa.

30.18. Interacción con VPN, rutas y WAN múltiples

Las comunicaciones VPN pueden aparecer en pestañas de interfaz o grupos, y su prioridad de reglas puede sorprender si existen permisos globales demasiado amplios. En sistemas con varias WAN, las reglas pueden asignar una pasarela o un grupo, produciendo policy routing. Esta selección puede afectar a la respuesta de una conexión entrante y debe coordinarse con NAT, rutas, gateway monitoring y estados.

La configuración de una regla no garantiza por sí sola conectividad: además tienen que existir rutas de ida y retorno, DNS cuando se utilizan nombres, traducciones cuando sean precisas, y ausencia de un bloqueo prioritario. La clasificación de una WAN mediante DHCP o puerta de enlace no debe confundirse con un permiso de paso.

30.19. Escenario práctico A: navegación desde una zona interna

01. Identificar una zona de origen y concretar qué servicios necesita alcanzar en el exterior.
02. Comprobar que el tráfico entra en el firewall por la interfaz correspondiente a esa zona.
03. Construir alias para orígenes, destinos o puertos si simplifican la política.
04. Crear las reglas Pass mínimas necesarias en la interfaz de entrada, con descripciones verificables.
05. Comprobar si el tráfico necesita NAT de salida para la WAN seleccionada.
06. Verificar resolución DNS, ruta, generación de estados y resultados en los registros.
07. Documentar los flujos permitidos y el comportamiento esperado para tráfico no autorizado.

30.20. Escenario práctico B: publicación controlada de un servicio

01. Validar que la publicación desde Internet es imprescindible y que el servidor está actualizado y segmentado.
02. Definir el origen permitido, servicio, interfaz WAN y dirección de destino tras la traducción.
03. Crear una redirección Port Forward cuando la arquitectura lo exija; revisar la regla de firewall asociada.
04. Limitar orígenes y protocolos, activar registros útiles y proteger la aplicación con autenticación y cifrado.
05. Probar desde una red externa de confianza, sin asumir que una prueba interna reproduce el camino de Internet.
06. Verificar la dirección traducida de destino y el retorno; revisar los registros y retirar permisos innecesarios.

30.21. Escenario práctico C: acceso temporal de mantenimiento

Una empresa necesita permitir durante una ventana planificada una conexión técnica específica. Se crea un alias para destinos autorizados, un Schedule para el intervalo, y una regla Pass limitada a interfaz, origen y servicio. Fuera del intervalo debe prevalecer la política restrictiva; no basta con definir el calendario. Es necesario confirmar qué sucede con las sesiones abiertas al terminar la ventana.

30.22. Escenario práctico D: continuidad y calidad de servicio

En un acceso limitado o un circuito de contingencia se puede limitar ancho de banda de flujos no críticos y priorizar una aplicación de comunicación. Primero medir capacidad estable, latencia y pérdidas, después seleccionar el mecanismo ALTQ o Limiters, asociarlo a las reglas oportunas y medir el efecto. Repetir las pruebas en cada WAN si el ancho de banda cambia con la ruta de salida.

30.23. Procedimiento de inspección inicial sin modificar producción

01. Entrar en Firewall y comprobar que se presentan los siete apartados de navegación.
02. Revisar Aliases e identificar los conjuntos usados de forma recurrente, sin modificarlos.
03. En NAT, determinar el modo de Outbound NAT y la existencia de redirecciones y asociaciones con reglas.
04. En Rules, recorrer pestañas de interfaces y grupos; localizar permisos amplios, registros y políticas de administración.

05. Comprobar en Schedules los calendarios activos y las reglas que los utilizan.
06. Identificar la existencia de políticas Traffic Shaper y direcciones Virtual IPs.
07. Revisar si Packet Flow Data está configurado y cuál es su destino autorizado, cuando la versión lo permita.
08. Generar un inventario técnico anónimo de dependencias y riesgos, sin exportar secretos ni datos personales.

30.24. Procedimiento seguro para cambiar una regla



Figura 30.3. Flujo recomendado para registrar, aplicar y validar modificaciones del firewall.

01. Formalizar la necesidad, el solicitante responsable, el alcance exacto y un criterio de aceptación.
02. Hacer copia de seguridad mediante Diagnostics → Backup & Restore y asegurar acceso administrativo alternativo.
03. Localizar la interfaz por la que entra el tráfico; buscar reglas Floating o de grupos que puedan prevalecer.
04. Preferir la regla más específica posible, utilizando descripciones y alias comprensibles.
05. Programar una ventana de intervención si puede afectar a servicios de producción o sesiones existentes.
06. Guardar y aplicar los cambios. Probar tanto los flujos autorizados como los que deben seguir bloqueados.
07. Consultar el registro, los estados y las rutas/NAT si el resultado no coincide con lo previsto.
08. Registrar evidencia, hora de implantación y procedimiento de reversión; restaurar si hay impacto no aceptado.

30.25. Diagnóstico: cómo distinguir bloqueo, ruta y traducción

Síntoma	Comprobación inicial	Causa probable que investigar
Conexión denegada de inmediato	Firewall log y reglas de la interfaz de entrada.	Regla Block/Reject o coincidencia más prioritaria.
Sin entrada en registro	Regla sin logging, estados, interfaz real, captura.	Tráfico en otra interfaz o filtrado sin registro.
Se permite, pero no hay servicio	Rutas, NAT, DNS, firewall del destino.	Retorno ausente, puerto incorrecto o servicio caído.
Cambio de bloqueo no corta sesión	Tabla de estados de la conexión.	Estado previo que sigue vigente.
Horario no tiene el efecto previsto	Reglas posteriores y vigencia del Schedule.	Regla posterior permite el tráfico.
IPv4 funciona, IPv6 falla	Reglas IPv6, rutas y conectividad de extremo.	Política o servicio IPv6 no configurado.

Síntoma	Comprobación inicial	Causa probable que investigar
Shaper reduce demasiado el caudal	Medición, cola/limiter, compatibilidad ALTQ.	Parámetros de QoS no ajustados al enlace.

30.26. Comprobaciones y evidencias de funcionamiento

Para contrastar un cambio, comenzar por Status → System Logs → Firewall, filtrando por interfaz, acción, origen/destino o protocolo según la necesidad. El registro representa reglas que generan eventos; una ausencia de líneas no certifica que no exista tráfico. Revisar también estados activos, contadores por regla, tablas de alias y, cuando proceda, capturas de paquetes y monitorización del gateway.

Conviene conservar un registro técnico de pruebas con fecha, tipo de prueba, resultado esperado, resultado observado, decisión y responsable funcional. Los registros completos, capturas y direcciones operativas deben mantenerse en repositorios protegidos; no se incluirán en materiales de publicación o formación.

30.27. Errores recurrentes y cómo prevenirlos

Los fallos más repetidos se originan al aplicar una regla en la interfaz incorrecta, ignorar otra regla precedente, confundir NAT con permisos, dejar permisos All/Any innecesarios, omitir IPv6, confiar en la ausencia de logs, pasar por alto un estado activo o elegir prioridades QoS no compatibles con el hardware. La mitigación principal es una metodología de cambio y pruebas de extremo a extremo, no la acumulación de reglas ad hoc.

30.28. Recomendaciones de seguridad y administración

Adoptar mínimo privilegio, descripciones uniformes y una convención de alias estable. Limitar el acceso administrativo a zonas y orígenes de confianza, revisar reglas de publicación periódicamente y conservar copias verificables. Documentar quién aprueba cambios, cuándo se aplican y qué dependencia tienen respecto a VPN, NAT, gateways o certificados. La activación de exportadores de flujo requiere especial atención a privacidad, origen/destino de la telemetría y retención.

Auditar las reglas amplias después de cada cambio sustancial, retirar excepciones caducadas y vigilar indicadores como estados, bloqueos inesperados y saturación. La documentación de reglas debe explicar por qué existen y bajo qué condiciones pueden retirarse; una regla funcional sin justificación también representa riesgo.

Riesgo de acceso remoto. Antes de bloquear, mover o reordenar reglas que alcanzan la administración del firewall, confirmar acceso por consola o una ruta de gestión alternativa. Una equivocación puede impedir la corrección desde la propia interfaz web.

30.29. Lista de aceptación para una política de firewall

Control	Evidencia mínima
Inventario	Zonas, flujos y servicios justificados.
Alcance	Interfaz de entrada, dirección, protocolo, origen/destino y horario.
Conflictos	Reglas Floating, grupos, reglas automáticas y orden revisados.
NAT / rutas	Traducciones y caminos de ida/retorno verificados.
Estados	Efecto sobre sesiones existentes y nuevas comprobado.
IPv6	Política coherente con la conectividad IPv6 habilitada.
Telemetría	Logs, tablas, estados y, si procede, exportación IPFIX verificables.
Reversión	Copia disponible y procedimiento de vuelta comprobado.
Registro del cambio	Resultado, fecha, aprobación y observaciones guardados.

30.30. Glosario operativo

Concepto	Definición breve
PF	Motor de filtrado de paquetes en el que se apoya pfSense.
State / estado	Registro de una comunicación que permite relacionar paquetes sucesivos.
Ruleset	Conjunto efectivo de reglas, incluidas las internas y de usuario.
NAT	Traducción de direcciones y, según modalidad, puertos.
Alias	Conjunto reutilizable de redes, hosts o puertos.
VIP	Dirección adicional administrada o anunciada por pfSense.
IPFIX / NetFlow	Formatos para exportar metadatos agregados de comunicaciones.
QoS / shaper	Mecanismos para gestionar prioridades, colas y límites.

30.31. Ficha neutra para revisar una nueva solicitud de acceso

La siguiente matriz permite transformar una petición genérica de conectividad en una decisión auditable antes de tocar Rules o NAT. No contiene direcciones, nombres propios ni parámetros de ninguna instalación. Cada casilla debe completarse únicamente en el registro interno de cambios y no en versiones destinadas a publicación.

Dato a confirmar	Criterio de revisión
Necesidad de negocio	Identificar el proceso y la justificación para abrir una comunicación.
Iniciador	Determinar quién empieza realmente la conexión.
Zona de origen	Comprobar la interfaz por la que el tráfico entra al firewall.
Zona de destino	Acreditar que el destino previsto está dentro del alcance aprobado.
Protocolo y servicio	Reducir a puertos y protocolos indispensables.
Horario y caducidad	Definir vigencia temporal, si aplica, y fecha de revisión.
NAT y direccionamiento	Aclarar si hay redirección, salida traducida o dirección virtual.
Impacto en otras reglas	Comprobar reglas Floating, grupos y reglas precedentes.
Prueba negativa	Demostrar también que conexiones fuera de alcance siguen bloqueadas.
Reversión	Confirmar copia, responsable y secuencia de recuperación.

La aprobación técnica se completa cuando se conocen el impacto, la ventana de aplicación y el resultado observable. Si no se dispone de acceso alternativo para un cambio que puede bloquear la gestión, el riesgo debe resolverse antes de aplicar la modificación.

30.32. Referencias técnicas oficiales de Netgate

Guía de menú Firewall | https://docs.netgate.com/pfsense/en/latest/menuguide/firewall.html

Fundamentos del firewall y estados | https://docs.netgate.com/pfsense/en/latest/firewall/fundamentals.html

Buenas prácticas y denegación por defecto | https://docs.netgate.com/pfsense/en/latest/firewall/best-practices.html

Orden entre NAT y filtrado | https://docs.netgate.com/pfsense/en/latest/nat/process-order.html

Aliases | https://docs.netgate.com/pfsense/en/latest/firewall/aliases.html

Network Address Translation | https://docs.netgate.com/pfsense/en/latest/nat/index.html

Packet Flow Data en pfSense Plus | https://docs.netgate.com/pfsense/en/latest/firewall/pflow.html

Reglas con horario | https://docs.netgate.com/pfsense/en/latest/firewall/time-based-rules.html

Traffic Shaper | https://docs.netgate.com/pfsense/en/latest/trafficshaper/index.html

Virtual IP Addresses | https://docs.netgate.com/pfsense/en/latest/firewall/virtual-ip-addresses.html

Registro del firewall | https://docs.netgate.com/pfsense/en/latest/monitoring/logs/firewall.html

Solución de problemas de reglas | https://docs.netgate.com/pfsense/en/latest/troubleshooting/firewall.html

Las rutas de navegación y las descripciones funcionales siguen la terminología de pfSense Plus y se apoyan en estas referencias oficiales. Algunas prestaciones, especialmente Packet Flow Data, requieren versiones específicas; la disponibilidad concreta depende de la versión instalada y de la plataforma.

31 Firewall → Aliases

IP · Ports · URLs · All | Definición, reutilización y verificación de objetos

Ruta de acceso: Firewall → Aliases. Este capítulo describe las cuatro pestañas de consulta y los formularios de creación, importación y edición documentados por Netgate. El ejemplo visual de partida corresponde a la vista IP sin entradas de usuario visibles; los detalles de las demás vistas y de sus formularios se fundamentan en la documentación oficial. Los ejemplos emplean exclusivamente nombres neutros y direcciones reservadas para documentación.



Figura 31.1. Organización funcional del apartado Aliases en pfSense Plus.

31.1. Propósito de los alias: reutilizar criterios sin multiplicar reglas

Un alias es un objeto con nombre que reúne direcciones IP, nombres FQDN, redes, puertos o fuentes de listas. Las reglas de firewall, las traducciones NAT y otras funciones compatibles pueden hacer referencia a ese nombre en vez de contener una lista extensa de elementos. El alias sirve para identificar destinos, orígenes o servicios: no realiza por sí solo una acción de permitir, bloquear o traducir tráfico.

Su ventaja operativa principal es la consistencia. Si varios controles utilizan el mismo conjunto de direcciones, mantenerlo en un único lugar evita divergencias y reduce la complejidad visible del conjunto de reglas. La contrapartida es que una modificación afecta simultáneamente a todas las reglas y subsistemas que lo utilizan; por eso deben documentarse las dependencias antes de editarlo.

Diferencia esencial. Firewall → Aliases administra conjuntos referenciables. Firewall → Virtual IPs administra direcciones IP adicionales del propio firewall. Un alias con una dirección no la asigna a ninguna interfaz ni hace que el firewall responda por ella.

31.2. Las cuatro pestañas y el alcance de cada una

Pestaña	Tipos principales	Qué permite examinar
IP	Host, Network	Alias de hosts, IP individuales, rangos y subredes.
Ports	Port	Puertos numéricos y rangos, independientemente del protocolo elegido en la regla.
URLs	URL (IPs/Ports), URL Table (IPs/Ports)	Datos importados desde una fuente remota o tablas descargadas periódicamente.
All	Todos y System Aliases	Vista consolidada y alias internos disponibles según funciones y versión.

Las pestañas son filtros de presentación. Un alias se clasifica en su ubicación correspondiente en función de su tipo, incluso si se inició la creación desde otra pestaña. La vista All es útil para inventariar tipos mezclados y para localizar los alias integrados que pfSense expone al administrador.

31.3. Lectura detallada de la tabla de resultados

Elemento visible	Interpretación	Acción o precaución
Name	Nombre técnico del objeto.	Debe ser único y no coincidir con nombres reservados.
Type	Clase de alias y sintaxis admisible.	Determina campos compatibles en reglas y NAT.
Values	Valores o fuentes definidos.	Una tabla descargada puede requerir consultar su contenido efectivo.
Description	Propósito administrativo del objeto.	Debe explicar función, no copiar secretos o topologías.
Actions	Controles de gestión por fila.	Editar o eliminar solo tras comprobar las dependencias.
Add (+)	Abre la creación de un alias.	Seleccionar tipo antes de introducir entradas.
Import	Importación masiva de alias admitidos.	Validar líneas y datos antes de guardar.
Icono de información / ayuda	Acceso contextual a explicación o ayuda.	No modifica el filtrado por sí mismo.

Una tabla IP sin entradas indica que no hay alias de usuario listados en esa pestaña. No permite deducir el contenido de Ports, URLs o All, ni que el firewall carezca de reglas, objetos internos o tablas generadas automáticamente.

31.4. Alta de alias: campos comunes del formulario

Campo	Descripción y comportamiento	Criterio recomendado
Name	Identificador compuesto por letras, números y guion bajo (_). No admite espacios ni colisiones con nombres reservados.	Nombre estable, sin datos sensibles.
Description	Texto explicativo de la finalidad del objeto.	Describir servicio, propietario funcional y uso.
Type	Determina Host, Network, Port, URL o URL Table y variantes IP/Ports.	Elegir el tipo más específico adecuado.
Entries	Lista de datos y sus descripciones por elemento. Cambia según el tipo.	Un elemento lógico por fila y comentarios claros.
Add / Delete en entries	Agrega o retira una fila en el editor.	Revisar duplicidades y referencias.
Save	Almacena la definición tras validarla.	Comprobar cambios efectivos en reglas y tablas.

En pfSense Plus, el editor rechaza nombres incompatibles con identificadores de interfaces, pasarelas o palabras internas de PF. La apariencia de algunos campos, iconos o botones puede variar entre versiones; comprobar los requisitos del editor instalado.

31.5. Pestaña IP: alcance de Host y Network

La pestaña IP concentra dos tipos fundamentales. Host representa destinos individuales, direcciones FQDN o conjuntos que se expanden en direcciones concretas. Network conserva prefijos CIDR y conjuntos de redes. Ambos pueden incluir nombres FQDN cuando sus entradas se resuelven correctamente; la elección afecta a cómo se expresan o expanden rangos y a la interpretación de las máscaras.

Tipo	Entradas aceptadas	Cuándo elegirlo
Host	IP individual, FQDN; rangos IPv4 o pequeñas subredes que el sistema expande a hosts.	Conjunto reducido de equipos o extremos específicos.
Network	Prefijo IPv4/IPv6, IP individual, FQDN o rango IPv4 convertido en CIDR.	Segmentos, subredes o colecciones de redes.

31.6. Alias Host: direcciones, nombres y rangos

Una entrada Host puede contener una dirección individual, como 192.0.2.10, o un nombre completo de dominio, como equipo.example.com; ambos son valores reservados para documentación. Cuando se introduce un rango IPv4 o una subred pequeña, pfSense lo transforma al guardar en direcciones individuales. Esta conversión puede aumentar de forma notable el tamaño del alias y su consumo de entradas de tabla.

Conviene emplear Host cuando la pertenencia tiene significado por dispositivo o servicio. No debe utilizarse para expresar grandes bloques sin estimar su expansión. Si el FQDN cambia de IP mediante DNS, el motor volverá a consultar sus registros a intervalos; no equivale a usar un mecanismo de filtrado web por nombre de dominio.

31.7. Alias Network: prefijos, máscaras y familias IP

Network conserva las direcciones como redes expresadas con longitud de prefijo: por ejemplo, 192.0.2.0/24 (bloque reservado para documentación) o 2001:db8:100::/64 (prefijo IPv6 documental). Para un host único se pueden utilizar /32 en IPv4 o /128 en IPv6. Una entrada FQDN requiere formalmente un prefijo de host, pero la máscara escrita no recorta las direcciones que devuelve DNS.

Un intervalo IPv4 puede convertirse internamente en el conjunto mínimo de subredes CIDR que cubren exactamente ese rango. En listas de redes mixtas, el motor utilizará la familia de direcciones que corresponda al tipo de regla; conviene comprobar explícitamente IPv4 e IPv6 para evitar permisos involuntarios.

31.8. Resolución de nombres FQDN: utilidad y límites

Los nombres de host se resuelven mediante consultas DNS A y AAAA realizadas por el firewall. Si la respuesta contiene varias direcciones, todas las retornadas en esa consulta pueden pasar a integrar el alias. Según Netgate, el intervalo predeterminado de reevaluación es de 300 segundos y se puede ajustar en System → Advanced → Firewall & NAT, opción Aliases Hostnames Resolve Interval.

No hay interpretación de comodines como *.example.com ni filtrado basado en la URL visitada, rutas HTTPS, registros SRV o coincidencias textuales de páginas. En servicios distribuidos por CDN, las direcciones que ve el firewall pueden diferir de las resueltas por los clientes; por ese motivo no debe utilizarse como mecanismo fiable de autorización o bloqueo de grandes servicios web basados solo en nombres.

Diagnóstico DNS. La existencia de un FQDN en la configuración no garantiza que haya IP operativas en la tabla. Comprobar la resolución del propio firewall y la tabla efectiva en Diagnostics → Tables.

31.9. Crear un alias IP de forma controlada

01. Acceder a Firewall → Aliases → IP y pulsar Add.
02. Asignar un Name sin espacios, por ejemplo EQUIPOS_MANTENIMIENTO (nombre ficticio).
03. Elegir Host si se agrupan extremos o Network si se agrupan prefijos; escribir una Description útil.
04. Introducir únicamente las direcciones, redes o FQDN autorizados, con una descripción por elemento cuando resulte pertinente.
05. Revisar el número de entradas, la familia IPv4/IPv6 y la posibilidad de expansión por rangos.
06. Guardar, confirmar el objeto en la pestaña IP y localizar sus referencias antes de habilitar cualquier regla nueva.
07. Aplicar la regla o uso que corresponda y probar desde un origen autorizado y otro no autorizado.

31.10. Pestaña Ports: grupos de puertos de transporte

Los alias Port almacenan números de puerto o intervalos inclusivos. El número individual debe encontrarse entre 1 y 65535; un rango se expresa con dos números separados por dos puntos, por ejemplo 8000:8010. El alias no representa por sí solo un protocolo: el protocolo TCP, UDP o SCTP se define en la regla que lo utiliza.

Esta separación permite reutilizar nombres técnicos en reglas distintas, siempre que el servicio realmente use esos puertos. También implica que un alias denominado “servicios_web” no filtra HTTP ni interpreta el contenido de las conexiones: solo identifica coincidencias numéricas dentro del protocolo y dirección configurados en la regla.

Valor de ejemplo	Interpretación	Matiz operativo
443	Solo el puerto numérico 443.	No autoriza automáticamente HTTPS; hace falta regla.
5000:5010	Intervalo que incluye ambos extremos.	Comprobar necesidades reales del servicio.

31.11. Crear, utilizar y comprobar un alias Ports

01. Entrar en Firewall → Aliases → Ports y seleccionar Add.
02. Asignar un nombre estable, por ejemplo PUERTOS_APLICACION, y una descripción basada en el servicio.
03. Escoger Type: Port; incorporar los números o rangos pertinentes, respetando el formato con dos puntos.
04. Guardar y comprobar la aparición en la tabla de Ports.
05. En una regla compatible de Firewall → Rules, seleccionar un protocolo explícito y referenciar el alias en Source Port o Destination Port según el flujo.
06. Probar el puerto permitido y al menos uno fuera del conjunto; revisar registros y estados si el resultado no coincide.

31.12. Pestaña URLs: importar fuentes externas de datos

La pestaña URLs no implementa un proxy ni un filtro de páginas web. Sus alias leen archivos de texto accesibles mediante URL que enumeran direcciones, prefijos, FQDN o puertos. El comportamiento tiene dos modelos diferentes: URL (IPs/Ports), que importa valores al crear el alias, y URL Table (IPs/Ports), que mantiene una tabla persistente cuya fuente se vuelve a consultar periódicamente.

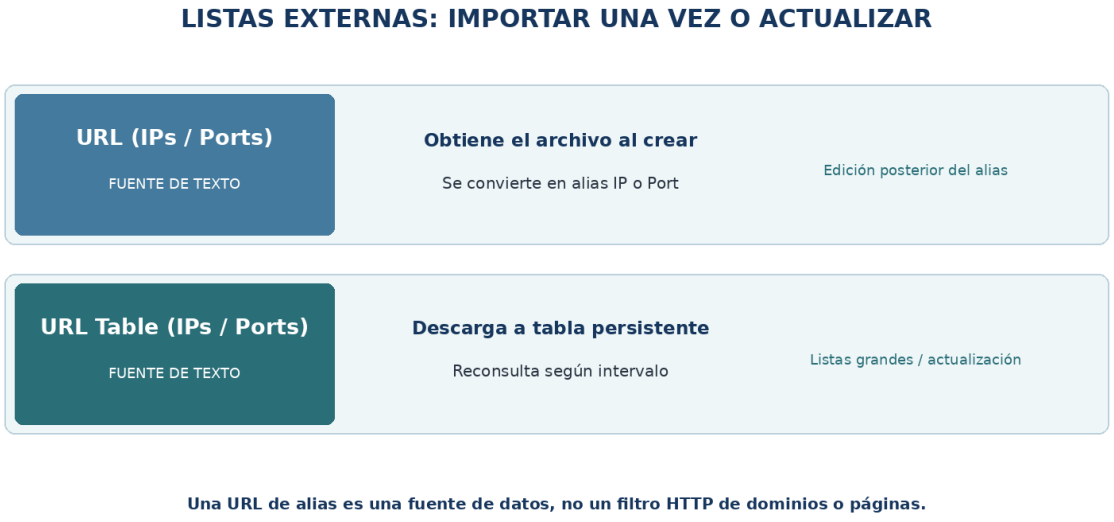


Figura 31.3. Comparación del ciclo de vida entre URL y URL Table.

31.13. URL (IPs) y URL (Ports): importación puntual

En URL (IPs), el recurso debe devolver líneas de direcciones IP, prefijos CIDR o FQDN; la GUI incorpora el resultado como un alias de tipo Network. En URL (Ports), la fuente contiene números o intervalos de puertos y se transforma en un alias de tipo Port. Netgate documenta un límite de 3.000 entradas leídas por cada URL al crear uno de estos alias.

La modificación posterior del fichero remoto no implica una actualización periódica de un alias URL convencional. Para datos sujetos a cambios frecuentes conviene utilizar la variante URL Table, en lugar de suponer que el alias normal se sincroniza en tiempo real.

31.14. URL Table (IPs) y URL Table (Ports): tablas persistentes

URL Table almacena una o más direcciones de descarga, transforma los resultados en una tabla PF persistente y permite fijar un intervalo en días para volver a obtener los contenidos. La GUI comprueba diariamente qué tablas necesitan actualizarse; el número de días configurado determina cuándo corresponde la siguiente descarga. El contenido completo no se edita de forma ordinaria fila a fila desde el mismo editor.

Estas tablas resultan adecuadas para colecciones voluminosas y listas administradas centralmente. No deben tratarse como una fuente de confianza automática: una lista de terceros puede ser errónea, incompleta, excesiva o manipulada. Verificar origen, formato, integridad de transporte y consecuencias de retirar o añadir elementos antes de incorporarla a una regla crítica.

31.15. Comparativa completa de tipos URL

Tipo documentado	Contenido esperado	Actualización	Uso aconsejado
URL (IPs)	IP, CIDR, FQDN en texto plano.	Importación inicial.	Lista acotada y estable.
URL (Ports)	Números y rangos de puerto.	Importación inicial.	Servicios con listado poco variable.
URL Table (IPs)	IP, CIDR, FQDN en texto plano.	Reconsulta según intervalo en días.	Listas amplias mantenidas externamente.
URL Table (Ports)	Números y rangos de puerto.	Reconsulta según intervalo en días.	Inventarios de puertos centralizados.

31.16. Formato de las listas y validación del origen

Los contenidos han de consistir en valores admitidos por el tipo elegido, presentados como una lista de texto plano. No se debe introducir una página HTML esperando que el firewall extraiga direcciones de su contenido, ni copiar vínculos de servicios que requieren formularios web, autenticación interactiva o scripts en el navegador. Es imprescindible comprobar que la URL responde desde el propio firewall y que el contenido tiene la estructura prevista.

Si se utiliza HTTPS, se recomienda mantener habilitada la verificación de certificados para las descargas. Netgate describe la opción “Verify HTTPS certificates when downloading alias URLs” en System → Advanced → Firewall & NAT; desactivarla debilita la autenticidad de la fuente y debe evitarse salvo una excepción debidamente evaluada.

Riesgo de dependencia externa. Una lista remota utilizada para permitir accesos puede ampliar el perímetro si el origen se modifica indebidamente. Una lista de bloqueo puede producir interrupciones masivas por falsos positivos. Aplicar control de cambios, supervisión y un plan de reversión.

31.17. Procedimiento: crear un alias URL Table

01. Preparar una fuente de texto plano bajo control administrativo, con contenido revisado, sin datos identificativos en documentación pública.
02. Comprobar desde el firewall la resolución DNS, acceso HTTPS y certificado de la fuente.
03. Acceder a Firewall → Aliases → URLs y pulsar Add.
04. Elegir URL Table (IPs) o URL Table (Ports) de acuerdo con el contenido real.

05. Completar Name, Description y la URL; configurar el intervalo de actualización en días de acuerdo con la criticidad y la frecuencia de cambios.
06. Guardar y verificar que el alias aparece en URLs y All; revisar la tabla si ya está cargada.
07. Referenciar el alias en una regla de prueba de alcance limitado y verificar decisiones observadas, nunca solo el nombre visible.
08. Documentar la persona o equipo que controla la fuente, periodicidad y procedimiento de bloqueo/reversión si deja de ser confiable.

31.18. Pestaña All: inventario global y objetos de sistema

All reúne los alias de distintas categorías y expone los Built-In System Aliases en su sección específica. Es la vista idónea para identificar nombres, distinguir tipos y detectar dependencias administrativas. No significa que todos los objetos internos sean editables como un alias creado por un administrador: algunos son generados y mantenidos por el sistema o por funciones habilitadas.

Las familias internas pueden tener variantes IPv4, IPv6 y duales, diferenciadas por sufijos 4, 6 o 46. La disponibilidad exacta depende de la versión y de las funcionalidades instaladas; comprobar qué denominaciones admite el sistema administrado.

Ejemplo de alias del sistema	Finalidad documentada
bogons	Redes consideradas bogon.
sshguard	Fuentes bloqueadas por protección frente a intentos repetidos de acceso.
snort2c	Direcciones bloqueadas por componentes IDS/IPS.

Otros alias internos documentados

Según las funciones habilitadas pueden aparecer vpn_networks (redes de determinadas VPN, sin garantizar rutas dinámicas), negate_networks (excepciones al policy routing), tonatsubnets (redes consideradas para NAT de salida) y conjuntos _private4_, _private6_ o _private46_ (direcciones privadas por familia). Estas denominaciones son ejemplos oficiales, no un inventario de ninguna instalación concreta.

31.19. Búsqueda, ordenación y dependencias al auditar All

El análisis debe centrarse primero en qué alias están presentes y después en dónde se usan. Dos alias pueden contener valores parecidos, pero uno ser manual y otro generado. Un mismo nombre dentro de una regla puede influir en múltiples VLAN, WAN o rutas de salida. Por tanto, cualquier sustitución o eliminación debe ir acompañada de una búsqueda de referencias funcionales y de un plan de pruebas.

La documentación oficial indica que el sistema expone alias útiles de forma interna; sus nombres concretos o su aparición pueden variar. La vista All facilita la localización, pero no sustituye la inspección de las tablas PF que materializan efectivamente el conjunto de IP.

31.20. Import: incorporación masiva de Host, Network y Port

La opción Import permite cargar muchas entradas desde un bloque de texto: para Host o Network se entra desde IP; para Port, desde Ports. Cada entrada se escribe en una línea. Netgate documenta que el texto posterior a un valor válido puede interpretarse como descripción de la entrada. Import crea un alias convencional, editable después; no una tabla URL Table dinámica.

01. Preparar una lista revisada y eliminar duplicados, líneas superfluas o valores que no correspondan al tipo.
02. Abrir IP o Ports según el contenido y pulsar Import.
03. Indicar Alias Name y Description con una finalidad inequívoca.
04. Pegar las entradas en Aliases to import, una por línea; incluir descripciones solo cuando el formato sea inequívoco.
05. Guardar y abrir el alias resultante para revisar entradas, rangos, máscaras y conversiones automáticas.
06. Consultar las referencias y probar el uso en una regla antes de introducir el objeto en una política de producción.

31.21. Convención de nombres y mantenimiento documental

Conviene aplicar una nomenclatura simple basada en el tipo y la función: HOSTS_*, REDES_*, PUERTOS_*, URLTAB_*. La denominación debe ser suficientemente precisa para evitar confusiones entre listas de bloqueo y listas de autorización, sin contener dominios internos o nombres sensibles en una publicación. Al cambiar el alcance, actualizar la descripción y el inventario de dependencias.

La documentación de Netgate restringe Name a caracteres alfanuméricos y guion bajo; también existen nombres reservados. Los alias pueden anidarse cuando pertenecen a tipos compatibles. No se pueden mezclar directamente conjuntos de IP con conjuntos de puertos dentro de un mismo objeto.

31.22. Alias anidados: compatibilidad y límites

Los alias Host y Network son compatibles para anidamiento y permiten componer conjuntos organizativos. También pueden anidarse alias URL con otros URL y URL Table con otros URL Table, dentro de las reglas de compatibilidad descritas por Netgate. La anidación simplifica catálogos amplios, pero dificulta entender a simple vista qué direcciones resultan finalmente incluidas.

Evitar capas innecesarias de anidación y documentar la jerarquía, especialmente cuando un alias de nivel superior se referencia en reglas de administración. Una modificación en un miembro inferior cambia el conjunto lógico de todos sus consumidores; verificar el resultado en tabla y mediante tráfico real.

31.23. Límites de tamaño y capacidad del firewall

Cada alias creado manualmente tiene un límite documentado de 5.000 miembros. Además, algunos navegadores presentan problemas prácticos al editar objetos con alrededor de 3.000 entradas. Para listas mayores debe estudiarse URL Table, con un dimensionamiento adecuado y una fuente externa gobernada.

Las tablas de PF consumen capacidad. Netgate indica que el total de alias y tablas debe caber aproximadamente en la mitad de Firewall Maximum Table Entries, cuyo valor predeterminado es 400.000; esto no equivale a prometer 200.000 entradas de usuario, porque también existen tablas internas y estructuras activas. Antes de ampliar límites, revisar RAM, carga y el comportamiento real del equipo.

31.24. Aplicación práctica en Firewall → Rules

En los campos compatibles, el autocompletado puede sugerir un alias al introducir sus primeras letras. El sistema filtra la propuesta por tipo: en dirección de origen o destino aparecen Host/Network; en un campo de puerto, Port. Es posible que determinadas pantallas permitan escribir el nombre completo sin usar la sugerencia.

Ejemplo conceptual: una regla en una interfaz interna puede permitir TCP desde el grupo HOSTS_ADMIN a los destinos SERVIDORES_APLICACION usando el grupo PUERTOS_APP. Los nombres son ilustrativos y no describen ninguna red real. El efecto concreto depende de la interfaz de ingreso, protocolo, acción y demás reglas que se evalúan antes.



Figura 31.2. Flujo lógico desde entradas definidas hasta tablas PF y políticas que las referencian.

31.25. Usos en NAT, VPN y otras pantallas compatibles

Además de Firewall → Rules, Netgate documenta alias reutilizables en port forwards, reglas de NAT de salida, determinados campos de VPN, rutas estáticas y otras opciones que aceptan estos objetos. No hay que asumir que todos los campos admiten todos los tipos: la interfaz de edición determina las clases válidas y el autocompletado puede mostrar solo las compatibles.

La inclusión de una IP en un alias no abre una publicación NAT, ni modifica automáticamente rutas o DNS. Cada tecnología conserva sus propias condiciones de funcionamiento. La política de firewall, las traducciones y la conectividad se comprueban por separado.

31.26. Diagnóstico: Diagnostics → Tables

Un alias de direcciones se materializa en una tabla del motor PF cuando se carga en el conjunto de reglas. Para revisar los miembros reales, acceder a Diagnostics → Tables y escoger la tabla correspondiente. Este paso es especialmente importante con FQDN o URL Table: el contenido en ejecución puede cambiar respecto a lo que un administrador escribió originalmente.

El control para retirar una entrada de una tabla desde Diagnostics es una herramienta de diagnóstico, no el método definitivo de editar alias manuales. Netgate advierte que las tablas pueden repoblarse cuando se recarga el filtrado. Para cambios persistentes, modificar el alias de origen o la fuente autorizada.

31.27. Escenario empresarial A: centralizar un conjunto autorizado

Una organización permite a determinados puestos acceder a una aplicación en una red separada. Los miembros se agrupan en un alias Host y el servicio se representa con un alias Port. La regla de entrada de la zona de origen utiliza ambos objetos y documenta la necesidad. La modificación de uno de los miembros se realiza en el alias y requiere comprobar que no afecta a otras reglas que consumen el mismo objeto.

01. Inventariar el conjunto autorizado sin registrar datos reales en materiales externos.
02. Definir alias separados para orígenes y puertos, y describir su uso.
03. Revisar si alguna otra regla ya utiliza esos alias.
04. Crear una regla restrictiva en la interfaz de entrada con acción, familia IP y protocolo adecuados.
05. Probar un miembro autorizado y un equipo no incluido; contrastar logs y estados.
06. Documentar propietario funcional, aprobador y condiciones de revisión.

31.28. Escenario empresarial B: lista externa de redes

Un servicio interno mantiene una lista de redes técnicas permitidas en un fichero de texto validado. Si la lista cambia periódicamente, URL Table (IPs) reduce la necesidad de edición manual. Sin embargo, la dependencia del repositorio, la conectividad HTTPS y la actualización de la tabla deben monitorizarse, y el diseño debe prever qué hacer cuando no es posible renovar o validar la lista.

No debe considerarse la lista por sí sola una solución de autenticación de identidad: una dirección IP puede ser compartida, dinámica o suplantable en determinados contextos. La regla necesita controles complementarios apropiados al riesgo y al tipo de acceso.

31.29. Escenario empresarial C: inventario de servicios

Una aplicación utiliza varios puertos de transporte definidos por su fabricante. Se documentan en un alias Port y se aplican únicamente a reglas cuyo protocolo y destino correspondan. Al migrar la aplicación, se revisa la definición y se comprueba el alcance de todas sus referencias, en lugar de mantener puertos obsoletos dispersos en docenas de reglas.

31.30. Comprobaciones recomendadas tras crear o editar

Verificación	Qué comprobar	Herramienta o evidencia
Definición	Nombre, tipo, cantidad de entradas y descripciones.	Firewall → Aliases y editor.
FQDN	Resolución A/AAAA y direcciones reales cargadas.	Diagnostics → DNS Lookup / Tables.

Verificación	Qué comprobar	Herramienta o evidencia
Listas URL	Acceso, autenticidad HTTPS, formato y actualización.	Fuente gestionada y Diagnostics → Tables.
Reglas	Interfaces, familias IP, protocolo y precedencia.	Firewall → Rules y logs.
Conectividad	Tráfico previsto permitido; tráfico no previsto bloqueado.	Pruebas de extremo a extremo.
Capacidad	Tamaño, límite de tabla y recursos del equipo.	System → Advanced y monitorización.

31.31. Problemas recurrentes y vías de solución

Síntoma	Causa que investigar	Actuación inicial
Alias no aparece al escribir	Tipo no compatible con ese campo.	Comprobar Host/Network frente a Port.
FQDN no produce coincidencias	DNS del firewall falla o tiene resultados diferentes.	Ver registros A/AAAA y Diagnostics → Tables.
Un URL Table deja de actualizarse	Fuente inaccesible, TLS, formato o periodicidad.	Verificar origen y programación de descarga.
Una lista bloquea demasiado	Valor erróneo o lista remota alterada.	Revisar fuente y revertir el cambio.
Importación rechazada	Sintaxis, entradas incorrectas o colisión de nombre.	Revisar líneas y nombre único.
El cambio no altera sesión activa	Estado previo del firewall.	Revisar tabla de estados antes de interrumpir.
Límite alcanzado	Número de entradas o tabla PF insuficiente.	Replantear tamaño, anidación y límites.

31.32. Riesgos de seguridad y control de cambios

Los alias que se utilizan para permitir acceso a la administración, publicación de servicios, túneles VPN o salida hacia Internet deben tratarse como elementos críticos. Un cambio en un alias compartido puede ampliar o reducir permisos en lugares aparentemente no relacionados. Además, los objetos descargados externamente añaden una dependencia de integridad, disponibilidad y confianza en el proveedor de la lista.

Advertencia de producción. Antes de editar o eliminar un alias usado en reglas, NAT o accesos de administración, realizar copia de seguridad, localizar referencias, conservar un acceso alternativo y definir un criterio verificable de reversión. El resultado del cambio puede afectar a conexiones y servicios.

01. Solicitar y documentar el cambio: motivo, impacto, alcance, aprobador y momento previsto.
02. Identificar consumidores: reglas, NAT y otros subsistemas compatibles; analizar las relaciones anidadas.
03. Exportar o respaldar la configuración del firewall por un canal administrativo protegido.
04. Editar el objeto procurando el cambio mínimo, sin introducir destinos o puertos innecesarios.
05. Guardar y aplicar los cambios según la interfaz; comprobar tablas, logs y pruebas funcionales.
06. Revisar el comportamiento de sesiones existentes y revertir si existe impacto no aceptado.
07. Registrar resultado, evidencia no sensible y responsables de futuras revisiones.

31.33. Buenas prácticas de diseño y administración

Crear alias cuando agrupan objetos con una finalidad estable y compartida, no por cada dirección aislada sin posibilidad de reutilización. Darles nombres claros, descripciones precisas y un propietario técnico. Evitar listas excesivas en Host cuando Network o URL Table sean mejores; separar puertos de direcciones y distinguir expresamente autorización de bloqueo.

Revisar periódicamente objetos sin uso, anidaciones, listas de terceros, FQDN sobre servicios CDN, direcciones que han quedado obsoletas y permisos temporales. Para controles dual-stack, contrastar tanto IPv4 como IPv6. Las políticas de mínimo privilegio, el tratamiento de estados y la inspección de tablas son más importantes que acumular alias.

31.34. Glosario de referencia

Término	Definición
Alias	Conjunto nombrado y reutilizable dentro de campos compatibles.
Host	Tipo con direcciones individuales y FQDN, con posible expansión de rangos.
Network	Tipo con prefijos CIDR, direcciones y nombres.
Port	Conjunto numérico de puertos o intervalos.
FQDN	Nombre de dominio completo, resuelto por DNS A/AAAA.
URL Table	Tabla PF alimentada por listas de texto descargadas periódicamente.
PF table	Estructura de coincidencia de direcciones mantenida por Packet Filter.
CIDR	Notación de red definida por dirección y longitud de prefijo.
Built-In System Alias	Alias que pfSense incluye o genera para funciones internas.

31.35. Referencias y documentación oficial de Netgate

Las referencias siguientes documentan funciones de pfSense y pfSense Plus. Algunas opciones, alias internos o presentaciones de botones pueden variar con la versión exacta o los paquetes habilitados. Las fuentes se consultaron para este capítulo el 17 de noviembre de 2026.

Aliases: organización en las cuatro pestañas — https://docs.netgate.com/pfsense/en/latest/firewall/aliases.html

Alias Types: Host, Network, Port, URL y URL Table — https://docs.netgate.com/pfsense/en/latest/firewall/aliases-types.html

Alias Configuration: campos, creación e Import — https://docs.netgate.com/pfsense/en/latest/firewall/aliases-config.html

Alias Features and Limitations: DNS, anidación, tamaño — https://docs.netgate.com/pfsense/en/latest/firewall/aliases-features.html

Alias Usage: autocompletado y uso en reglas — https://docs.netgate.com/pfsense/en/latest/firewall/aliases-usage.html

Diagnostics → Tables: contenido efectivo de tablas PF — https://docs.netgate.com/pfsense/en/latest/monitoring/status/firewall-tables.html

System → Advanced → Firewall & NAT: intervalos y certificados — https://docs.netgate.com/pfsense/en/latest/config/advanced-firewall-nat.html

31.36. Ficha práctica de validación de un alias

Control	Resultado esperado / evidencia no sensible
Objetivo y tipo	La finalidad y clase de alias están justificadas.
Origen de datos	Miembros verificados o URL con procedencia confiable.
Integridad	Formato válido; certificado y transporte comprobados.
Dependencias	Inventario de reglas, NAT y anidaciones revisado.
Efecto en política	Solo coincide el conjunto previsto; no amplía permisos.
Comprobación	Pruebas positivas y negativas superadas.
Retirada y reversión	Método probado/documentado antes de la puesta en producción.
Mantenimiento	Responsable y revisión programada según el riesgo.

Criterio de aceptación: el objeto debe identificar únicamente los miembros previstos, su conjunto efectivo debe ser verificable y los consumidores no deben autorizar servicios adicionales de forma inesperada. Las

evidencias reales de producción deben conservarse en sistemas protegidos, no en publicaciones del manual.

31.37. Ejercicios de aplicación y criterios de respuesta

Las siguientes situaciones permiten razonar sobre el uso de alias sin depender de una topología concreta. No son instrucciones para alterar equipos en producción: el objetivo es reconocer qué objeto elegir, qué limitaciones existen y cómo se demostraría su funcionamiento.

Situación	Tipo aconsejado	Justificación y prueba
Autorizar tres equipos concretos	Host	Mantener entradas separadas; ensayar acceso de un miembro y de un no miembro.
Restringir acceso a una subred	Network	Usar prefijo CIDR; verificar que no se incluyen direcciones fuera del bloque.
Agrupar los puertos de una aplicación	Port	Especificar protocolo en la regla; ensayar al menos un puerto excluido.
Actualizar diariamente una lista administrada	URL Table (IPs/Ports)	Comprobar fuente, certificado, intervalo y contenido de tabla.
Auditar objetos internos presentes	All	Distinguir alias del sistema de alias creados por administración.

31.38. Guía rápida de decisión antes de usar un alias

Un alias apropiado minimiza los cambios necesarios y simplifica los permisos sin ocultar su alcance. Antes de ponerlo en servicio, responder afirmativamente a las comprobaciones de definición, vigencia, compatibilidad y reversión. Si cualquiera de ellas permanece sin validar, continuar las pruebas en un entorno controlado y no dar por aprobada la política.

01. Confirmar que el elemento agrupa direcciones, redes o puertos; si se pretende asignar IP al firewall, corresponde otra función.

02. Elegir Host/Network para direcciones, Port para servicios y URL Table si hace falta actualización periódica.

03. Comprobar si la pertenencia es estática o depende de DNS, una lista externa o una capa de anidación.

04. Revisar todas las reglas, NAT y funciones que reutilizan el objeto, con especial cuidado en accesos administrativos.

05. Inspeccionar el conjunto efectivo cuando se trate de direcciones variables: Diagnostics → Tables.

06. Comprobar efectos sobre IPv4 e IPv6 y realizar pruebas positivas y negativas en el camino real del tráfico.

07. Conservar responsable técnico, fecha de revisión y procedimiento de reversión documentados.

El valor profesional de un alias no reside en ahorrar una línea de una regla: reside en expresar una intención verificable y mantenerla de forma consistente durante todo el ciclo de vida de la red.

32 Firewall → NAT

Port Forward · 1:1 · Outbound · NPt | Traducción, permisos, precedencias y diagnóstico

Ruta de acceso: Firewall → NAT. El apartado reúne cuatro mecanismos de traducción de direcciones, con finalidades diferentes y reglas propias. Se estudian las vistas de administración, los parámetros de los formularios de alta, los riesgos de exposición, el comportamiento con múltiples enlaces y los procedimientos de comprobación. Los datos de los ejemplos son didácticos, independientes de cualquier infraestructura concreta.



Figura 32.1. Mapa funcional de las cuatro pestañas de NAT.

32.1. Qué es NAT y cuándo es necesario

Network Address Translation modifica una o varias direcciones —y, en algunos modos, los puertos— de un paquete al atravesar el firewall. Se utiliza para publicar servicios a través de direcciones externas, compartir direcciones públicas entre varios clientes, controlar la dirección visible de salida y, en escenarios IPv6 específicos, sustituir prefijos de red. pfSense Plus conserva estados de conexión para relacionar tráfico de ida y de respuesta.

NAT no crea conectividad por sí solo: debe existir una interfaz utilizable, rutas válidas hacia el destino y el origen, reglas de filtrado compatibles y, si el destino es un servicio, un proceso escuchando en el equipo receptor. Una traducción correcta puede coexistir con un bloqueo del firewall o un problema en el servidor.

32.2. Comparación rápida de las cuatro pestañas

Pestaña	Dirección / transformación	Caso habitual	Precaución principal
Port Forward	Destino de paquetes que entran; opcionalmente puerto.	Exponer un servicio interno concreto.	No confundir redirección con permiso.
1:1	Mapeo externo-interno, en ambos sentidos, sin cambiar puertos.	Asignar IP externa dedicada a un host.	Un filtro demasiado amplio puede exponer todos sus puertos.
Outbound	Origen y, normalmente, puerto de salida.	Clientes privados navegando mediante WAN.	No selecciona la WAN ni sustituye la política de rutas.
NPt	Prefijo de dirección IPv6, preservando parte de host.	IPv6 multi-WAN con prefijos enrutados.	No es PAT ni transforma a una IP única.

32.3. Conceptos esenciales: origen, destino, estado y puerto

Concepto	Significado	Ejemplo de lectura
Dirección de origen	IP del equipo que inicia el paquete.	Un cliente dentro de LAN.
Dirección de destino	IP a la que se dirige el paquete.	IP externa ofrecida por WAN.
Puerto origen	Puerto de transporte elegido por el iniciador.	Habitualmente dinámico y efímero.
Puerto destino	Servicio solicitado en el receptor.	TCP/443, UDP/53, etc.
Estado	Relación registrada de ida y vuelta.	Permite reconocer respuestas legítimas.
Regla de filtro	Política para permitir o denegar tráfico.	Se evalúa aparte de la traducción.

32.4. Orden de procesamiento y precedencias

En el tráfico entrante, las reglas de Port Forward tienen precedencia sobre las reglas 1:1 que pudieran alcanzar al mismo destino externo. Para conexiones salientes que coinciden, 1:1 tiene precedencia sobre Outbound NAT; dentro de las reglas de salida se evalúa la lista desde arriba y se emplea la primera coincidencia. Esta prioridad explica por qué una regla aparentemente bien definida no llega a actuar.

En las reglas de filtrado de entrada se comprueba la dirección de destino ya traducida; por ejemplo, en WAN el filtro debe permitir el destino interno al que apunta el Port Forward. Las interfaces y la política de enrutamiento siguen siendo determinantes, en particular cuando hay dos WAN.

Principio de seguridad. NAT no es un mecanismo de autorización. Configurar una dirección o un puerto traducido no sustituye una política de filtrado restrictiva ni el endurecimiento del servidor receptor.

32.5. Pantalla principal de Port Forward: tabla Rules

En Firewall → NAT → Port Forward, la tabla Rules enumera las traducciones de entrada definidas. Una tabla sin filas indica que no se muestran reglas de Port Forward en esa vista; no demuestra que falten traducciones 1:1, de salida o reglas automáticas en otras pantallas. En la interfaz aparecen controles de inserción arriba o abajo, selección y acciones sobre filas.

Cabecera	Qué representa	Qué conviene comprobar
Casilla de selección	Selecciona filas para operaciones agrupadas.	Evitar selecciones accidentales antes de Delete/Toggle.
Interface	Interfaz por la que entra el paquete original.	WAN específica y no un grupo de rutas.
Protocol	Protocolo IP al que se aplica la redirección.	TCP, UDP, TCP/UDP u otro según servicio.
Source Address / Ports	Origen y puerto de origen admitidos para coincidir.	Fuente normalmente restringible; puerto origen casi siempre Any.
Dest. Address / Ports	Dirección y puerto externos antes del NAT.	Deben coincidir con lo que recibe realmente la WAN.
NAT IP / NAT Ports	Destino y puerto internos después de traducir.	Servicio alcanzable y puerto escuchando.
Description	Motivo administrativo de la regla.	Documentación y justificación de acceso.
Actions	Edición, clonado y otras funciones por fila, según versión.	Revisar efecto de cambios en reglas asociadas.

32.6. Botones de mantenimiento de la lista

Control	Acción	Riesgo / recomendación
Add superior	Inserta nueva regla al inicio de la lista.	Puede anteponerse a una coincidencia general existente.
Add inferior	Inserta nueva regla al final.	Puede no alcanzarse si existe coincidencia anterior.

Control	Acción	Riesgo / recomendación
Delete	Borra las reglas seleccionadas.	Puede cortar inmediatamente una publicación tras aplicar.
Toggle	Activa o desactiva reglas seleccionadas.	Útil para pruebas controladas, deja registro de cambio.
Save	Guarda los cambios de orden/estado presentes en la lista.	Comprobar también Apply Changes cuando el sistema lo solicita.
Separator	Agrega separación visual para clasificar la lista.	No crea NAT ni concede permisos.
Ayuda contextual (?)	Abre información de la pantalla.	Sin impacto en el tráfico.

32.7. Port Forward: campos generales del formulario

Campo oficial	Función	Comportamiento al modificarlo
Disable	Inhabilita la entrada sin eliminarla.	La traducción de esa regla deja de aplicarse.
No RDR (NOT)	Excepción que evita redirigir tráfico coincidente.	Se reserva a políticas avanzadas, no como bloqueo genérico.
Interface	Selecciona el ingreso al que se aplica la regla.	En Multi-WAN se necesitan reglas por interfaz cuando proceda.
Address Family	Limita IPv4 o IPv6 y exige coherencia con los destinos.	Una familia incorrecta impide coincidencia.
Protocol	Selecciona TCP, UDP, TCP/UDP u otro protocolo IP disponible.	Los campos de puerto aparecen solo en protocolos que usan puertos.
Source	Dirección/red y puerto(s) de origen; opciones avanzadas.	Restringir por IP si la aplicación lo permite; puerto de origen Any.
Destination	IP externa (WAN Address, VIP, alias, etc.); Invert Match cuando aparece.	Debe coincidir con el destino original recibido.
Destination port range	Puerto o rango de entrada original.	Para un puerto basta From; To puede quedar en blanco.
Redirect target IP	IP final que recibirá el tráfico.	Debe ser alcanzable; se recomienda un único host de destino.
Redirect target port	Puerto final del servidor.	Puede ser distinto del público; rangos mantienen igual longitud.
Description	Finalidad de la redirección.	No altera el comportamiento de PF.

32.8. Port Forward: opciones avanzadas y asociación con el filtro

Opción	Finalidad técnica	Criterio operativo
No XMLRPC Sync	Impide la sincronización de esa regla en alta disponibilidad vía XMLRPC.	Usarla solo con un diseño HA explícito.
NAT Reflection	Default, NAT+Proxy, Pure NAT o Disable, según reglas/opciones disponibles.	Preferir split DNS en redes internas si es viable.
Filter Rule Association: None	No genera filtro asociado.	Crear una regla de permiso separada si hace falta.
Add associated filter rule	Crea una regla vinculada, actualizada junto con el Port Forward.	Habitualmente la opción más sencilla para mantener consistencia.
Add unassociated filter rule	Crea regla independiente sin seguimiento automático.	Requiere revisarla manualmente tras cambios.
Pass	Usa rdr pass para permitir tráfico sin regla de filtro separada.	No es compatible con Multi-WAN; evitar salvo necesidad justificada.

Los campos avanzados que se muestran al editar una entrada pueden variar según protocolo, familia y versión exacta de pfSense Plus. La columna Actions de la lista es independiente de las opciones del formulario; tampoco debe confundirse la selección de filas con la activación de una regla.



Figura 32.2. Secuencia de redirección y autorización, con direcciones ficticias.

32.9. Ejemplo guiado: publicar un servicio concreto

Escenario ilustrativo: una organización ofrece un servicio HTTPS en el servidor interno ficticio 10.77.40.20, escuchando en TCP/8443. La IP externa de ejemplo es 203.0.113.25, perteneciente a un bloque reservado para documentación. El objetivo es recibir TCP/443 desde orígenes autorizados y enviarlo al puerto interno, sin publicar otros puertos.

01. Confirmar que la IP externa está realmente asignada o enrutada hacia pfSense y que el servidor interno responde desde su red.
02. En Firewall → NAT → Port Forward, pulsar Add y seleccionar la interfaz WAN por la que llegará la solicitud.
03. Elegir Address Family IPv4, Protocol TCP y Source Address limitado a los orígenes autorizados si son conocidos.
04. Establecer Destination en la dirección externa pertinente y Destination port range en TCP/443.
05. Indicar Redirect target IP 10.77.40.20 y Redirect target port 8443; escribir una Description descriptiva.
06. Seleccionar Add associated filter rule, guardar y aplicar los cambios; revisar la regla generada en Firewall → Rules → WAN.
07. Probar desde una conexión realmente externa y observar registros, estados y capturas si es necesario.

No exponer administración. Una redirección que utilice una IP y un puerto donde ya escucha la GUI, una VPN u otro servicio de pfSense puede tener precedencia sobre ese servicio desde la interfaz afectada. Verificar coincidencias antes de aplicar.

32.10. Port Forward: seguridad, alcance y límites

Conviene publicar solo los servicios estrictamente necesarios, preferentemente detrás de una VPN o un reverse proxy cuando encaje con el diseño. No usar TCP/UDP por comodidad si el servicio requiere un único protocolo. Restringir orígenes si son estables, mantener el receptor actualizado, registrar accesos y acordar una ventana de revisión y retirada del permiso.

Una misma combinación de IP externa, protocolo y puerto que atiende a cualquier origen no puede redirigirse simultáneamente a dos servidores diferentes por simples reglas equivalentes. Para alojar múltiples servicios HTTPS en una IP y puerto suele necesitarse un proxy inverso en capa de aplicación, no duplicar Port Forwards. Las reglas de NAT no sustituyen comprobaciones del cortafuegos del propio servidor.

32.11. Port Forward desde LAN: split DNS y NAT reflection

Un equipo interno que intenta conectarse a un FQDN público puede resolverlo a la IP externa del firewall. El acceso interno a esa dirección no funciona automáticamente igual que el acceso desde Internet. Netgate

documenta alternativas como split DNS —resolución interna hacia la IP privada del servidor— y NAT Reflection, que crea una vía de retorno/redirección bajo condiciones específicas.

Para despliegues ordinarios, split DNS suele ser más sencillo y predecible. La reflexión puede introducir complejidad de retorno y comprobación adicional; se habilita solo cuando esté justificada. Un error de pruebas habitual es verificar una publicación desde un equipo de la misma LAN y concluir equivocadamente que falla desde Internet.

32.12. Port Forward con doble WAN y CGNAT

Una regla de redirección es específica de la interfaz por la que entra el tráfico. Si existen dos accesos, y ambos deben aceptar solicitudes, se necesita estudiar cada WAN por separado (dirección, llegada real del tráfico, regla de NAT, filtro y retorno). El failover de tráfico saliente no hace que una publicación entrante cambie de proveedor por sí sola.

Cuando el operador entrega una dirección privada o compartida mediante CGNAT, un Port Forward en el firewall propio no crea una ruta entrante desde Internet a través de la traducción del proveedor. Se requiere una dirección pública accesible, una redirección en el equipo aguas arriba o una solución de acceso remoto apropiada.

32.13. Pestaña 1:1: función y diferencias frente a Port Forward

La traducción 1:1 vincula una dirección externa con una interna y afecta al destino de las conexiones entrantes y al origen de las conexiones salientes que cumplen sus condiciones. A diferencia de un Port Forward, no limita por defecto a un servicio ni cambia el número de puerto: la restricción real de acceso se establece mediante reglas de firewall independientes. También pueden mapearse redes del mismo tamaño cuando sus prefijos están alineados.

Debe reservarse para supuestos donde exista un recurso de direccionamiento externo adecuado y una necesidad real de identidad IP estable. Para una sola publicación de servicio sobre una WAN con una única dirección, Netgate recomienda normalmente utilizar Port Forward.

32.14. 1:1: columnas, acciones y opciones del editor

Campo	Interpretación	Atención al configurarlo
Disabled	Desactiva la traducción 1:1.	Afecta entradas y salidas que dependan de ese mapeo.
No BINAT (NOT)	Excluye coincidencias de otra regla 1:1 posterior.	Solo para excepciones avanzadas.
Interface	Interfaz en la que se traduce.	No equivale a fijar automáticamente la ruta de salida.
Address Family	IPv4 o IPv6.	En IPv6 puede ser más adecuado NPt para prefijos.
External subnet IP	IP o red externa a la que se traduce.	Ha de existir VIP apropiada o ruta hacia el firewall.
Internal IP	IP o red interna asociada.	El equipo debe devolver su tráfico a través de pfSense.
Destination	Restricción opcional de extremos; por defecto Any.	En salida restringe destino; en entrada restringe origen.
Description	Finalidad del mapeo.	No afecta traducción.
NAT reflection	Comportamiento de acceso interno vía IP externa.	Analizar retorno, topología y DNS.

32.15. 1:1: condiciones, precedencia y permisos

Para recibir tráfico en una IP externa diferente de la IP primaria de la interfaz, el firewall debe poder atenderla o recibirla enrutada. Puede requerirse un Virtual IP apropiado; crear la entrada 1:1 sin disponer de direccionamiento externo válido no la vuelve alcanzable. La dirección interna tiene que ser única y estar correctamente enrutada.

En tráfico entrante, un Port Forward más específico puede prevalecer sobre el mapeo 1:1. En tráfico saliente, el mapeo 1:1 suele prevalecer sobre Outbound NAT para la interfaz correspondiente. No se

generan permisos universales: una política WAN que permita cualquier tráfico dirigido al host interno puede exponer servicios no previstos. Comprobar siempre el destino post-NAT de la regla del firewall.

32.16. Procedimiento 1:1 para un host con IP externa dedicada

01. Obtener la IP externa adicional mediante asignación válida, IP virtual o ruta hacia pfSense, según el modo del proveedor.
02. Comprobar en Firewall → Virtual IPs y en la tabla de rutas que el direccionamiento está disponible donde corresponde.
03. Abrir Firewall → NAT → 1:1, pulsar Add y fijar la WAN correspondiente, familia IP y dirección External subnet IP.
04. Indicar la dirección del host interno en Internal IP; mantener Destination en Any salvo restricción de diseño.
05. Guardar y aplicar; crear de forma independiente reglas WAN que permitan únicamente los servicios autorizados.
06. Comprobar entrada desde el exterior, salida del host con IP externa esperada y ausencia de exposición de puertos adicionales.
07. Revisar prioridad con otros Port Forwards y con reglas Outbound NAT, incluyendo interfaces de respaldo.

32.17. 1:1 de subred: tamaño, alineación y alcance

pfSense permite traducir un bloque entero a otro de idéntico tamaño y alineación, conservando la correspondencia relativa de host. Antes de crear una regla de este tipo hay que validar la disponibilidad de todo el espacio externo, la ruta de retorno, la ausencia de solapamientos y los filtros que lo acompañan. Es una operación de arquitectura de direccionamiento, no un atajo para publicar cualquier rango de servidores.

32.18. Pestaña Outbound: para qué sirve el NAT de salida

Outbound NAT, también denominado Source NAT, modifica el origen de conexiones que salen por una interfaz. En redes IPv4 típicas permite que múltiples clientes con direcciones privadas utilicen la IP externa de la WAN. En despliegues con más de una salida, se ejecuta después de que el enrutamiento y las reglas de política hayan determinado el camino correspondiente; seleccionar una regla Outbound NAT no fuerza por sí mismo el uso de una WAN.

32.19. Outbound: los cuatro modos del panel

Modo	Qué reglas se utilizan	Uso recomendado / riesgo
Automatic Outbound NAT	Reglas autogeneradas a partir de redes internas, WAN, rutas y VPN que corresponden.	Opción habitual para una instalación sencilla.
Hybrid Outbound NAT	Reglas manuales prioritarias y automáticas para el resto.	Ajustes particulares sin rehacer toda la traducción.
Manual Outbound NAT	Solo reglas manuales existentes.	Control total; omisiones pueden cortar acceso de subredes.
Disable Outbound NAT	Desactiva traducción de salida.	Redes completamente enrutadas, sin necesidad de NAT.

Cuando la lista está vacía y se cambia a Manual, pfSense puede crear un conjunto inicial equivalente al automático; eso no exime de revisar y mantener todas las subredes e interfaces tras cambios futuros. Las reglas visibles en Outbound carecen de efecto manual si el modo sigue en Automatic. En Hybrid y Manual las entradas se procesan de arriba abajo: gana la primera coincidencia.

Punto crítico. Cambiar de Automatic/Hybrid a Manual o Disable puede dejar sin salida redes, VPN y servicios dependientes de NAT. Exportar la configuración, inventariar fuentes y disponer de una vía de recuperación antes de aplicar.

32.20. Outbound: campos de coincidencia — General Options

Control	Función	Consejo práctico
Disabled	Desactiva la regla específica.	No equivale a cambiar el modo general.
Do not NAT	Excepción: no traducir un flujo coincidente.	Ubicar antes de reglas generales; revisar origen/destino.
Interface	Interfaz efectiva de egreso donde operará la regla.	Debe coincidir con la WAN real elegida por routing.
Address Family	Familia IP a la que se aplica.	Evitar NAT IPv6 si no existe necesidad excepcional.
Protocol	Protocolo objeto de traducción.	Any en general; restringir para casos como UDP específico.
Source	Red o alias de la que procede el tráfico.	Evitar Any si incluye al propio firewall y su monitorización.
Source Port	Puerto de origen que debe coincidir.	Normalmente Any; muchas aplicaciones usan efímeros.
Destination	IP/red/alias destino a la que aplica el NAT.	Any en casos estándar; restringir para excepción concreta.

32.21. Outbound: traducción y opciones de puertos

Control	Significado	Uso y efectos secundarios
Translation / Address	Dirección de origen resultante: Interface Address, VIP o conjunto compatible.	La elección tiene que estar disponible/enrutada.
Pool Options	Algoritmo para escoger una IP de traducción dentro de un pool.	Default, Round Robin, Sticky, Random, Hash o Bitmask según origen del pool.
Port or Range	Fija puerto(s) origen traducidos.	Usar solo cuando un protocolo lo exija.
Static Port	Conserva el puerto de origen original.	Puede ayudar a SIP/RTP o algunos protocolos; no activar globalmente.
Endpoint-independent Mapping	Mapeo experimental de puerto/conectividad para ciertos clientes.	No combinar con Static Port; comprobar soporte y seguridad.
No XMLRPC Sync	Excluye esta regla de sincronización HA.	Solo con política HA comprobada.
Description	Motivo de la excepción de NAT.	Identificar servicio, flujo y razón del cambio.

Las opciones de Pool dependen de si se ha elegido un alias de hosts o un único bloque: con alias de hosts solo se admiten variantes Round Robin documentadas. Una regla Outbound NAT no acepta un alias formado por múltiples prefijos de red para definir el bloque de traducción. Static Port y Endpoint-independent Mapping son opciones incompatibles entre sí.



Figura 32.3. Diferencia entre la reescritura del origen IPv4 y la traducción de prefijos IPv6.

32.22. Cómo introducir una excepción Outbound sin interrumpir la red

01. Examinar el modo actual y las Automatic Rules que se muestran en Firewall → NAT → Outbound.
02. Si el comportamiento habitual debe mantenerse, seleccionar Hybrid Outbound NAT; guardar el cambio de modo.
03. Pulsar Add en la zona de reglas manuales y elegir la interfaz WAN de salida correspondiente.
04. Definir la subred de origen precisa, el protocolo y, solo si procede, un destino específico; evitar Source = Any.
05. En Translation, seleccionar Interface Address o el recurso externo correctamente definido. Activar Static Port solo si existe un requisito verificado.
06. Guardar, aplicar los cambios y situar la excepción encima de otras entradas más amplias.
07. Validar tráfico de clientes normales, tráfico específico de la excepción, monitorización de gateway, DNS y conexiones VPN.

32.23. Outbound con múltiples WAN, VPN y alta disponibilidad

Cada WAN puede necesitar su traducción adecuada para las redes que salen por ella. La elección de la interfaz de salida es responsabilidad del enrutamiento y de las reglas con gateway o gateway group; NAT se aplica posteriormente en la interfaz correspondiente. En modo Manual deben contemplarse las redes LAN, otras subredes internas, rutas estáticas y redes de clientes VPN que realmente necesiten NAT en cada salida.

En entornos con CARP/HA puede interesar traducir tráfico hacia una dirección virtual CARP para mantener una identidad externa compartida. No se deben transformar de forma indiscriminada direcciones del propio firewall o de los nodos de respaldo; una regla de excepción Do not NAT puede ser necesaria en escenarios concretos.

32.24. Static Port, aplicaciones especiales y preservación de estados

Por defecto, el NAT saliente puede reescribir puertos de origen para reducir colisiones y mejorar ciertas propiedades de seguridad; hay excepciones automáticas documentadas, como IKE/UDP 500. Algunas aplicaciones de telefonía o juegos pueden requerir conservar el puerto de origen, por lo que se crea una regla específica de Static Port, acotada a la red y al protocolo necesarios, nunca una regla global precipitada.

La activación de Static Port no garantiza por sí sola la interoperabilidad SIP, RTP o VPN: también afectan los temporizadores, la topología, filtros del proveedor y los protocolos de señalización. Si existe Endpoint-independent Mapping, se evaluará aparte y nunca simultáneamente con Static Port.

32.25. Pestaña NPt: traducción de prefijos de red IPv6

NPt (Network Prefix Translation) sustituye un prefijo IPv6 interno por otro prefijo IPv6 externo enrutado, manteniendo los bits de identificación de host. Es una función distinta del NAT/PAT IPv4, del NAT64 y de 1:1 sobre direcciones individuales. pfSense implementa NPt de forma con estado y no de la misma manera que NPT66 según RFC 6296; no debe presentarse como equivalente sin matices.

NPt se utiliza principalmente en topologías IPv6 multi-WAN donde se desea mantener estable la numeración interna y traducirla al prefijo enrutado de una WAN concreta. También puede estudiarse con direccionamiento interno ULA, aunque Netgate desaconseja ese diseño como opción preferente para este caso.

32.26. NPt: campos del formulario

Campo	Descripción	Condición de validez
Disabled	Impide aplicar esa entrada NPt.	Comprobar la repercusión en el egreso IPv6.
Interface	WAN por la que sale el tráfico que debe traducirse.	Debe tener camino de salida y prefijo externo enrutado.
Source IPv6 Prefix	Subred de origen IPv6 que utilizarán los clientes internos.	Longitud de prefijo correcta, normalmente /64.
Destination IPv6 Prefix	Prefijo externo al que se traduce.	Debe estar enrutado hacia pfSense, no ser la sola IP WAN.
Description	Finalidad de la entrada.	Identificar origen y vínculo administrativo.

32.27. NPt: restricciones que determinan si funcionará

Los prefijos deben tener el mismo tamaño; no se puede usar NPt para convertir una /64 completa en una única dirección WAN, ni para traducir a un prefijo que el proveedor no enruta hacia el firewall. La dirección WAN usada para el enlace no es necesariamente el prefijo de red externo delegado o enrutado que NPt necesita.

La traducción solo resuelve el cambio de numeración: deben existir rutas IPv6, anuncios RA o configuración de clientes coherentes, permisos de firewall, delegación válida y conectividad de retorno. Si se usan varias WAN con prefijos distintos, cada una se diseña y comprueba de manera independiente.

32.28. Procedimiento NPt para un prefijo interno IPv6

01. Verificar que el enlace externo tiene un prefijo IPv6 enrutado hacia el firewall, no solo una dirección de enlace.

02. Inventariar el prefijo IPv6 de la LAN, su longitud y los anuncios o rutas que utilizan los clientes.

03. Acceder a Firewall → NAT → NPt y pulsar Add.

04. Elegir Interface como la WAN pertinente; indicar Source IPv6 Prefix y Destination IPv6 Prefix del mismo tamaño.

05. Anotar Description, guardar y aplicar la configuración.

06. Permitir el tráfico IPv6 en Firewall → Rules según el principio de mínimo privilegio.

07. Comprobar salida y retorno con pruebas IPv6 desde clientes, capturas en ambas interfaces y verificación de rutas.

32.29. Cómo elegir el tipo de NAT adecuado

Necesidad	Mecanismo inicial	Motivo de elección
Publicar un puerto TCP concreto	Port Forward	Limita traducción a protocolo/puerto y facilita filtro vinculado.
Dar IP externa específica a un servidor	1:1	Vincula una IP interna a una externa para tráfico en ambos sentidos.
Proporcionar Internet IPv4 a LAN privada	Outbound Automatic	Reglas de traducción habituales sin mantenimiento manual.

Necesidad	Mecanismo inicial	Motivo de elección
Excepción de traducción para VPN/VoIP	Outbound Hybrid	Conserva automatismos y aplica excepción específica.
IPv6 multi-WAN con prefijos enrutados	NPt	Sustituye prefijos preservando el identificador de host.
Entrar por CGNAT desde Internet	Ningún Port Forward local por sí solo	Requiere solución de conectividad aguas arriba o túnel.
Acceso interno a FQDN público	Split DNS / reflexión según diseño	No deducir funcionamiento interno a partir de NAT WAN.

32.30. Comprobación sistemática de NAT: cinco planos

El diagnóstico eficiente separa la prueba en cinco planos: llegada del paquete a la interfaz correcta, coincidencia de la traducción, permiso del firewall, alcanzabilidad del destino y retorno de la sesión. Las herramientas de pfSense permiten observar cada nivel sin asumir que una regla visible está funcionando.

Plano	Herramienta orientativa	Resultado que debe buscarse
Llegada física/IP	Diagnostics → Packet Capture en WAN.	Paquetes originales alcanzan destino y puerto externos.
Traducción	Reglas activas, estados PF y capturas posteriores.	Dirección y puerto cambian según se ha configurado.
Filtrado	Firewall → Rules y Status → System Logs → Firewall.	Se permite explícitamente el destino ya traducido.
Destino	Captura en LAN, prueba desde el firewall y log del servidor.	El servicio recibe y acepta el tráfico.
Respuesta	Capturas WAN/LAN, Diagnostics → States y rutas.	Retorno simétrico y estado correcto.

32.31. Incidencias frecuentes y forma de resolverlas

Síntoma	Causa probable	Acción de diagnóstico
Port Forward no responde	No llega tráfico, falta regla WAN o servicio cerrado.	Capturar en WAN y LAN; revisar filtro y puerto de escucha.
Funciona desde fuera, no desde dentro	Falta split DNS/reflexión o retorno incorrecto.	Comparar FQDN/IP por ubicación del cliente.
Servicio del firewall deja de responder	Port Forward solapa IP/puerto de servicio local.	Revisar las coincidencias sobre la misma interfaz.
1:1 publicado pero sin acceso	No hay ruta/Virtual IP o falta permiso de filtro.	Verificar IP externa y destino interno traducido.
El cliente IPv4 no sale	Falta Outbound NAT al usar Manual/Disable.	Comprobar modo, regla fuente, WAN y rutas.
La excepción híbrida no actúa	Regla amplia arriba o interfaz distinta.	Ordenar reglas y revisar salida real.
La WAN secundaria no admite entrada	CGNAT, dirección distinta o retorno.	Validar IP pública y accesibilidad del proveedor.
NPt IPv6 falla	Prefijo no enrutado o tamaños distintos.	Comprobar prefijos, rutas, reglas y tráfico IPv6.
VoIP falla con puertos reescritos	NAT inadecuado o SIP/ALG del extremo.	Probar Static Port específico y capturas.
Cambio visible sin efecto	No se aplicaron cambios o estados preexistentes.	Apply Changes, estados activos y nueva conexión de prueba.

32.32. Procedimiento de cambio seguro y recuperación

01. Describir el objetivo y confirmar quién usa el flujo afectado; inventariar dependencias y reglas existentes.
02. Exportar una copia de seguridad de la configuración y prever una vía de gestión local u out-of-band.

03. Definir el cambio mínimo y su ventana: nueva regla, prioridad, WAN, IP externa e interfaz interna.
04. Crear primero permisos restringidos, cuando sea viable, evitando solapamientos con la administración del firewall.
05. Guardar, aplicar y probar con conexiones nuevas desde ubicaciones válidas; registrar evidencias.
06. Si hay pérdida de servicio, revertir el cambio concreto y revisar estados; no cambiar simultáneamente NAT, gateway y reglas sin trazabilidad.
07. Documentar fecha, responsable, alcance y criterio de retirada, sin almacenar secretos en el documento técnico.

32.33. Buenas prácticas de seguridad y administración

Utilizar VPN para administración remota antes que publicar directamente servicios sensibles; separar servicios expuestos en segmentos específicos; emplear controles de aplicación y parcheo de hosts; definir orígenes mínimos y registrar intentos de acceso. Revisar periódicamente redirecciones sin uso, VIP obsoletas y excepciones de salida que ya no se necesitan.

Para Outbound NAT, conservar Automatic salvo necesidad justificada y preferir Hybrid para personalizaciones acotadas. En Multi-WAN, validar tanto los flujos normales como los de contingencia. En IPv6, priorizar encaminamiento extremo a extremo sin NAT salvo casos donde NPt aporte una ventaja verificable.

32.34. Lista de comprobación final para una modificación NAT

Comprobación	Criterio de aceptación
Objetivo	Se identifica un servicio o flujo concreto y su propietario funcional.
Entrada	La dirección/puerto original llega a la interfaz declarada.
Traducción	Destino o fuente transformados conforme al diseño.
Regla de filtro	El filtro autoriza el destino post-NAT y no otros servicios.
Enrutamiento	Gateway y ruta de retorno existen y son coherentes.
Conexiones existentes	Se sabe si deben renegociarse estados tras el cambio.
Multi-WAN	Todas las salidas previstas y las rutas de retorno se han probado.
IPv6	Se verifica direccionamiento/longitud y prefijo enrutado si hay NPt.
Reversión	Existe backup, acceso y procedimiento de recuperación.
Documentación	Quedan registro, evidencias y fecha de revisión.

32.35. Glosario técnico

Término	Definición
DNAT / Redirect	Modificación del destino que reciben los paquetes entrantes.
SNAT / Outbound NAT	Modificación de la dirección origen de paquetes salientes.
PAT / Overload	Compartir una IP mediante traducción de puertos de transporte.
VIP	Dirección IP virtual adicional configurada en el firewall.
CGNAT	NAT de operador: tráfico entrante no depende solo del firewall local.
Hairpin / Reflection	Acceso desde red interna a publicación mediante su dirección externa.
Split DNS	Respuestas DNS distintas dentro y fuera para un mismo nombre.
Static Port	Conservación del puerto original en traducción de salida.

Término	Definición
NPt	Traducción con estado de un prefijo IPv6 por otro prefijo.
NAT64	Transición entre tráfico IPv6 e IPv4; función diferente de NPt.
Estado PF	Registro temporal que vincula un flujo a su tratamiento bidireccional.

32.36. Matriz de aceptación: comprobar un servicio publicado

Esta ficha permite validar un Port Forward sin confundir la publicación con el acceso autorizado. Anotar únicamente resultados generales en la documentación compartida; no copiar IP operativas, nombres de hosts ni datos de clientes cuando no sean necesarios.

Prueba	Condición de éxito	Qué hacer si falla
Alcance externo	Cliente fuera de la LAN alcanza la dirección publicada.	Verificar conectividad y llegada de paquetes a WAN.
NAT correcto	Paquetes llegan al host y puerto internos previstos.	Revisar destino original, interfaz y prioridad.
Filtro restrictivo	Solo orígenes y servicios autorizados tienen acceso.	Corregir regla vinculada o filtro manual.
Reversibilidad	Deshabilitar la regla elimina la publicación sin afectar gestión.	Preparar reversión y revisar servicios solapados.
Monitorización	Logs y estados permiten explicar conexiones válidas y bloqueadas.	Activar registros necesarios y comprobar rutas.
Documentación	Quedan finalidad, responsable y fecha de revisión.	Completar registro de cambio y caducidad.

32.37. Referencias oficiales y normas de consulta

Documentación de referencia del fabricante, consultada para las definiciones, campos, prioridades y precauciones de cada una de las cuatro pestañas. La disposición exacta de controles puede variar según la versión y las capacidades habilitadas en pfSense Plus.

01. Network Address Translation — Netgate. https://docs.netgate.com/pfsense/en/latest/nat/index.html

02. Port Forwarding — Netgate. https://docs.netgate.com/pfsense/en/latest/nat/port-forwards.html

03. 1:1 NAT — Netgate. https://docs.netgate.com/pfsense/en/latest/nat/1-1.html

04. Outbound NAT — Netgate. https://docs.netgate.com/pfsense/en/latest/nat/outbound.html

05. IPv6 Network Prefix Translation (NPt) — Netgate.
https://docs.netgate.com/pfsense/en/latest/nat/npt.html

06. Ordering of NAT and Firewall Processing — Netgate.
https://docs.netgate.com/pfsense/en/latest/nat/process-order.html

07. Multi-WAN and NAT — Netgate. https://docs.netgate.com/pfsense/en/latest/multiwan/nat.html

08. Troubleshooting NAT — Netgate.
https://docs.netgate.com/pfsense/en/latest/troubleshooting/nat.html

09. NAT Reflection — Netgate. https://docs.netgate.com/pfsense/en/latest/nat/reflection.html

10. IPv6 and NAT — Netgate. https://docs.netgate.com/pfsense/en/latest/network/ipv6/nat.html

33 Firewall → Packet Flow Data

Seguimiento de estados · NetFlow v5 · IPFIX · Exportadores · Seguridad y diagnóstico

Ruta de acceso: Firewall → Packet Flow Data. Esta función permite enviar información estructurada de comunicaciones de red a recolectores externos. Se examinan los controles de la vista principal y, separadamente, las opciones adicionales que Netgate documenta para los formularios de exportación y las reglas del firewall. El capítulo utiliza únicamente ejemplos de documentación y esquemas propios.



Figura 33.1. Arquitectura de generación y envío de registros de flujo a partir de estados PF.

33.1. Objetivo: convertir estados de conexión en información útil

Packet Flow Data exporta metadatos de tráfico desde el motor PF del firewall para que una plataforma receptora pueda agrupar comunicaciones, analizar patrones de uso, producir estadísticas y facilitar investigaciones operativas. Se basa en la infraestructura nativa pflow(4) y no necesita un daemon independiente ni instalar paquetes adicionales.

Un registro de flujo resume una comunicación, normalmente mediante direcciones, protocolo, puertos, recuentos y referencias temporales según el formato; no incorpora el contenido íntegro de aplicaciones como una captura PCAP. El detalle concreto que presente el colector depende del protocolo seleccionado, de las plantillas o campos disponibles y de su capacidad para interpretar los registros.

33.2. Disponibilidad, versiones y límites de alcance

La función nativa está disponible en pfSense Plus a partir de la versión 24.03 y no se incluye en pfSense CE. Puede exportar NetFlow v5 e IPFIX, permite configurar hasta 16 exportadores distintos y admite el seguimiento general o por reglas concretas. NetFlow v5 no contiene registros de flujos IPv6; para observar IPv6 corresponde seleccionar IPFIX y un colector compatible.

El sistema solo puede generar datos para tráfico que origine estados en el firewall y esté incluido en la política de seguimiento. Que una interfaz reciba paquetes no implica que todos ellos se registren: los bloqueos, el tráfico que no conserva estado y las conexiones ya existentes requieren un tratamiento distinto.

33.3. Qué se considera un flujo y en qué se diferencia de un paquete

Concepto	Qué representa	Uso principal
Paquete	Unidad puntual de transmisión, encabezado y posible carga útil.	Analizar errores o secuencias concretas con captura.
Estado PF	Entrada de conexión que permite filtrar retornos y acumular estadísticas.	Decidir tratamiento y conocer conexiones activas.
Flujo exportado	Resumen estructurado asociado a una comunicación observada por el firewall.	Contabilizar, clasificar y correlacionar tráfico.

Concepto	Qué representa	Uso principal
Colector	Servicio externo que recibe, interpreta y almacena exportaciones.	Consultas históricas, visualización y alertas.
Firewall log	Registro de eventos asociados a reglas y decisiones.	Diagnosticar permisos, bloqueos y política.

33.4. Lectura de la pantalla principal: tres zonas

La vista se organiza en Packet Flow Data Information, Global Packet Flow Options y Packet Flow Exporters. La primera es un texto explicativo; la segunda permite activar el mecanismo y determinar el comportamiento inicial de las reglas; la tercera inventaría las configuraciones de salida hacia colectores. Una lista sin filas visibles significa que esa pantalla no muestra exportadores configurados.

Zona	Elementos visibles	Acción del administrador
Packet Flow Data Information	Texto descriptivo de NetFlow/IPFIX y estados.	Comprender la dependencia de las reglas con estado.
Global Packet Flow Options	Enable, Track by Default y Save.	Definir el comportamiento global y guardarlo.
Packet Flow Exporters	Tabla de 8 columnas y botón Add.	Crear y administrar destinos de exportación.

33.5. Packet Flow Data Information: significado práctico

El texto introductorio indica que se pueden exportar flujos a uno o varios colectores externos usando formatos como NetFlow e IPFIX. También aclara que la recopilación parte de estados creados por tráfico que coincide con reglas del firewall, bien de forma predeterminada o mediante selección por regla. Esta limitación evita confundir la función con un capturador universal de todo el tráfico que circula por el dispositivo.

33.6. Enable: activar la recopilación y exportación

La casilla Enable Packet Flow Data Tracking and Exporting habilita el mecanismo global. Al marcarla, pfSense prepara el módulo pflow(4) del núcleo y la configuración de los exportadores; sin ella no hay exportación operativa, aunque existan entradas definidas en la tabla. Desmarcarla desactiva el servicio global para estados nuevos, pero la transición de los estados existentes tiene particularidades.

Advertencia de ciclo de vida. Los cambios de habilitación solo se aplican a los estados creados después del cambio. Estados anteriores pueden seguir comportándose según la configuración con la que nacieron. No reiniciar ni vaciar estados indiscriminadamente: la desconexión de sesiones afecta a usuarios y servicios.

33.7. Track by Default: política global de seguimiento

La casilla Enable Packet Flow tracking on all rules by default establece cómo se tratan los estados nuevos cuando una regla mantiene la opción Use global default. Activada significa seguimiento general; desactivada significa que ninguna regla lo hace por defecto y que se ha de marcar expresamente Always track en las reglas elegidas.

El control no convierte el tráfico bloqueado en flujos ni altera la acción Pass/Block/Reject. Solamente define el alcance del registro exportado para reglas que crean estados. Una excepción por regla puede incluir o excluir tráfico con independencia del valor global.

33.8. Matriz de comportamiento entre opción global y reglas

Enable global	Track by Default	Valor de la regla	Resultado para estados nuevos
Desactivado	Cualquiera	Cualquiera	No hay exportación global activa.
Activado	Desactivado	Use global default	No se sigue el flujo.
Activado	Desactivado	Always track Packet Flow Data	Se sigue el flujo.

Enable global	Track by Default	Valor de la regla	Resultado para estados nuevos
Activado	Activado	Use global default	Se sigue el flujo.
Activado	Activado	Never track Packet Flow Data	Se excluye el flujo.
Activado	Cualquiera	Regla sin estados	No existe estado exportable.



Figura 33.2. Regla global y excepciones: interpretación para estados nuevos, si el exportador está operativo.

33.9. Save y Apply Changes: secuencia de cambios

El botón Save situado bajo las opciones globales conserva la selección de Enable y Track by Default. Cuando la interfaz presenta Apply Changes, este paso debe completarse para activar la configuración pendiente, igual que en otras páginas de pfSense. El botón Add de exportadores abre un formulario diferente; guardar los controles globales no sustituye la creación del colector ni su verificación.

33.10. Packet Flow Exporters: qué muestra la tabla de exportadores

La parte inferior de la pantalla contiene Source Address, Source Port, Dest. Address, Dest. Port, Flow Protocol, Observation Domain, Description y Actions. Estos campos identifican desde qué extremo sale el tráfico de exportación, a dónde se envía y cómo debe interpretarlo el colector. La visualización de esas columnas no significa por sí misma que un flujo esté llegando a su destino.

Columna visible	Significado técnico	Comprobación recomendada
Source Address	IP local de origen utilizada para los datagramas de exportación.	Que sea válida y enrutable hacia el colector.
Source Port	Puerto UDP emisor; puede dejarse a elección automática.	Evitar colisiones si se fija.
Dest. Address	IP del equipo receptor.	Que sea alcanzable desde el firewall.
Dest. Port	Puerto de escucha del colector.	Coincidir con su configuración UDP.
Flow Protocol	Codificación NetFlow v5 o IPFIX.	Compatibilidad y soporte IPv6/NAT.
Observation Domain	Identificador lógico de origen para el colector.	Identificar exportadores sin ambigüedad.
Description	Texto descriptivo para administración.	Finalidad y responsable de la salida.
Actions	Operaciones sobre cada exportador existente.	Revisar impacto antes de modificar o eliminar.

33.11. Acciones de la tabla y estado de las entradas

La documentación de Netgate describe un indicador de activación/desactivación por fila, así como Edit (lápiz), Clone (duplicar) y Delete (papelera, con confirmación). Una entrada deshabilitada se representa con

menor contraste. Add abre un exportador nuevo y deja de mostrarse cuando se alcanza el límite permitido. Cuando todavía no se ha definido ningún exportador, los controles de edición por fila no se presentan: corresponden a entradas ya creadas.

Clonar una entrada copia su definición y exige revisar especialmente origen, puerto fijo, destino, protocolo e identificador de observación para evitar configuraciones duplicadas no intencionadas. Eliminar una entrada interrumpe el envío hacia ese colector, no elimina automáticamente los datos que el receptor ya hubiera guardado.

33.12. Formulario Add: opciones documentadas por Netgate

Al elegir Add se abre el editor de una configuración de exportación. Sus campos, documentados por Netgate, se muestran durante la creación o edición de un exportador y complementan las columnas de la vista de resumen.

Campo del editor	Comportamiento	Recomendación
Description	Identifica la finalidad de la configuración.	Nombre funcional sin datos personales.
Enable	Activa o desactiva este exportador individual.	Probar con una entrada antes de desplegar más.
Source IP Address	Selecciona interfaz local, VIP u otra dirección apta.	Escoger una dirección enrutable y estable.
Source Port	Puerto de origen; vacío usa uno aleatorio.	Dejar vacío salvo requisito del colector.
Destination IP Address	IP v4/v6 del colector.	Asegurar ruta, control de acceso y disponibilidad.
Destination Port	Puerto receptor; vacío utiliza 2055.	Hacer coincidir con el servicio receptor.
Flow Protocol	NetFlow v5 o IPFIX.	Preferir IPFIX si hay tráfico IPv6.
Observation Domain	Identificador de dominio de observación.	Valor coordinado con el recolector; 1 por defecto.

33.13. Source IP Address: selección y rutas

Source IP Address es un selector de direcciones locales válidas, incluidas interfaces y direcciones IP virtuales, y no una lista arbitraria de IP de clientes. Debe corresponder a la familia de destino IPv4 o IPv6. Si el colector se alcanza por una VPN, normalmente conviene seleccionar el origen de la interfaz de túnel correspondiente o una dirección local con ruta de retorno reconocible por el colector.

Una fuente incorrecta puede impedir la ruta de respuesta, hacer que un filtro remoto descarte el flujo o provocar dificultades de correlación. En entornos con WAN alternativa, el origen explícito debe comprobarse también en escenarios de contingencia.

33.14. Source Port: uso de puerto fijo o dinámico

Source Port identifica el extremo emisor de la exportación. Por defecto se deja en blanco para que el sistema elija un puerto aleatorio. Netgate advierte que, si se fija, no debe encontrarse en uso por otro servicio del firewall, incluidos otros exportadores, y debe seleccionarse también Source IP Address de forma explícita.

El puerto de origen no es el puerto al que escucha el recolector; confundir Source Port y Destination Port es una causa de incidencias evitables. En general, no hace falta fijar el puerto origen para instalar un sistema de recepción de flujos.

33.15. Destination IP Address y Destination Port

Destination IP Address define un destino IP literal IPv4 o IPv6: el recolector de NetFlow/IPFIX. El puerto de destino debe coincidir con el configurado en el servicio receptor. Si Destination Port se deja vacío, Netgate especifica el puerto 2055. Este valor es un valor predeterminado de pfSense, no una obligación de todos los productos receptores.

Los paquetes de exportación deben llegar por una ruta válida y superar las políticas de seguridad del recorrido. La familia de Source IP Address debe coincidir con la familia del Destination IP Address; por ejemplo, una fuente IPv6 para un colector IPv6. La familia del transporte de exportación es independiente de los flujos que representan las plantillas de IPFIX.

33.16. Flow Protocol: cuándo usar NetFlow v5 o IPFIX

Aspecto	NetFlow v5	IPFIX
Compatibilidad	Amplio soporte en colectores tradicionales.	Requiere colector con decodificador IPFIX.
Datos IPv4	Sí.	Sí.
Datos IPv6 de flujos	No, v5 no representa IPv6.	Sí, con soporte del receptor.
Información NAT44	Sin el mecanismo descrito para IPFIX.	Incluye información NAT44 conforme a RFC 8158.
Elección típica	Compatibilidad heredada centrada en IPv4.	Observabilidad IPv4/IPv6 y más flexibilidad.

NetFlow v5 e IPFIX son formatos de exportación de metadatos, no una vía para reenviar paquetes originales ni una alternativa a TLS. El tráfico de exportación debe protegerse con segmentación o mediante un túnel de confianza cuando atraviesa redes no controladas.

33.17. Observation Domain: identidad del dominio exportador

Observation Domain permite diferenciar conjuntos de flujos en un colector, especialmente al integrar varios dispositivos o distintas exportaciones. Su valor es un entero sin signo de 32 bits distinto de cero, desde 1 hasta 4 294 967 295. En blanco utiliza 1. El receptor puede utilizar este campo para interpretar el origen y separar registros; no todos los colectores lo aprovechan.

Coordinar los identificadores en lugar de asignarlos sin criterio facilita la operación y evita mezclar informes de orígenes diferentes. No constituye un control de autenticación ni sustituye la validación del origen de red.

33.18. Hasta dieciséis exportadores: usos y costes

Pueden definirse hasta 16 configuraciones independientes, enviando flujos a varios colectores y/o utilizando formatos diferentes. Es útil para compatibilidad entre sistemas, pruebas de migración o conservación separada, pero cada destinatario adicional aumenta el tráfico y los elementos que administrar. No se debe asumir que dos destinos reciben exactamente las mismas estadísticas si sus opciones o formatos difieren.

33.19. Reglas individuales: Use global default, Always y Never

En Firewall → Rules, dentro de las opciones avanzadas de una regla compatible con estados, pfSense Plus permite controlar Packet Flow Data por regla. Los valores documentados son Use global default, Always track Packet Flow Data y Never track Packet Flow Data. Un cambio de seguimiento no crea una regla nueva de permiso ni transforma la acción de filtrado; se aplica a los estados que genere esa regla.

Una política de seguimiento selectivo es apropiada para medir tráfico de aplicaciones relevantes sin registrar innecesariamente cada conexión de estaciones o segmentos. La opción Never track puede excluir categorías sensibles cuando el marco de privacidad lo requiera.

33.20. Ciclo de vida de estados: por qué no se exportan sesiones antiguas

La exportación depende de la decisión tomada cuando se crea un estado. Al activar Packet Flow Data, las conexiones que ya tenían estado no pasan automáticamente a producir datos; al desactivarlo, estados existentes pueden seguir generando datos durante su ciclo de vida. Lo mismo requiere cautela cuando se cambia el alcance predeterminado o una excepción por regla.

Netgate señala que reiniciar el equipo o restablecer estados permite homogeneizar el comportamiento, pero estas operaciones son disruptivas. En una red empresarial se debe preferir un ensayo con conexiones nuevas y programar una intervención si realmente es necesario eliminar estados en producción.

Pérdida de servicio. Vaciar la tabla de estados puede cortar temporalmente VPN, sesiones de administración y conexiones de usuarios. Esta acción no es un paso normal de habilitación ni de diagnóstico inicial; debe estar justificada, autorizada y disponer de reversión.

33.21. Procedimiento A: activar exportación general a un colector

01. Confirmar que el equipo utiliza pfSense Plus 24.03 o posterior y que existe un colector compatible y autorizado.
02. Decidir formato (NetFlow v5 si únicamente se necesita IPv4 y compatibilidad heredada; IPFIX para IPv6 y capacidades adicionales).
03. En Firewall → Packet Flow Data, activar Enable Packet Flow Data Tracking and Exporting.
04. Activar Track by Default si la política aprobada exige seguir los estados de todas las reglas salvo excepciones.
05. Pulsar Save para conservar las opciones globales.
06. En Packet Flow Exporters, pulsar Add y escribir una Description neutra, Enable y el origen IP apropiado.
07. Indicar el destino real del colector en Destination IP Address; comprobar Destination Port, Flow Protocol y Observation Domain.
08. Guardar el exportador y completar Apply Changes cuando se muestre.
09. Generar una conexión de prueba NUEVA cuya regla cree estado y revisar tanto los registros recibidos como los estados de pfSense.
10. Documentar el alcance, el responsable del colector, el volumen previsto y la política de conservación de datos.

33.22. Procedimiento B: seguimiento selectivo de una aplicación

01. En las opciones globales, mantener Enable activado y desactivar Track by Default; guardar.
02. Crear o revisar una regla de paso que genere estado para el flujo de interés. No ampliar permisos por motivos de monitorización.
03. En las opciones avanzadas de la regla seleccionar Always track Packet Flow Data.
04. Guardar y aplicar la regla; establecer un nuevo flujo de prueba que coincida con ella.
05. Confirmar en el colector que aparecen los registros de esa comunicación y que los no seleccionados no se exportan por defecto.
06. Usar Never track en una regla concreta solo cuando exista un criterio documentado para excluirla.

33.23. Procedimiento C: migrar de NetFlow v5 a IPFIX

01. Inventariar compatibilidad, retención, identificadores y filtros del colector actual.
02. Preparar un receptor que pueda interpretar las plantillas y los elementos de IPFIX.
03. Añadir un exportador IPFIX de prueba sin modificar la política de filtrado de usuarios.
04. Comprobar la recepción de flujos IPv4 y, donde exista conectividad, IPv6 mediante nuevas conexiones.
05. Comparar recuentos en una ventana controlada y revisar la interpretación de información NAT44 si aplica.
06. Tras validar la migración, deshabilitar y posteriormente retirar el exportador obsoleto con registro de cambio.

33.24. Validar el envío: cuatro niveles de comprobación



Figura 33.3. Cadena de comprobaciones sin alterar de manera masiva las conexiones existentes.

Nivel	Prueba	Interpretación
Configuración	Enable activo, exportador habilitado y parámetros guardados.	Si falla, no hay un origen exportador operativo.
Estados PF	Conexión nueva permitida y visible en Diagnostics → States.	Sin estado o sin seguimiento no habrá flujo exportable.
Tránsito	Captura temporal controlada en la ruta al colector, filtrando por su puerto UDP.	Confirma salida o llegada; no verifica la interpretación de datos.
Colector	Servicio escuchando, recibe y decodifica registros de protocolo correcto.	Valida recepción efectiva y posterior consulta.
Integridad	Revisar dirección de origen, tiempo, volumen y campos NAT disponibles.	Permite detectar registros asociados incorrectamente.

33.25. Diagnóstico en pfSense y en el receptor

Para comprobar el estado de la comunicación puede utilizarse Diagnostics → States, filtrando por extremos de la conexión de ensayo. Si hace falta confirmar paquetes de exportación, una captura puntual en Diagnostics → Packet Capture puede comprobar tráfico UDP hacia el destino del colector, utilizando la interfaz por la que realmente sale. Las herramientas de captura pueden tener restricciones de visualización y deben reservarse para tareas de soporte autorizadas.

La presencia de datagramas de exportación no demuestra por sí sola que el colector interprete las plantillas. Revisar que el listener está activo, que el protocolo corresponde al esperado, que su puerto coincide con el configurado y que los relojes se encuentran sincronizados. Si no aparecen registros de una sesión ya establecida, repetir con una conexión nueva antes de reiniciar servicios.

33.26. Incidencias habituales y su resolución

Síntoma	Posible causa	Comprobación o corrección
No aparece ningún flujo	Enable global desactivado.	Habilitar, guardar y confirmar configuración aplicada.
Hay tráfico, pero no flujos	Track by Default apagado sin Always por regla.	Revisar matriz de seguimiento y regla concreta.
La conexión funciona, pero no se exporta	Estado previo al cambio o regla sin estado.	Probar con conexión nueva; revisar State Type.
El colector no recibe	Origen sin ruta, UDP filtrado o destino erróneo.	Revisar rutas, source IP, destino y puerto.

Síntoma	Posible causa	Comprobación o corrección
Recibe paquetes, pero no muestra datos	Formato incompatible o receptor mal configurado.	Verificar NetFlow v5/IPFIX y capacidad de decodificación.
Faltan flujos IPv6	Elección de NetFlow v5.	Utilizar IPFIX con colector compatible.
Falla un Source Port fijo	Colisión con otro servicio o falta Source IP específica.	Dejar puerto origen en blanco o revisar asignación.
Informes confusos de varios equipos	Observation Domain no coordinado.	Revisar separación de orígenes y configuración del receptor.
Se siguen viendo datos tras desactivar	Estados preexistentes aún activos.	Esperar finalización normal o programar limpieza justificada.

33.27. Escenario empresarial: control de utilización de enlaces

Una organización desea identificar qué grupos de comunicación generan carga y en qué franjas se utiliza una conexión. La captura agregada de flujos puede alimentar gráficos por origen, destino, protocolo y ventana temporal. Es un complemento de la monitorización de ancho de banda: las cifras pueden diferir de los contadores físicos por criterios de estado, muestreo del receptor y precisión temporal. Para una visión de todo el enlace conviene correlacionar con métricas de interfaz y no asumir equivalencia exacta.

33.28. Escenario empresarial: investigación de comunicaciones anómalas

En una revisión autorizada, un colector permite agrupar destinos frecuentes, conversaciones atípicas y variaciones de volumen en servicios permitidos. El análisis de flujos aporta contexto técnico, pero no prueba por sí solo que exista un incidente ni revela los contenidos cifrados. Debe correlacionarse con DNS, reglas, logs, endpoint y otras fuentes de observabilidad conforme a las políticas internas de seguridad.

33.29. Escenario empresarial: consolidación de varios firewalls

Cuando varias pasarelas exportan al mismo recolector, el esquema de direcciones de origen, Observation Domain, zonas de red y convenciones de etiquetas debe quedar definido previamente. Pueden emplearse varios exportadores para una migración o un colector de contingencia, aunque esto multiplica el tráfico de telemetría. El receptor necesita separar correctamente registros y aplicar retención y accesos por función.

33.30. Rendimiento, dimensionamiento y administración

La exportación nativa aprovecha los estados PF y evita instalar un proceso de captura independiente, pero no es gratuita: consume recursos del firewall y ancho de banda hacia los colectores, con mayor impacto potencial a medida que crecen las conexiones nuevas y los destinos de exportación. Evaluar el crecimiento de la tabla de estados, el procesamiento del colector, su almacenamiento y la velocidad de llegada de registros.

El volumen depende de la actividad, no únicamente del número de interfaces. Para implantaciones importantes, comenzar por seguimiento selectivo en una ventana de medición, revisar resultados y ampliar gradualmente. La activación no altera las reglas de permiso, pero puede afectar al rendimiento si el equipo está cerca de sus límites. Comprobar métricas antes y después.

33.31. Seguridad del colector y confidencialidad de los metadatos

Los metadatos de flujos revelan relaciones entre dispositivos, horarios de comunicación, servicios utilizados y volúmenes; pueden contener información sensible de actividad empresarial o personal aunque no incorporen el contenido de paquetes. Definir finalidad, base organizativa de tratamiento, accesos limitados, conservación, eliminación y procedimientos de auditoría.

Se recomienda que el colector esté en una red de gestión protegida, con reglas de recepción restrictivas, almacenamiento protegido y autenticación independiente para consultar los datos. NetFlow v5 e IPFIX exportados de esta forma no deben tratarse como un canal cifrado por defecto: si se envía a través de redes no confiables, proteger el tránsito con una VPN o transporte seguro de red adecuado.

33.32. Qué no resuelve Packet Flow Data

No equivale a…	Por qué
Packet Capture / PCAP	No guarda todos los paquetes ni su carga útil íntegra.
Firewall Rules	No permite ni bloquea conexiones; solo sigue estados sujetos a política.
Syslog de seguridad	No sustituye eventos de bloqueo o motivos de reglas.
IDS/IPS	No realiza por sí solo detección o bloqueo por firmas de amenazas.
Monitorización L2	No observa indiscriminadamente todo lo que circula por un switch.
Cálculo exacto de facturación	Los criterios de cobertura, cierre de estado y formato deben validarse.
Inventario de aplicaciones	Puertos y flujos no bastan para identificar con certeza aplicaciones.

33.33. Cambio seguro, reversión y recuperación

01. Exportar copia de configuración y documentar valores globales y exportadores afectados.
02. Identificar colector, cambios de destino y volumen esperado, y preparar plan de prueba.
03. Deshabilitar primero el exportador específico si el problema afecta a un único destino.
04. Deshabilitar Enable global si se necesita detener la exportación global; guardar y aplicar.
05. Comprobar el estado de las sesiones existentes antes de interpretar la ausencia de tráfico exportado.
06. No reiniciar ni restablecer todos los estados salvo autorización explícita y ventana de mantenimiento.
07. Validar que se han recuperado los recursos esperados y registrar el resultado.

33.34. Lista de aceptación para la implantación

Control	Criterio de aceptación
Versión	pfSense Plus 24.03+ verificado.
Objetivo	Se conoce qué se observa y por qué.
Alcance	Política global y excepciones por regla documentadas.
Estados	Las reglas de prueba crean estado y se usan flujos nuevos.
Exportador	Fuente, destino, puertos y formato validados.
Colector	Listener activo; decodificación y retención confirmadas.
IPv6	IPFIX seleccionado si se necesitan flujos IPv6.
Seguridad	Rutas protegidas y permisos de acceso al repositorio revisados.
Rendimiento	Recursos y ancho de banda evaluados antes/después.
Reversión	Copia, responsable y modo de desactivación previstos.

33.35. Glosario técnico

Término	Definición operativa
PF	Motor de filtrado de paquetes y seguimiento de estados.
pflow(4)	Mecanismo nativo que exporta información de flujos desde PF.
NetFlow v5	Formato heredado de exportación de flujos IPv4.
IPFIX	Estándar flexible de exportación de información de flujos, compatible con IPv6.
Exporter	Configuración del origen que envía datos a un colector.
Collector	Sistema que recibe y almacena registros de flujo.

Término	Definición operativa
Observation Domain	Identificador lógico para distinguir la procedencia de flujos.
State / estado	Entrada mantenida por el firewall para una conexión o comunicación.
Keep State	Tipo de regla que permite crear registros de conexión.
NAT44	Traducción de direcciones IPv4; IPFIX admite información específica conforme a RFC 8158.
Telemetría	Mediciones técnicas utilizadas para supervisión y análisis operativo.

33.36. Referencias oficiales y criterios de interpretación

Las definiciones y límites de campos se han contrastado con Netgate. La vista principal presenta los controles globales y el resumen de exportadores; el formulario de alta y las opciones avanzadas de las reglas se documentan en sus apartados correspondientes. La presentación concreta de controles puede variar según la versión de pfSense Plus.

01. Firewall Packet Flow Data — Netgate. https://docs.netgate.com/pfsense/en/latest/firewall/pflow.html

02. Configuring Firewall Rules / Packet Flow Data — Netgate.
https://docs.netgate.com/pfsense/en/latest/firewall/configure.html

03. Firewall Fundamentals / Stateful Filtering — Netgate.
https://docs.netgate.com/pfsense/en/latest/firewall/fundamentals.html

04. Viewing Firewall States in the GUI — Netgate.
https://docs.netgate.com/pfsense/en/latest/monitoring/status/firewall-states-gui.html

05. Monitoring Bandwidth Usage — Netgate.
https://docs.netgate.com/pfsense/en/latest/monitoring/graphs/bandwidth-usage.html

06. Reset State Table — Netgate. https://docs.netgate.com/pfsense/en/latest/monitoring/status/firewall-states-reset.html

07. Release Notes pfSense Plus 24.03 — Netgate.
https://docs.netgate.com/pfsense/en/latest/releases/rn-plus-24-03.html

08. RFC 7011 — Specification of IPFIX. https://www.rfc-editor.org/rfc/rfc7011

09. RFC 8158 — IPFIX Information Elements for NAT. https://www.rfc-editor.org/rfc/rfc8158

34 Firewall → Rules

Pestañas de filtrado · Editor de reglas · Estados · Orden de evaluación · Seguridad y diagnóstico

Ruta de acceso: Firewall → Rules. El editor se abre al crear una regla o pulsar Edit sobre una existente. El capítulo explica las seis vistas observadas —Floating, WireGuard, WAN, LAN, WAN secundaria y OpenVPN— y los campos visibles del formulario. Se desarrolla aparte el catálogo de opciones condicionales y avanzadas documentadas por Netgate, cuya presentación puede variar según versión, tipo de regla y protocolo.



Figura 34.1. Ruta conceptual de evaluación para paquetes nuevos sin estado previo.

34.1. Finalidad y alcance del filtrado en pfSense Plus

Las reglas definen qué comunicaciones pueden atravesar el firewall o alcanzar sus propios servicios. El administrador decide acción, protocolo, familia IP, origen y destino; opcionalmente añade puertos, horarios, pasarelas, límites y registro. El control es con estado por defecto: una regla Pass que crea estado permite el retorno de la sesión sin otra regla simétrica.

Una regla no sustituye el enrutamiento, NAT ni el control de servicios. Una comunicación puede estar permitida por las reglas y fallar por ausencia de ruta, gateway, negociación VPN, DNS, servicio de escucha o traducción adecuada. El diseño profesional combina todos esos elementos.

34.2. Cómo interpreta pfSense el tráfico: entrada, estado y prioridad

Las reglas en pestañas de interfaz se examinan normalmente sobre los paquetes que ENTRAN por ella. Una conexión iniciada desde un equipo LAN se controla al entrar en LAN; si el destino responde, los paquetes de retorno suelen coincidir con un estado previamente creado. Una conexión nueva desde Internet se decide sobre la WAN por la que llega.

Para una conexión nueva, el orden funcional general es: reglas flotantes aplicables, reglas de grupo (incluidas las pestañas de grupos VPN) y reglas de interfaz. Las reglas normales se recorren de arriba abajo y la primera coincidencia decisiva se aplica. Las flotantes sin Quick presentan semántica especial y no deben confundirse con esa regla general.

Precaución. Modificar un permiso puede no afectar de inmediato a sesiones ya establecidas. Eliminar estados masivamente corta conexiones activas; se reserva para cambios controlados y no es un paso normal del alta de una regla.

34.3. Las seis pestañas de la vista Rules

Pestaña	Qué tráfico examina	Para qué se emplea
Floating	Paquetes en una o varias interfaces, entrada y/o salida.	Control global especializado, tagging, shaping o coincidencias salientes.

Pestaña	Qué tráfico examina	Para qué se emplea
WireGuard	Tráfico interior de túneles WireGuard según grupo.	Autorizar destinos accesibles a través de la VPN.
WAN	Tráfico que entra por una conexión externa principal.	Publicaciones, acceso a servicios, restricciones de origen.
LAN	Tráfico iniciado desde equipos o redes de la LAN.	Control de salida, acceso entre segmentos y al propio firewall.
WAN secundaria	Tráfico entrante por una segunda conexión externa.	Accesos autorizados por el enlace alternativo y retorno correcto.
OpenVPN	Tráfico interior de instancias OpenVPN según grupo.	Permitir solo redes, equipos y aplicaciones necesarios.



Figura 34.2. Ámbito de las pestañas y diferencia entre interfaz y grupo VPN.

34.4. Floating: reglas flotantes y control avanzado

Floating es una pestaña especial que puede actuar en múltiples interfaces y en sentido in, out o any. Incluye la acción Match, pensada para aplicar características como colas y etiquetado sin tomar por sí misma una decisión Pass o Block. Quick determina cuándo se detiene el análisis: con Quick una coincidencia decisiva prevalece; sin Quick la evaluación de reglas flotantes puede usar la última coincidencia, lo que exige un diseño cuidadoso.

El filtrado out en una WAN se evalúa después de NAT saliente, por lo que el origen ya puede ser la dirección traducida. Para distinguir hosts internos en ese punto pueden utilizarse Tag y Tagged. En conexiones mult-WAN, una regla flotante o de grupo no recibe automáticamente el mismo tratamiento reply-to que la regla de una WAN concreta.

Recomendación. Priorizar reglas de interfaz para escenarios ordinarios. Utilizar Floating únicamente cuando exista una necesidad explícita, un mapa del flujo y pruebas de retorno.

34.5. WireGuard: tráfico del túnel frente a tráfico de transporte

El tráfico cifrado para establecer WireGuard llega desde Internet al puerto UDP de escucha y requiere el permiso pertinente en la WAN receptora. Una vez descifrado, los paquetes interiores se controlan con reglas de la pestaña WireGuard o de una interfaz WireGuard asignada. Son dos filtros diferentes: permitir el UDP exterior no autoriza automáticamente el acceso a la red interior.

Una regla de la pestaña de grupo WireGuard se examina antes que la de una interfaz VPN asignada. Si el grupo incluye una regla genérica que permite todo, una restricción posterior de la interfaz asignada puede no llegar a evaluarse. Para distinguir túneles o mantener el retorno por el mismo túnel, puede ser preferible la pestaña de la interfaz asignada, con el uso de reply-to cuando procede.

34.6. WAN: conexiones iniciadas desde el exterior

La pestaña WAN contiene permisos explícitos para conexiones que llegan desde fuera. De manera habitual no se permite ninguna conexión nueva entrante hasta que exista una regla adecuada. Si se activan en la interfaz las opciones de bloqueo de redes privadas y bogon, aparecen reglas automáticas representadas en la lista con su acción y contadores. No son permisos de administración creados por el usuario.

El engranaje de algunas entradas automáticas conduce a la configuración que controla su existencia, no a un formulario ordinario para reordenarlas. En conexiones entrantes con NAT Port Forward, además de la traducción debe existir una política de filtrado o un modo expresamente configurado para permitirlas. Aplicar el mínimo privilegio: solo protocolo, destino, puerto y origen necesarios.

34.7. LAN: permisos salientes y protección de la administración

En una instalación de referencia pueden aparecer reglas por defecto que permiten tráfico IPv4 e IPv6 desde LAN a cualquier destino y una regla automática Anti-Lockout para mantener el acceso a los servicios de administración del propio firewall. Son ejemplos de comportamiento inicial, no una política empresarial recomendada a largo plazo. La política debe ajustarse a los segmentos, aplicaciones y equipos autorizados.

Anti-Lockout se gobierna por configuración administrativa; deshabilitarla sin haber creado permisos equivalentes para equipos de gestión puede dejar inaccesible la interfaz web o SSH. Antes de implantar denegación de salida, asegurar primero los servicios esenciales: DNS, DHCP cuando corresponda, tiempo, administración, autenticación, actualización y servicios corporativos aprobados.

34.8. WAN secundaria: reglas propias y simetría de retorno

Una WAN alternativa dispone de su propia pestaña y reglas para conexiones nuevas que entren a través de ella. No existe herencia automática de permisos desde la WAN principal. Para tráfico publicado, verificar también gateway, regla NAT, dirección de escucha, origen admitido, monitorización y posibilidad real de conexiones entrantes; algunos accesos móviles o privados no admiten publicación directa.

Las reglas de interfaz WAN pueden incorporar reply-to para forzar que las respuestas regresen por el enlace que recibió la conexión. Evitar trasladar indiscriminadamente estos permisos a un grupo multi-WAN o a Floating, donde la gestión del retorno puede ser distinta.

34.9. OpenVPN: entrada descifrada y reglas de grupo

La pestaña OpenVPN controla el tráfico interior descifrado de instancias OpenVPN. Una regla de permiso amplia se aplica a los túneles cubiertos por esa pestaña; en escenarios de varios grupos de usuarios o distintas sedes puede ser más seguro crear reglas específicas y, cuando convenga, utilizar pestañas de interfaces OpenVPN asignadas.

Para permitir que un cliente llegue a un servidor OpenVPN expuesto al exterior, la WAN necesita el permiso sobre el puerto/protocolo de escucha. La regla OpenVPN interior autoriza posteriormente las conexiones desde la VPN a recursos corporativos. En interfaces OpenVPN asignadas, la pestaña de grupo OpenVPN se evalúa antes de la pestaña de la instancia asignada; el diseño debe evitar reglas generales que anulen restricciones específicas.

34.10. Leer la tabla Rules (Drag to Change Order)

Columna / elemento	Significado y comprobación
Selección	Casilla para seleccionar varias filas antes de copiar, borrar, mover o cambiar estado.
Indicador de acción	Marca Pass, Block o Reject; puede aparecer atenuado si la regla está inactiva.
States	Cantidad de estados activos creados por la regla y volumen asociado; permite abrir detalle.
Protocol	Protocolo IP; * indica cualquier protocolo compatible con el ámbito de la regla.
Source / Port	Origen de la comunicación y puerto de origen si aplica; * indica sin restricción.

Columna / elemento	Significado y comprobación
Destination / Port	Destino y puerto de destino; puede mostrar macros o alias.
Gateway	Pasarela o grupo elegido por policy routing, si se ha configurado.
Queue	Cola de tráfico asociada, cuando se utiliza shaping/ALTQ.
Schedule	Horario que determina en qué periodos puede coincidir la regla.
Description	Texto administrativo que ayuda a reconocer el propósito.
Actions	Iconos de mover, editar, duplicar, alternar, eliminar y limpiar estados cuando proceda.

34.11. Estados, contadores, iconos y métricas operativas

States muestra el número de conexiones activas asociadas a la regla y el volumen registrado para esas conexiones. Al posicionarse sobre el contador pueden verse evaluaciones, paquetes, bytes, estados y estados creados; al pulsar el valor se consulta el detalle de estados. Estos contadores pueden reiniciarse o cambiar por recargas del conjunto de reglas y no constituyen por sí mismos una auditoría histórica.

Los iconos de acción identifican permitir (marca de verificación), bloquear (cruz), rechazar, registro activado y opciones avanzadas. Los iconos de reglas automáticas o generadas por el sistema pueden variar respecto de las filas editables. Los asteriscos de columnas indican coincidencia amplia, no que el valor carezca de efecto.

34.12. Botones y acciones de administración de la lista

Control	Resultado	Riesgo o precaución
Add superior	Crea regla nueva al inicio del listado actual.	Una coincidencia temprana puede prevalecer sobre otras.
Add inferior	Crea regla nueva al final del listado.	Puede quedar inalcanzable si otra anterior captura el tráfico.
Edit (lápiz)	Abre el formulario de una regla existente.	Cambiar Interface puede mover la regla de pestaña.
Copy / duplicar	Clona una regla como punto de partida o copia seleccionadas.	Revisar origen, interfaz, dirección y orden del destino.
Toggle	Desactiva/activa una o varias reglas.	Puede interrumpir el establecimiento de conexiones nuevas.
Delete	Elimina las reglas seleccionadas, previa confirmación.	No confundir una prueba temporal con una eliminación definitiva.
Save en la lista	Persiste cambios de orden y separadores.	No abandonar sin guardar tras arrastrar.
Separator	Inserta etiqueta visual entre grupos de reglas.	No permite ni bloquea tráfico.
Ancla	Desplaza filas seleccionadas a una posición de la lista.	Puede cambiar precedencia de los permisos.
Borrar estados (X)	Elimina estados creados por la regla según ámbito soportado.	Puede cortar sesiones; no equivale a desactivar la regla.
Engranaje automático	Abre configuración asociada a una regla generada.	Su comportamiento difiere del editor normal.
Apply Changes	Carga los cambios pendientes en el motor de filtrado.	Confirmar la conectividad inmediatamente después.

34.13. Orden de reglas, primera coincidencia y separadores

En las listas habituales, la regla superior tiene prioridad frente a otra inferior para el mismo tráfico. Un Block que coincide antes que un Pass bloquea la conexión; un Pass amplio al comienzo puede impedir que se

alcance una denegación posterior. Para mover reglas se puede arrastrar y guardar el orden o seleccionar filas y usar el ancla. Los separadores son ornamentales y documentales: no modifican la evaluación.

01. Identificar el flujo por interfaz de entrada, protocolo, dirección de origen/destino y puerto.
02. Detectar reglas preexistentes que puedan coincidir antes de la regla nueva.
03. Crear la regla más específica y situarla por encima de los permisos generales que la ocultarían.
04. Guardar el orden y aplicar los cambios, si el sistema lo solicita.
05. Probar una conexión nueva y revisar estados y eventos de la regla correcta.

34.14. Avisos de reglas automáticas y bloqueo implícito

Un aviso de que no hay reglas definidas por el usuario en una pestaña WAN no significa que el firewall carezca de toda protección o que el tráfico quede permitido: el comportamiento habitual para nuevas conexiones que no coinciden con una autorización es el bloqueo implícito. Reglas de redes privadas, bogons o Anti-Lockout pueden aparecer como entradas automáticas según la configuración.

El bloqueo implícito por defecto no es equivalente a Reject: normalmente descarta paquetes. Un registro de denegación tampoco demuestra por sí solo que exista una regla manual Block, pues puede proceder de una regla automática o de la política final.

34.15. Acceso al formulario Edit Firewall Rule

Se abre desde Firewall → Rules, seleccionando la pestaña correspondiente y pulsando el lápiz de la fila. Al crear una regla desde Add se muestra un formulario similar, aunque no contiene necesariamente historial de creación. Sus apartados básicos son Action, Disabled, Interface, Address Family, Protocol, Source, Destination, Extra Options, Advanced Options y Rule Information.

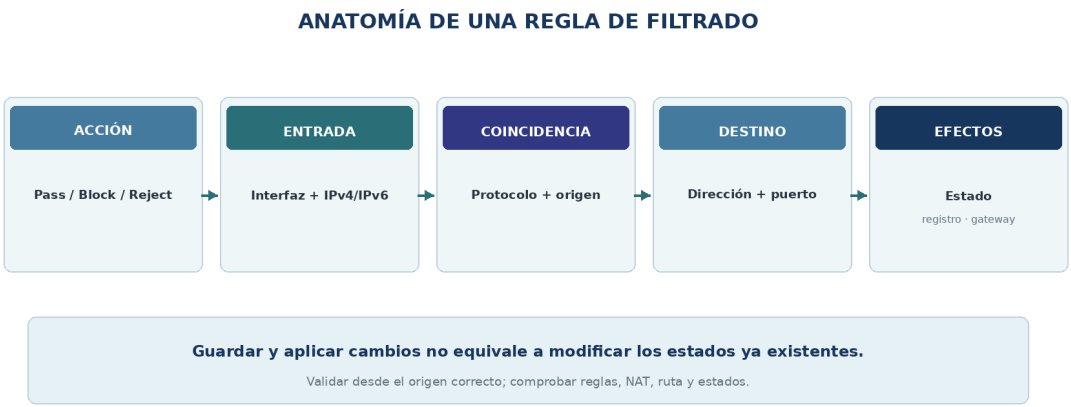


Figura 34.3. Cinco decisiones fundamentales que componen una regla.

34.16. Action: Pass, Block y Reject

Acción	Qué hace	Cuándo conviene
Pass	Permite paquetes coincidentes; por defecto puede establecer estado para el retorno.	Conceder acceso estrictamente necesario.
Block	Descarta silenciosamente el paquete original.	Política de denegación no informativa y filtrado perimetral.
Reject	Descarta y devuelve respuesta de rechazo compatible (por ejemplo, TCP RST o ICMP).	Algunos rechazos internos donde se desea error inmediato.

Reject puede acelerar la notificación al cliente de que un servicio no está disponible, pero también revela una respuesta explícita. Tanto Reject como Block descartan el paquete original. Para tráfico ajeno a TCP/UDP, la respuesta concreta depende del protocolo y del soporte del motor de filtrado.

34.17. Disabled: conservar la regla sin aplicarla

Disable this rule mantiene el objeto en la lista, pero impide que coincida con conexiones nuevas. Es útil para ventanas de mantenimiento y pruebas reversibles. Una regla desactivada no es lo mismo que una regla que bloquea; además, las conexiones con estado previo pueden mantener su comportamiento hasta que expiren o se eliminen sus estados.

34.18. Interface: interfaz de entrada y cambio de pestaña

Este selector determina el ámbito de entrada que debe coincidir. La interfaz puede ofrecer WAN, LAN, OpenVPN, WireGuard e interfaces opcionales o secundarias. Sus etiquetas son configurables por el administrador. Cambiar la interfaz en una regla de interfaz normalmente traslada la regla a la pestaña seleccionada.

Antes de elegir se debe responder: «¿por cuál interfaz entra por primera vez el tráfico iniciado desde el origen?». No es correcto elegir WAN simplemente porque el destino final sea Internet: para una conexión iniciada en LAN, la regla suele pertenecer a LAN.

34.19. Address Family: IPv4, IPv6 e IPv4+IPv6

IPv4 solo examina tráfico IPv4; IPv6, solo IPv6; IPv4+IPv6 permite una regla compatible con ambas familias. Un alias mixto se resolverá con entradas apropiadas a cada familia. No puede asumirse que tener una regla IPv4 autorice IPv6: deben revisarse ambas políticas, en especial cuando se usa delegación de prefijos.

Según la versión y la selección, pueden aparecer controles condicionales como Enable NAT64 al escoger IPv6, con parámetros de traducción específicos. Comprobar su disponibilidad y requisitos en la versión instalada.

34.20. Protocol: catálogo de opciones y particularidades

Protocolo	Cuándo se aplica y qué implica
Any	Todos los protocolos IP elegibles; no restringe a TCP.
TCP	Conexiones TCP y puertos; control de banderas y estados.
UDP	Datagramas UDP y puertos; DNS, QUIC, VPN u otras aplicaciones.
TCP/UDP	Coincidencia combinada de ambos protocolos en una regla.
ICMP	Mensajes de diagnóstico/control; puede mostrar subtipos de ICMP.
ESP / AH	Protocolos de seguridad IPsec, sin puertos TCP/UDP.
GRE / EoIP	Encapsulación de túneles; no equivale a abrir un puerto web.
IPV6	Número de protocolo IP-in-IP IPv6; no significa «todo IPv6».
IGMP / PIM	Control de grupos y enrutamiento multicast.
OSPF	Protocolo de enrutamiento dinámico.
SCTP	Transporte con puertos y características propias.
CARP / PFSYNC	Funciones de redundancia y sincronización de estados en escenarios HA.

La lista exacta de nombres disponibles depende de la versión. Los campos de puertos aparecen para protocolos que tienen puertos —TCP, UDP y SCTP, entre otros contextos—; para ICMP se muestran normalmente subtipos. No se deben crear reglas genéricas Any cuando basta permitir un protocolo y un puerto concreto.

34.21. Source: tipos de coincidencia y selección

Source identifica la dirección o red desde la cual se origina la comunicación. El selector puede incorporar Any, Address or Alias, Network, familias de clientes de acceso remoto (PPTP, PPPoE, L2TP cuando se

emplean), dirección de cada interfaz y subredes conectadas de cada interfaz. Un alias puede representar conjuntos de hosts o redes gestionados de manera centralizada.

Tipo de fuente	Efecto de la coincidencia
Any	Acepta cualquier dirección de origen compatible con la familia de la regla.
Address or Alias	IP individual o alias con entradas de host/red compatibles.
Network + /prefijo	Red CIDR específica; el desplegable /0.../32 corresponde a longitud IPv4.
Clientes VPN/PPP de servidor	Coincidencia con rango de clientes de un servicio de acceso remoto aplicable.
Interfaz Address	Dirección o direcciones propias configuradas en una interfaz de pfSense.
Interfaz Subnets	Redes directamente configuradas en esa interfaz, no cualquier destino alcanzable a través de ella.

La etiqueta «WAN subnets» NO significa Internet; representa las redes directamente asociadas a la WAN, incluida la repercusión de VIP. «LAN address» es la dirección del propio firewall en LAN, no el conjunto de ordenadores de la LAN. Esta distinción es esencial al definir permisos.

34.22. Source → Invert match y máscara CIDR

Invert match invierte la condición: la regla coincide con orígenes que NO pertenecen al objeto elegido. Es potente, pero puede producir efectos inesperados cuando se usa con macros de subred e IP virtuales. Debe explicitarse en la descripción, revisarse la expansión del alias y probarse tráfico permitido y excluido.

El selector de prefijo /32 representa un solo host IPv4; /24 representa una red con 256 direcciones nominales; /0 cubre todo el espacio de direcciones IPv4. Para IPv6 se usan longitudes de prefijo IPv6 según la configuración elegida. Evitar más amplitud de la imprescindible.

34.23. Source Port Range: por qué normalmente se deja Any

Para TCP/UDP los clientes suelen abrir conexiones desde puertos efímeros; por eso Source Port Range se deja normalmente Any. Limitar el puerto de origen al número del servicio (por ejemplo, «HTTPS») es un error habitual: el puerto 443 suele ser destino del servidor, no origen del navegador. El campo de puerto de origen puede estar oculto tras Display Advanced dentro de Source.

34.24. Destination: Any, direcciones, redes y This Firewall (self)

Destination define el destinatario: Any, Address or Alias, Network, direcciones/subredes asociadas a interfaces y This Firewall (self), entre otros valores que correspondan a la configuración. «This Firewall (self)» abarca las direcciones del dispositivo; no es equivalente a una única interfaz ni a todas las máquinas protegidas.

En una regla de acceso administrativo, usar como destino el propio firewall (o su dirección concreta) y únicamente el puerto necesario es más preciso que permitir tráfico a Any. En comunicaciones entre redes, el destino debe ser la red/host real y la decisión debe tomarse en la interfaz por la que entra el origen.

34.25. Destination → Invert match, puerto y rango

Invert match en Destination coincide con destinos que no pertenezcan al conjunto seleccionado. Hay que recordar que un alias, una macro de subred o un grupo de IP virtuales puede contener elementos no evidentes a simple vista. El campo Destination Port Range se muestra para transportes con puertos y suele permitir un único puerto o un intervalo From–To inclusivo; para varios valores discontinuos conviene un alias de puertos.

No sustituir erróneamente «puerto de destino» por «puerto de origen». Las reglas que cruzan NAT Port Forward se evalúan de acuerdo con el orden de procesamiento de NAT y filtrado; comprobar el destino traducido cuando se diagnostica una coincidencia.

34.26. Extra Options: Log y Description

Log packets that are handled by this rule crea un evento cuando un paquete coincide con la regla según la política de registro. Es recomendable para bloqueos críticos, accesos sensibles y pruebas con alcance delimitado. Registrar absolutamente todo consume almacenamiento, CPU y recursos del servicio syslog; considerar un recolector remoto autorizado para necesidades de conservación.

Description documenta el objetivo, servicio y razón de la regla sin afectar a la coincidencia. La documentación de Netgate establece un límite de 52 caracteres para la descripción. Utilizar una etiqueta breve y clara, y conservar el detalle administrativo en la documentación de cambios.

34.27. Advanced Options: acceso y naturaleza condicional

Display Advanced despliega ajustes especializados. Algunos controles solo aparecen para determinados protocolos, familias IP, tipos de interfaz o versiones compatibles. Los apartados siguientes explican su función y las condiciones que deben verificarse antes de utilizarlos.

34.28. Advanced Options: reconocimiento de tráfico y etiquetado

Opción documentada	Función	Criterio de utilización
Source OS	Intenta identificar sistema operativo por huella TCP pasiva p0f.	No confiar como autenticación: la huella puede falsificarse.
Diffserv Code Point	Coincide con el valor DSCP recibido en cabecera IP.	No marca DSCP; requiere control desde origen.
IP Options	Permite coincidencia con paquetes que contienen opciones IP.	Casos específicos, por ejemplo tráfico multicast.
Disable Reply-To	Evita reply-to automático de reglas WAN específicas.	Solo con necesidad fundada de enrutamiento especial.
Tag / Tagged	Marca paquetes y filtra según marca en otras reglas.	Asociación con Floating y shaping posterior a NAT.
VLAN Priority Match / Set	Coincide o establece prioridades PCP 802.1p.	Solo en entornos VLAN y equipos compatibles.

34.29. Advanced Options: límites y protección de estados

Control	Qué limita / modifica	Advertencia
Maximum state entries	Total de estados que esta regla puede crear.	La regla puede dejar de coincidir cuando llega al límite.
Maximum unique source nodes	Cantidad de orígenes únicos con estados.	No equivale a estados máximos por host.
Maximum established connections per host	Conexiones TCP establecidas por origen.	Aplicable cuando el protocolo y estado lo permiten.
Maximum state entries per host	Estados por origen independientemente de fase.	Control útil ante exceso de conexiones.
Maximum new connections / per second	Tasa de nuevas sesiones TCP por origen.	Un umbral demasiado bajo bloquea tráfico legítimo.
State timeout in seconds	Tiempo de inactividad antes de caducar estados.	Un valor corto puede cortar aplicaciones persistentes.
TCP Flags	Banderas que deben estar activas y conjunto evaluado.	Requiere conocimiento de handshake TCP.
No pfsync	Evita sincronizar estados de la regla con HA.	Riesgo de pérdida de sesiones durante failover.

34.30. Advanced Options: State Policy y State Type

State Policy permite mantener el valor global o elegir estados vinculados a interfaz (Interface Bound States) o flotantes (Floating States). Cambia dónde puede reutilizarse una entrada de estado, importante para rutas asimétricas. Debe evaluarse con HA, VPN y múltiples WAN, no establecerse indiscriminadamente.

State Type	Comportamiento práctico
Keep	Crea y mantiene estado; opción por defecto recomendada.
Sloppy State	Reduce comprobaciones estrictas para situaciones de enrutamiento asimétrico; menor protección.
Synproxy	PF interviene en el saludo inicial TCP; puede reducir rendimiento y compatibilidad de extensiones.
None	No crea estados; caso avanzado que exige comprobar el tráfico de retorno y las reglas de salida.

Para tráfico que sale por otra interfaz, una política de estado aplicada solo a la regla de entrada puede no ser suficiente en configuraciones avanzadas; Netgate recomienda cautela y puede requerir reglas flotantes complementarias.

34.31. Advanced Options: reglas temporales, gateway, shaping y Packet Flow Data

Control	Uso correcto
Packet Flow Data	Use global default / Always track / Never track para estados creados; solo pfSense Plus 24.03+.
No XMLRPC Sync	Impide sincronizar esta regla con nodos HA por XMLRPC; distinto de No pfsync.
Schedule	Limita la coincidencia a días y horas configurados; fuera de horario se omite la regla.
Gateway	Enrutamiento por política (policy routing), incluyendo gateways y grupos si existen.
In/Out Pipe (Limiters)	Asigna límites de ancho de banda a flujo entrante/saliente en la interfaz.
Ackqueue / Queue	Utiliza colas de traffic shaping compatibles con ALTQ.
VLAN Priority Match / Set	Coincidencia y modificación de prioridad 802.1p, cuando exista compatibilidad.

La elección de Gateway en una regla de LAN no es una orden global sobre toda la red: enruta conexiones que coinciden con esa regla. Una regla que fuerza la salida por WAN no debería capturar sin excepciones tráfico destinado a VPN o redes internas. En Multi-WAN hay que revisar también rutas, NAT, respuestas y comportamiento de estados.

34.32. Rule Information: Tracking ID, Created y Updated

Tracking ID es un identificador asignado por el sistema para correlacionar una regla con el conjunto de reglas y sus registros; no está pensado para ser modificado. Created y Updated muestran metadatos de auditoría relativos al alta y las modificaciones: fecha, usuario y fuente administrativa, según los datos almacenados por pfSense.

Estos metadatos son sensibles en una publicación porque pueden revelar identidad administrativa, equipos o momentos de intervención. Los ejemplos editoriales deben limitarse a nombres de campo y explicación de su uso; nunca copiar valores de una instalación real. No todos los objetos de reglas automáticas mantienen identificadores inmutables entre recargas.

34.33. Procedimiento 1: crear un permiso mínimo en una LAN

01. Definir la necesidad de acceso, origen, destino, puerto, protocolo, responsable y plazo de revisión.
02. Confirmar por qué interfaz entra la conexión iniciada por el cliente. Seleccionar esa pestaña en Firewall → Rules.
03. Pulsar Add superior o inferior según el orden necesario y escoger Action = Pass; mantener Enabled.
04. Indicar Address Family, Protocol, Source y Destination con redes o alias apropiados.
05. Introducir Destination Port Range cuando el protocolo lo admita; dejar Source Port en Any salvo motivo técnico.
06. Anotar Description breve y activar Log durante la validación si es apropiado.

07. Comprobar opciones avanzadas: sin gateway alternativo si se requiere ruta normal; State Type por defecto.
08. Guardar, aplicar y situar la regla antes de permisos más amplios que podrían capturar esa conexión.
09. Iniciar una conexión nueva y verificar servicio, registro, contadores y ruta de retorno.
10. Documentar aprobación y revisión, y retirar permisos temporales al concluir su necesidad.

34.34. Procedimiento 2: publicar un servicio mediante WAN y NAT

01. Confirmar disponibilidad del servicio, exposición autorizada y medidas de autenticación/cifrado.
02. Configurar Firewall → NAT → Port Forward para el destino y puerto previstos, cuando proceda.
03. Verificar que exista una regla de filtrado que permita la conexión externa; no confundir NAT con permiso.
04. Restringir el origen cuando sea viable; elegir dirección/puerto de destino coherentes con la traducción.
05. Aplicar cambios, validar desde un origen externo y consultar estados, reglas, NAT y registros.
06. Comprobar que no se ha ampliado accidentalmente el acceso a otros servicios o interfaces.

34.35. Procedimiento 3: restringir recursos accesibles desde una VPN

01. Identificar si el tráfico llega mediante OpenVPN, WireGuard o una interfaz VPN asignada.
02. Separar autorización del puerto de transporte VPN (WAN) de autorización de paquetes descifrados (pestaña VPN).
03. Crear alias de orígenes autorizados y alias de recursos o servicios de destino cuando sea útil.
04. En la pestaña VPN, crear reglas Pass explícitas para combinaciones concretas, evitando Any→Any general.
05. Si hay interfaz asignada, revisar las reglas del grupo que se evalúan antes y eliminar coincidencias demasiado amplias.
06. Guardar, aplicar, probar conectividad permitida y comprobar que la no autorizada queda bloqueada.
07. Revisar estados y reply-to/rutas si las respuestas no regresan correctamente al túnel.

34.36. Procedimiento 4: bloquear sin perder acceso a la GUI

01. Identificar el equipo de administración y la ruta alternativa de acceso o consola si falla la gestión.
02. Crear un alias de equipos de gestión y una regla Pass desde ese origen a los puertos de administración del firewall.
03. Ubicar la regla por encima del nuevo bloqueo general y verificar una conexión de gestión nueva.
04. Solo entonces modificar bloqueos amplios o la protección Anti-Lockout, si la política lo exige.
05. Aplicar, reabrir sesión administrativa y comprobar navegación y acceso fuera de banda.
06. En caso de fallo, utilizar el procedimiento de recuperación aprobado por el fabricante.

Riesgo de bloqueo administrativo. No desactivar Anti-Lockout ni aplicar bloqueos globales en remoto sin acceso de recuperación, una ventana controlada y reglas de administración verificadas.

34.37. Procedimiento 5: aplicar una regla con horario

01. Crear el calendario en Firewall → Schedules según el horario aprobado.
02. Crear o editar la regla en Firewall → Rules y seleccionar Schedule en las opciones avanzadas.
03. Guardar y aplicar; probar nuevas conexiones dentro y fuera del intervalo.
04. Verificar estados existentes y la política de caducidad: no asumir que las sesiones en marcha se cortan exactamente a la hora indicada.
05. Registrar resultados y revisar zonas horarias y cambios de horario de verano.

34.38. Procedimiento 6: política de salida con gateway específico

01. Crear y validar el gateway o gateway group bajo System → Routing.
02. Localizar la pestaña de entrada del tráfico interno que se desea desviar.
03. Definir primero exenciones para destinos internos/VPN si corresponde.
04. Crear regla de paso específica para los orígenes/servicios requeridos.
05. En Advanced Options seleccionar Gateway o gateway group autorizado.
06. Guardar y aplicar; verificar salida efectiva, NAT, DNS y rutas de respuesta.
07. Probar pérdida y retorno del enlace en un entorno controlado, sin confundir monitorización con filtrado.

34.39. Ejemplos empresariales didácticos sin configuración real

Escenario	Política orientativa	Comprobación
Separación administrativa	Solo origen de gestión → servicio concreto del firewall; denegar resto cuando proceda.	Inicio de sesión desde puesto autorizado y rechazo desde otro.
Red de invitados	Permitir DNS y salida aprobada; bloquear acceso a redes internas.	Revisar accesos locales y salida exterior desde origen invitado.
Acceso remoto de soporte	VPN: permitir usuarios autorizados únicamente a sistema/puertos aprobados.	Conexión VPN establecida y prueba al recurso previsto.
Aplicación interna	Permitir clientes definidos → servidor definido → puerto de aplicación.	Prueba de función y prueba negativa de otros puertos.
Salida por enlace alternativo	Regla específica de LAN con Gateway group; exenciones internas.	Comprobar ruta, NAT y recuperación en failover.

34.40. Diagnóstico metódico de fallos de reglas

Síntoma	Posible explicación	Dónde mirar
No alcanza servicio interno	Regla en interfaz de salida en vez de entrada.	Pestaña de origen, contadores y estados.
Regla nunca registra uso	Regla superior captura los paquetes.	Orden real Floating → grupo → interfaz.
Bloquea una restricción de VPN	Un Pass previo en grupo autoriza todo.	Reglas de OpenVPN/WireGuard e interfaces asignadas.
Navegación fallida pese a Pass TCP	Faltan UDP/DNS/ICMP u otro tráfico necesario.	Protocol, logs y pruebas de aplicación.
Tráfico existente sigue pasando	Estado creado antes del cambio.	Diagnostics → States, conexión nueva.
Respuesta sale por otra WAN	Policy routing / reply-to / NAT inconsistentes.	Gateway, states, route, interfaz WAN.
Regla Source LAN address no casa	Se esperaba red de clientes, no dirección del firewall.	Address vs Subnets vs alias.
Regla no permite IPv6	Address Family seleccionado solo IPv4.	Familia IPv6, rutas, subredes y permisos.
Redirección NAT no responde	Falta regla Pass, ruta o servicio; CGNAT.	NAT, Firewall Rules, captura y upstream.
Acceso web al firewall perdido	Anti-Lockout deshabilitada o regla de gestión ausente.	Consola/recuperación y política LAN.
Bloqueo o registro excesivo	Log activado en regla demasiado amplia.	Registros y volumen syslog.
Regla de horario no corta sesión	Estado previo activo.	Estados, expiración y documentación horaria.

34.41. Métodos de validación y observabilidad

El diagnóstico empieza por conocer el flujo real y generar una conexión nueva desde el origen correcto. Consultar Firewall → Rules para el orden y el contador, Status → System Logs → Firewall para el evento registrado, Diagnostics → States para conexiones actuales y Diagnostics → Packet Capture para confirmar entrada o salida cuando sea imprescindible. La captura de paquetes solo debe realizarse con alcance limitado y autorización.

Si una regla permite pero un servicio falla, contrastar conectividad de capa 2/3, DNS, rutas estáticas, gateway, NAT, VPN, escucha local y firewall del host. Si una regla bloquea, confirmar que no haya otra coincidencia anterior, una regla especial automática o una conexión autorizada por estado preexistente.

34.42. Matriz de verificación funcional antes y después del cambio

Control	Antes	Después / criterio de aceptación
Acceso al firewall	Existe ruta de administración y sesión de respaldo.	La GUI y alternativa siguen disponibles.
Orden del conjunto	Se registra posición y reglas anteriores.	La coincidencia nueva llega a la fila prevista.
Permiso autorizado	Origen y destino han sido aprobados.	Solo la combinación requerida funciona.
Prueba negativa	Se define origen, servicio o protocolo excluido.	El acceso no autorizado permanece denegado.
IPv4 e IPv6	Se conocen las familias realmente utilizadas.	No queda una familia involuntariamente abierta.
VPN y Multi-WAN	Se documenta la ruta y el túnel.	Hay retorno y no se fuerza gateway erróneo.
Registro y estados	Se define necesidad de log y ventana de prueba.	Contadores, estados y eventos coherentes.
Reversión	Existe copia o punto de recuperación.	Se puede deshacer el cambio con seguridad.

34.43. Seguridad, rendimiento y gestión del cambio

- Mínimo privilegio: preferir origen, destino, protocolo y puerto concretos; revisión periódica de excepciones.
- Documentar propietario, solicitud, necesidad y fecha de revisión de cada regla; evitar descripciones ambiguas.
- No confundir una lista de reglas corta con un diseño correcto: priorizar trazabilidad, coherencia y pruebas negativas.
- No usar Source OS como medida fuerte de autenticación ni Synproxy como solución universal contra denegación de servicio.
- No habilitar registro masivo ni límites de estado agresivos sin dimensionar impacto y falsos positivos.
- Las modificaciones de NAT, rutas, WAN, grupos o reglas VPN deben comprobarse de extremo a extremo.
- Utilizar copia de configuración, control de cambios, ventana y procedimiento de marcha atrás para cambios críticos.
- Revisar la exposición del propio firewall y de los puertos de administración de manera independiente del tránsito.

34.44. Glosario esencial

Término	Definición breve
PF	Motor de filtrado y gestión de estados utilizado por pfSense.
Stateful	Tratamiento que recuerda conexiones y autoriza tráfico de respuesta asociado.

Término	Definición breve
Ingress	Sentido de entrada del paquete por una interfaz determinada.
Floating	Regla especial aplicable a varias interfaces y direcciones.
Quick	Termina evaluación al coincidir cuando procede; relevante en flotantes.
Interface group	Conjunto de interfaces con una pestaña y reglas comunes.
Alias	Nombre que agrupa direcciones, subredes o puertos para reutilización.
Anti-Lockout	Permiso automático para evitar perder administración local del firewall.
Reply-to	Mecanismo que influye en la ruta de retorno de estados en WAN/VPN asignada.
Policy routing	Elección de gateway según regla en vez de ruta predeterminada.
Tracking ID	Identificador de regla para correlación técnica y registros.
NAT	Traducción de direcciones y/o puertos, distinta de filtrado.

34.45. Referencias oficiales de Netgate

Se han contrastado las opciones y advertencias con la documentación de pfSense Software. La correspondencia exacta de campos puede variar entre versiones y tipos de regla; el software utilizado en este manual es pfSense Plus, sin una versión concreta identificada.

- **Configuring Firewall Rules.** https://docs.netgate.com/pfsense/en/latest/firewall/configure.html
- **Introduction to the Firewall Rules screen.** https://docs.netgate.com/pfsense/en/latest/firewall/rule-list-intro.html
- **Rule Methodology.** https://docs.netgate.com/pfsense/en/latest/firewall/rule-methodology.html
- **Floating Rules.** https://docs.netgate.com/pfsense/en/latest/firewall/floating-rules.html
- **Ordering of NAT and Firewall Processing.** https://docs.netgate.com/pfsense/en/latest/nat/process-order.html
- **Interface Groups.** https://docs.netgate.com/pfsense/en/latest/interfaces/groups.html
- **VPNs and Firewall Rules.** https://docs.netgate.com/pfsense/en/latest/vpn/firewall-rules.html
- **WireGuard and Rules / NAT.** https://docs.netgate.com/pfsense/en/latest/vpn/wireguard/rules.html
- **OpenVPN Firewall Rules.** https://docs.netgate.com/pfsense/en/latest/vpn/openvpn/firewall-rules.html
- **Reset State Table / Source Tracking Table.** https://docs.netgate.com/pfsense/en/latest/monitoring/status/firewall-states-reset.html
- **Troubleshooting Firewall Rules.** https://docs.netgate.com/pfsense/en/latest/troubleshooting/firewall.html

35 Firewall → Schedules

Calendarios · Reglas horarias · Rango de fechas · Estados · Diagnóstico y seguridad

Ruta de acceso: Firewall → Schedules. El listado presenta las columnas Name, Range: Date / Times / Name, Description y Actions, además de Add y la ayuda. Una tabla vacía indica que no hay horarios definidos. La distribución del formulario de creación puede variar entre versiones.

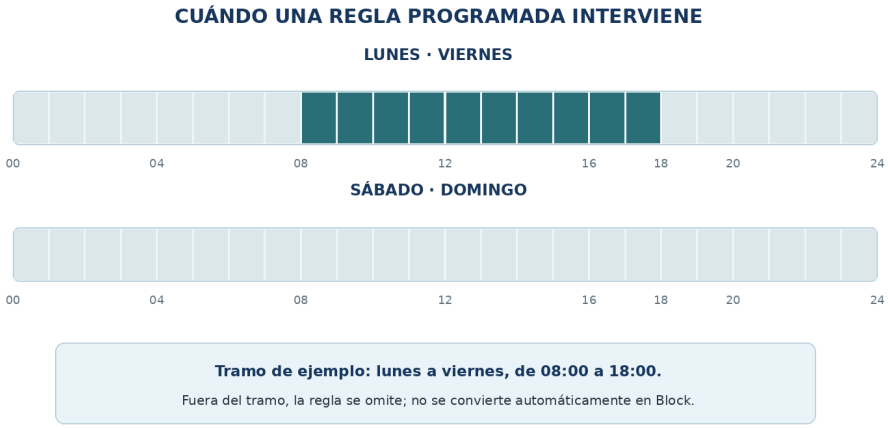


Figura 35.1. Ejemplo neutro de ventana semanal y comportamiento fuera del horario.

35.1. Propósito de los calendarios en un firewall empresarial

Un Schedule es un objeto reutilizable que delimita cuándo puede actuar una regla de filtrado: fechas concretas, días de la semana y una o varias franjas horarias. No decide qué paquetes permitir o denegar por sí mismo. Su efecto aparece cuando se vincula a una regla de Firewall → Rules que conserva sus condiciones habituales de interfaz, protocolo, origen, destino, puerto y acción.

Es útil para limitar accesos administrativos, permisos temporales de terceros, uso de servicios por franjas, ventanas de intervención y conexiones de teletrabajo. Para una política robusta, primero se decide qué se autoriza o deniega y luego en qué horario debe aplicarse. El calendario no reemplaza autenticación, segmentación ni registro de cambios.

35.2. Pantalla principal: lectura de la vista Schedules

La ruta Firewall → Schedules abre el inventario de calendarios. Cuando no existen calendarios definidos, el inventario aparece vacío. Esto no implica que el firewall carezca de otras políticas de control temporal o de configuraciones independientes de esta función. La vista descrita no incorpora pestañas adicionales.

Elemento observado	Función	Interpretación administrativa
Schedules	Título del bloque central.	Inventario de objetos temporales reutilizables.
Name	Nombre interno de cada calendario.	Identifica el objeto utilizado en reglas.
Range: Date / Times / Name	Resumen de los intervalos definidos.	Permite reconocer fechas, horas y etiquetas de tramos.
Description	Descripción administrativa.	Explica objetivo de negocio y alcance del horario.
Actions	Controles por fila, si existen calendarios.	Operaciones de mantenimiento según versión.
Add (icono +)	Acceso al editor de un calendario nuevo.	Inicia un objeto sin alterar todavía las reglas.
Icono de información / ayuda	Acceso a ayuda contextual de la página.	Consultar antes de cambiar horarios críticos.

35.3. Lista vacía, operaciones de mantenimiento y precauciones

Cuando no hay registros, únicamente se muestra Add y no existen filas que seleccionar. Una vez creados calendarios, la lista resume cada definición y permite acceder a su mantenimiento. Netgate documenta la visualización de rangos y su modificación desde el editor; la forma precisa de los iconos y controles de borrado puede variar entre versiones, por lo que debe verificarse la disponibilidad de cada acción en la versión instalada.

Borrar o cambiar un calendario usado por reglas altera la ventana efectiva de control. Antes de eliminarlo, consultar sus dependencias, elegir alternativa y verificar los permisos resultantes. Una modificación del objeto compartido repercute en todas las reglas que lo referencian.

Advertencia. Crear un Schedule no bloquea ni permite tráfico. Es necesario vincularlo a una regla y aplicar la modificación de las reglas para que tenga efecto.

35.4. Cómo abrir el formulario de creación

01. Abrir Firewall → Schedules desde el menú superior.

02. Pulsar Add en el margen derecho de la tabla.

03. Asignar Schedule Name y Description; añadir uno o varios intervalos con el calendario y la hora.

04. Revisar cada tramo incorporado a la lista del editor.

05. Guardar mediante Save y confirmar que el objeto aparece en Schedules.

06. Vincularlo a una regla desde Firewall → Rules; guardar y aplicar los cambios pendientes.

El flujo anterior se basa en la documentación de Netgate para el editor de calendarios. Los nombres de controles del formulario se ajustan a la documentación oficial de Netgate; la disposición exacta puede diferir según versión.

35.5. Schedule Name: formato, estabilidad y significado

Schedule Name es el identificador que se ofrecerá para escoger el calendario desde una regla. La documentación oficial indica emplear letras y dígitos, sin espacios. Un ejemplo genérico sería AccesoOficina. Conviene mantener un nombre breve, inequívoco y sin elementos propios de una organización. No renombrar objetos en uso sin analizar qué reglas los referencian.

35.6. Description: documentación del propósito

Description es un texto libre destinado a que un administrador entienda la finalidad del horario. Debe aclarar qué ventana representa, si se repite semanalmente o corresponde a fechas específicas y quién debe validar su utilización. No sirve para definir coincidencias: introducir una hora en la descripción no cambia el calendario.

35.7. Month y calendario: días concretos frente a recurrencia semanal

El editor incluye un selector Month y un calendario. Seleccionar fechas determinadas crea rangos ligados a días específicos; pulsar los encabezados de día de semana permite definir patrones recurrentes como lunes, miércoles y viernes, aplicables cada semana. En la documentación se ilustra asimismo la selección de una fecha concreta entre los próximos meses.

No confundir la selección de una fecha determinada con una recurrencia anual garantizada. Para cierres y festivos excepcionales, revisar la fecha real y la duración de su vigencia, y mantener un procedimiento de renovación si fuera necesario.

35.8. Start Time y Stop Time: semántica del intervalo

Los campos Start Time y Stop Time establecen las horas de comienzo y fin de un tramo en formato de 24 horas. La zona horaria empleada es la local del firewall. La documentación de Netgate establece expresamente que un intervalo no puede atravesar la medianoche; para cubrir un día completo usa 00:00 a 23:59.

La interfaz no es un sistema de cron ni un reloj de control horario de empleados. Los límites y el orden de evaluación se expresan en reglas de filtrado; las pruebas deben contemplar inicios y finales de franja, cambios de hora y conexiones ya abiertas.

35.9. Time Range Description y Add Time: construir un horario complejo

El campo opcional Time Range Description etiqueta un tramo individual, por ejemplo JornadaLunes. Tras escoger días y horas, el botón Add Time inserta ese tramo en la lista de intervalos del calendario. Se pueden repetir las operaciones para franjas distintas, como la jornada laboral, un horario reducido y una ventana de mantenimiento.

Guardar sin haber añadido al menos un tramo útil puede producir un objeto sin el efecto esperado. Revisar la lista de rangos antes de pulsar Save; no asumir que una selección visible en el calendario se ha incorporado si no se ha confirmado mediante Add Time.

35.10. Guardar, revisar y modificar intervalos

Save persiste el calendario definido. Al volver a la lista, deben revisarse nombre, resumen de rangos y descripción. Para actualizar un intervalo, entrar de nuevo en su definición, modificar o sustituir los tramos según los controles disponibles, guardar y confirmar las reglas que lo utilizan. No cambiar un calendario activo en producción sin un análisis de impacto.

35.11. Reglas con horario: la lógica que evita errores

El Schedule decide cuándo existe a efectos prácticos la regla vinculada. Dentro del intervalo, la regla puede Pass, Block o Reject según lo configurado. Fuera del intervalo, pfSense omite esa regla y continúa con las demás reglas aplicables. No convierte Pass en Block ni Block en Pass automáticamente.



Figura 35.2. La ausencia de coincidencia temporal conduce a evaluar las reglas restantes.

35.12. Ejemplo A: permitir únicamente dentro de una franja

Objetivo: permitir a un segmento de usuarios alcanzar un servicio empresarial en días laborables de 08:00 a 18:00 y denegar ese acceso fuera de horario. Crear el calendario JornadaOficina. Colocar una regla Pass limitada a origen, destino y puerto, vinculada al calendario, por encima de reglas que podrían afectar a la misma comunicación. Después, asegurar que no exista una regla Pass general posterior que permita exactamente el mismo tráfico fuera de horario; si la hay, añadir una denegación específica o rediseñar la política.

Momento	Regla Pass con horario	Regla general posterior	Resultado
Laborable, 10:00	Activa y coincidente	No se evalúa	Permitido
Laborable, 20:00	Se omite	Si permite lo mismo	Permitido: diseño incorrecto

Momento	Regla Pass con horario	Regla general posterior	Resultado
Laborable, 20:00	Se omite	No existe permiso equivalente	Bloqueado por política restante

35.13. Ejemplo B: bloquear solamente durante una franja

Objetivo: restringir un protocolo entre las 09:00 y las 12:00. Crear un calendario de ese intervalo y asociarlo a una regla Block (o Reject si está justificado) situada antes del permiso normal. Durante la ventana se aplica el bloqueo; fuera de ella la regla se omite y el permiso subyacente puede actuar. Esta técnica exige identificar antes el permiso que quedará debajo.

35.14. Prioridad y ubicación de las reglas

En las pestañas de interfaz, las reglas ordinarias se procesan de arriba abajo. Una regla horaria no tiene prioridad especial: su posición sigue siendo determinante. Por ejemplo, una regla general Pass situada encima puede captar el tráfico antes de que se alcance un bloqueo programado. En reglas flotantes existen matices de Quick que deben evaluarse de acuerdo con el diseño expuesto en el capítulo de Rules.

Para un flujo nuevo, la regla debe situarse en la interfaz donde el tráfico entra. En conexiones iniciadas desde una LAN hacia Internet, la evaluación habitual se produce en LAN; no debe ponerse la regla en WAN solo porque la comunicación tenga destino exterior.

35.15. Cómo asociar el calendario a una regla existente

01. Acceder a Firewall → Rules y escoger la pestaña de entrada correcta.

02. Editar la regla mediante el control Edit o crear una nueva con el ámbito mínimo necesario.

03. Comprobar Action, Address Family, Protocol, Source, Destination y los puertos.

04. En Advanced Options seleccionar el Schedule previamente creado, en lugar de none.

05. Guardar la regla y aplicar los cambios si aparece el aviso correspondiente.

06. Volver a la lista de reglas y comprobar la columna Schedule y su indicador de actividad.

07. Probar desde un origen controlado en horario activo e inactivo.

Netgate documenta que la lista de reglas muestra un indicador de actividad del Schedule; la ayuda emergente del indicador puede informar del estado actual. Si Schedule queda en none, la regla no tendrá límite temporal por este mecanismo.

35.16. Sesiones existentes y expiración de horarios

pfSense mantiene una tabla de estados para conexiones que atraviesan reglas Pass con seguimiento de estado. Por defecto, cuando vence un calendario, se eliminan los estados de conexiones admitidas por esa regla programada; esto permite interrumpir el acceso concedido en la ventana autorizada. No debe confundirse con el simple efecto sobre paquetes nuevos de una regla omitida fuera de horario.

La opción de sistema Do not kill connections when schedule expires, situada en System → Advanced → Miscellaneous, permite conservar las conexiones existentes al finalizar el horario. Puede ser apropiada para continuidad de ciertas sesiones, pero reduce la rigidez del corte horario. Su alcance es global y debe evaluarse antes de activarla.

Riesgo operativo. Modificar la política de eliminación de estados puede interrumpir sesiones, aplicaciones o acceso remoto. No realizar pruebas en reglas de administración sin acceso alternativo.

35.17. Horarios que cruzan medianoche: turno nocturno

Un turno de lunes a viernes que empieza a las 22:00 y termina a las 06:00 del día siguiente no puede definirse como un único intervalo 22:00–06:00. Debe representarse con dos rangos: lunes–viernes 22:00–23:59 y martes–sábado 00:00–06:00. Con ello se conserva la madrugada posterior al viernes y no se incluye por error la madrugada del lunes anterior al primer turno.

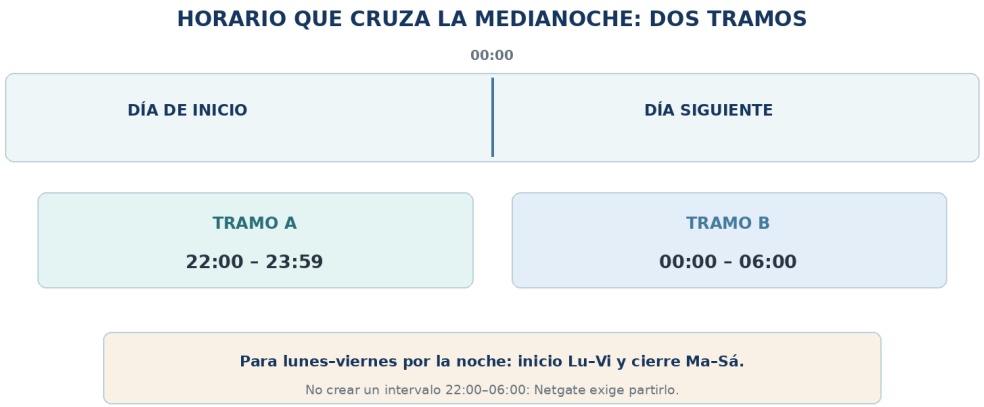


Figura 35.3. Descomposición de una jornada nocturna semanal en dos rangos válidos.

35.18. Zonas horarias, NTP y horario de verano

Los rangos se evalúan con la hora local configurada en pfSense. En System → General Setup se define Time Zone; es preferible una zona geográfica real, porque incorpora cambios legales de horario de verano, frente a una zona GMT de desplazamiento fijo. Netgate advierte que al cambiar la zona puede ser necesario reiniciar para que todos los procesos utilicen el nuevo ajuste.

El reloj debe sincronizar correctamente por NTP, revisable en Status → NTP. Si fallan la resolución DNS o los servidores horarios, el Schedule puede ejecutarse en instantes distintos a los previstos. En los cambios de hora estacionales, algunas horas pueden repetirse o no existir; evaluar y ensayar las franjas críticas próximas a ese momento.

35.19. Escenario práctico: ventanas de mantenimiento

Una empresa necesita permitir temporalmente un servicio técnico de mantenimiento sin abrir el acceso permanentemente. Definir un Schedule de fecha y franja acotada; crear una regla Pass restringida a origen autorizado, destino concreto y puerto imprescindible; habilitar registro selectivo y cerrar la regla por caducidad. Verificar que no quede un permiso más general, y comprobar al finalizar que no existan nuevas conexiones aceptadas fuera del intervalo.

Para accesos administrativos especialmente sensibles, un calendario por sí solo no es una medida suficiente: añadir autenticación fuerte, VPN, control de origen y procedimiento de autorización. Evitar exponer directamente la GUI del firewall por una mera ventana horaria.

35.20. Escenario práctico: acceso laboral a una aplicación

Crear un calendario LunVieAplicacion, asociarlo a una regla de paso desde la VLAN de usuarios hacia la dirección o alias del servidor de aplicación y limitar los puertos necesarios. La política restante debe denegar el mismo acceso fuera de horario, aunque siga autorizando DNS, NTP o servicios corporativos esenciales. Usar un alias de origen y otro de destino simplifica modificaciones futuras.

35.21. Escenario práctico: denegación horaria con excepciones

Cuando se desea denegar un servicio en un horario concreto pero permitirlo el resto del día, la regla Block programada se coloca por encima de la regla Pass pertinente. Las excepciones para sistemas críticos deben representarse como reglas explícitas de mayor prioridad y alcance reducido; una excepción que permita Any hacia Any anulando el bloqueo daría una falsa impresión de control.

35.22. Limitaciones: qué no sustituye un Schedule

Necesidad	¿La resuelve Schedules?	Herramienta/complemento apropiado
Permitir o bloquear flujos a una hora	Sí, al vincularlo a una regla.	Firewall → Rules
Programar encendido de equipos	No.	Gestión del dispositivo o plataforma
Limitar el caudal a 20 Mb/s	No; no regula velocidad.	Limiters / Traffic Shaper

Necesidad	¿La resuelve Schedules?	Herramienta/complemento apropiado
Autenticar al empleado	No.	VPN, IdP, MFA y permisos
Crear un trabajo automático de mantenimiento	No.	Planificador de la plataforma correspondiente
Auditar quién tuvo acceso	No por sí solo.	Logs, estados y controles externos

35.23. Comprobación del funcionamiento

01. Confirmar que el reloj del firewall y la zona horaria sean correctos y que NTP esté sincronizado.
02. Abrir Schedules y verificar los días, las horas y cada rango incorporado.
03. Abrir la regla asociada y confirmar el Schedule seleccionado y el orden de reglas.
04. Realizar una conexión nueva desde un equipo de prueba dentro del horario; verificar el resultado.
05. Repetir fuera del horario con una conexión nueva; comprobar ausencia de permisos solapados.
06. Consultar los registros y Diagnostics → States para diferenciar un fallo de regla de un estado ya existente.
07. Documentar la prueba, el resultado y el plan de reversión.

35.24. Diagnóstico: síntomas y causas típicas

Síntoma	Causa probable	Comprobación y corrección
Se permite acceso fuera de horario	Otra regla Pass posterior permite el mismo flujo.	Revisar lista completa y crear bloqueo/alcance correcto.
No se aplica nunca el calendario	Schedule sin tramos o no vinculado a la regla.	Verificar Add Time, Save y selección de Schedule.
Se ejecuta una hora antes/después	Zona horaria o NTP incorrectos.	Revisar General Setup y Status → NTP.
Se corta una sesión al cierre	Limpieza predeterminada de estados programados.	Evaluar política de conexiones y su impacto.
No se corta una sesión existente	Conservación global de conexiones o estado aún válido.	Revisar Miscellaneous y Diagnostics → States.
El bloqueo no tiene efecto	Regla anterior intercepta flujo o interfaz incorrecta.	Revisar orden, entrada y estados existentes.
El turno nocturno no encaja	Intervalo cruza medianoche.	Separar en dos rangos y desplazar día de cierre.

35.25. Registros, estados y reglas de diagnóstico

Status → System Logs → Firewall permite estudiar coincidencias registradas, pero no todas las reglas Pass registran tráfico por defecto. Si se necesita una prueba, activar Log de forma delimitada y retirar el exceso de detalle al finalizar. Diagnostics → States permite identificar conexiones existentes que pueden sobrevivir a un cambio de política, según las opciones y los estados vigentes.

Un registro de denegación no demuestra por sí solo que una regla horaria haya actuado: verificar la regla coincidente, el instante, el origen, el destino y el orden. Cuando exista una desconexión al vencer el horario, relacionarla con la limpieza de estados documentada y no atribuirla automáticamente al ISP o a la VPN.

35.26. Seguridad, gobernanza y ciclo de vida de los calendarios

- Definir propietarios funcionales y responsables técnicos de cada calendario; revisar si continúa justificado.
- Preferir permisos específicos, de mínima duración y con condiciones concretas de origen, destino y servicio.
- No utilizar un Schedule para sustituir un proceso de baja de usuarios o revocación de credenciales.
- Mantener nombres estables y descripciones que diferencien recurrencia semanal de fecha única.

- Evaluar efectos de una modificación sobre todas las reglas que comparten el objeto.
- Probar el inicio y el fin del intervalo, así como el siguiente tramo o la transición de día.
- Conservar copia de configuración y disponer de acceso administrativo fuera del camino afectado.

35.27. Alta disponibilidad y entornos con varios cortafuegos

En un par HA con sincronización de configuración (XMLRPC), los Schedules pueden sincronizarse si se habilita la opción Firewall schedules; cuando una regla utiliza el calendario, también deben sincronizarse las reglas asociadas. La replicación no compensa una diferencia de hora entre nodos: verificar NTP y zona horaria en ambos, así como la conmutación y el estado de la regla temporal después del failover.

35.28. Plan de cambio y reversión

01. Realizar copia de seguridad y documentar la regla que se va a modificar.
02. Verificar que no se afectarán la GUI, la consola remota o conexiones VPN esenciales.
03. Crear el calendario sin modificar aún los permisos productivos.
04. Asociarlo a una regla de prueba o de alcance limitado y aplicar los cambios.
05. Comprobar las dos situaciones: tiempo activo y tiempo inactivo.
06. Extender la regla al alcance previsto y supervisar estados, registros y usuarios afectados.
07. Si surge una incidencia, revertir la selección del Schedule o restaurar la regla previa; aplicar cambios y comprobar nuevas conexiones.

35.29. Matriz de validación para administración y auditoría

Prueba	Criterio de aceptación	Evidencia a registrar
Identificación	Nombre válido y descripción comprensible.	Ficha del objeto temporal.
Rangos	Días y horas coinciden con la política.	Listado del calendario, sin datos sensibles.
Asociación	Regla adecuada usa el calendario.	ID administrativo interno de cambio.
Horario activo	Resultado previsto con conexión nueva.	Hora, regla y comprobación técnica.
Horario inactivo	No existe permiso alternativo indeseado.	Prueba negativa fuera de ventana.
Sesiones existentes	Comportamiento de estados conocido y aprobado.	Resultado de prueba de expiración.
Reloj	NTP sincronizado y zona geográfica correcta.	Evidencia de estado anonimizada.
Reversión	Procedimiento probado o documentado.	Validación y aprobación final.

35.30. Glosario técnico

Concepto	Definición
Schedule	Objeto que describe fechas, días y rangos horarios reutilizables.
Time Range	Tramo horario individual que pertenece a un calendario.
Rule Action	Acción Pass, Block o Reject que se ejecuta si la regla está activa y coincide.
State	Entrada del filtro con estado que representa una comunicación ya permitida.
NTP	Protocolo de sincronización horaria del firewall.
Time Zone	Zona horaria local utilizada para interpretar fechas y horas.

Concepto	Definición
Rule Order	Secuencia de prioridad que determina qué regla coincide primero.
HA/XMLRPC	Entorno redundante y mecanismo de sincronización de configuración.

35.31. Referencias oficiales Netgate

Netgate, Time Based Rules — https://docs.netgate.com/pfsense/en/latest/firewall/time-based-rules.html

Netgate, Configuring Firewall Rules (Schedule) — https://docs.netgate.com/pfsense/en/latest/firewall/configure.html

Netgate, Advanced Configuration: Miscellaneous (Schedules) — https://docs.netgate.com/pfsense/en/latest/config/advanced-misc.html

Netgate, General Configuration Options: Time Zone — https://docs.netgate.com/pfsense/en/latest/config/general.html

Netgate, Troubleshooting Clock Issues — https://docs.netgate.com/pfsense/en/latest/troubleshooting/time-synchronization.html

Netgate, Troubleshooting Firewall Rules — https://docs.netgate.com/pfsense/en/latest/troubleshooting/firewall.html

Netgate, High Availability Synchronization Settings — https://docs.netgate.com/pfsense/en/latest/highavailability/settings.html

36 Firewall → Traffic Shaper

By Interface · By Queue · Limiters · Wizards | Prioridades, caudales y diagnóstico

Ruta: Firewall → Traffic Shaper. La vista inicial corresponde a By Interface: muestra las pestañas By Interface, By Queue, Limiters y Wizards, un árbol con interfaces de red y un icono de información. Las pantallas desplegadas y los formularios de las demás pestañas se describen según la documentación oficial de Netgate; su presentación y disponibilidad exactas dependen de la versión y de las capacidades de las interfaces.

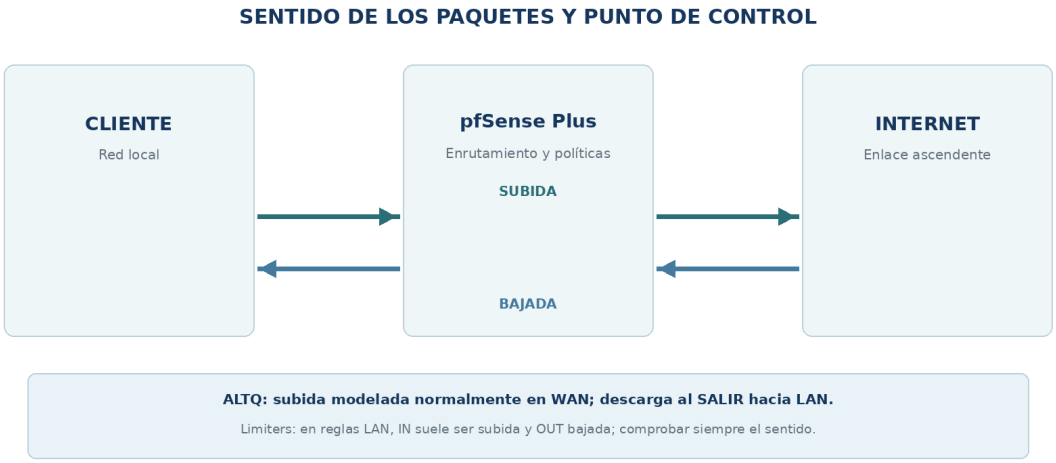


Figura 36.1. Sentido de la transmisión y localización lógica del control de QoS.

36.1. Finalidad del control de tráfico en pfSense Plus

Traffic Shaper es el área de calidad de servicio (QoS) del firewall. Permite ordenar qué comunicaciones reciben servicio primero cuando hay congestión, distribuir cuotas entre clases, limitar velocidad máxima de usuarios o redes y reducir la latencia ocasionada por colas saturadas. La política de QoS no decide por sí sola si una conexión está autorizada: ese trabajo corresponde a las reglas de firewall.

Sus aplicaciones incluyen comunicaciones de voz, sesiones interactivas, videoconferencia, aplicaciones corporativas y protección del enlace frente a descargas o copias masivas. No crea ancho de banda ni sustituye una ampliación de capacidad: administra el enlace disponible. La efectividad se mide especialmente bajo saturación, no en reposo.

36.2. Arquitectura: ALTQ frente a Limiters

Enfoque	ALTQ (By Interface / By Queue / Wizards)	Limiters
Motor	ALTQ integrado con PF y el controlador de interfaz.	dummynet, mediante pipes y queues.
Objetivo	Priorizar, distribuir y estructurar colas de salida.	Imponer caudales máximos y aplicar ponderaciones.
Aplicación	Colas vinculadas a reglas, a menudo Floating Match.	In/Out Pipe en opciones avanzadas de reglas.
Límites por IP	No es su vía principal para cuota dinámica por cliente.	Sí, usando máscaras de origen/destino.
Soporte hardware	Requiere controladores compatibles con ALTQ.	No depende de soporte ALTQ del adaptador.
Impacto	Puede reducir rendimiento máximo del firewall.	Introduce procesamiento y colas; monitorizar carga.

Enfoque	ALTQ (By Interface / By Queue / Wizards)	Limiters
Decisión práctica. Si el objetivo es garantizar prioridad para servicios interactivos con clasificación por reglas, estudiar ALTQ; si la necesidad es un tope de velocidad total, por dispositivo o por red, preferir Limiters. Coexistir es posible en diseños avanzados, pero aumenta complejidad de diagnóstico y exige ensayos.		

36.3. Pantalla inicial y navegación entre las cuatro pestañas

Elemento visible	Interpretación	Acción y precaución
By Interface	Árbol ALTQ agrupado por interfaz de salida.	Abrir la interfaz para revisar su cola raíz y subcolas.
By Queue	Vista alternativa de colas ALTQ.	Localizar, editar y comparar colas por nombre/estructura.
Limiters	Gestión de pipes y colas dummynet.	Crear límites de subida/bajada, máscaras y políticas.
Wizards	Asistentes para generar ALTQ.	Revisar riesgo de sobrescritura antes de finalizar.
Árbol de interfaces	Enlaces de interfaces configuradas.	No indica por sí solo que la QoS esté activa.
Icono de información	Ayuda contextual.	Consultar detalles antes de alterar cola raíz.

En el árbol de By Interface aparecen nombres de interfaces asignadas. La pantalla no aporta números de caudal, disciplina o colas hijas hasta entrar en su configuración; no debe inferirse ninguna política efectiva a partir del listado vacío o de simples enlaces de interfaz.

36.4. Terminología clave: cola raíz, subcola, scheduler y regla

Una cola raíz representa la capacidad de transmisión modelada de una interfaz. Las colas hijas definen clases o destinos de prioridad. El scheduler es el algoritmo con el que el sistema decide el orden y la cuota de servicio. Las reglas asocian conexiones a esas colas: si una comunicación no coincide con el criterio correspondiente, puede terminar en la cola predeterminada o no quedar modelada como se esperaba.



Figura 36.2. Árbol conceptual de colas y vínculo entre clasificación y tratamiento del tráfico.

36.5. Dirección de tráfico: subida y bajada sin confusiones

El shaping ALTQ actúa sobre el tráfico que sale del firewall por una interfaz: la subida hacia Internet suele gobernarse en la salida WAN y la descarga hacia los clientes, en la salida LAN. En limitadores asociados a una regla Pass entrante en LAN, In normalmente corresponde a tráfico que entra al firewall desde el cliente

(subida) y Out al tráfico que sale hacia el cliente (bajada). En una regla ubicada en WAN el sentido se invierte respecto a esa interpretación.

Es imprescindible comprobar dónde se evalúa la regla y hacia dónde circulan los paquetes. Etiquetar un pipe como “inbound” no garantiza que controle descarga: los campos In/Out se definen desde la perspectiva del firewall. En reglas Floating de dirección out la interpretación necesita una comprobación adicional.

36.6. By Interface: árbol de interfaces y selección de cola raíz

Ruta: Firewall → Traffic Shaper → By Interface. Cada nombre del árbol abre su configuración ALTQ y, cuando existen, las colas subordinadas. Desde esta vista se puede intervenir sobre una interfaz de salida concreta: resulta especialmente útil al ajustar la capacidad contratada, cambiar un scheduler o revisar por qué una cola carece de tráfico.

01. Abrir By Interface y elegir una interfaz de ejemplo, sin modificar todavía sus parámetros.
02. Identificar si existe una cola raíz y cuál es su planificador; registrar la configuración actual.
03. Comprobar la capacidad de salida medida y su margen operativo antes de cambiar Bandwidth.
04. Verificar qué colas hijas existen y cuál está marcada como predeterminada.
05. Guardar sólo después de revisar reglas de clasificación y otras interfaces afectadas.
06. Aplicar los cambios pendientes y probar conexiones nuevas con tráfico controlado.

36.7. Parámetros de la cola raíz: Bandwidth y Scheduler Type

Bandwidth de raíz expresa la capacidad modelada de salida. En una WAN representa principalmente el caudal de subida; en una LAN se relaciona con el tráfico descargado que el firewall entrega a dicha red. Con varias WAN, la distribución precisa depende de si los enlaces operan en paralelo, como respaldo o en rutas selectivas: no se debe sumar siempre velocidades que nunca están activas simultáneamente.

Scheduler Type selecciona la disciplina ALTQ usada en la interfaz. PRIQ simplifica prioridades, CBQ reparte clases con topes, HFSC permite curvas de servicio y CoDel se centra en retardo. Según la documentación de Netgate, el asistente maneja PRIQ/CBQ/HFSC, mientras que CoDel y FAIRQ exigen configuración manual. Los campos exactos visibles cambian según scheduler seleccionado.

36.8. Planificadores ALTQ: comparación técnica

Planificador	Función	Observaciones profesionales
PRIQ	Atiende antes las colas de mayor prioridad (0–15).	Simple; una cola alta puede privar de recursos a una baja.
CBQ	Reparto por clases, cuotas y prioridades (0–7).	Permite tomar capacidad libre del padre cuando se habilita Borrow.
HFSC	Garantías y reparto mediante curvas de servicio.	Potente para voz y aplicaciones sensibles a latencia.
CoDel	Gestión activa del retardo en cola.	Se usa sin la complejidad de las jerarquías ALTQ tradicionales.
FAIRQ	Reparto justo entre conexiones y colas.	Configuración manual; no es una opción del asistente.

36.9. PRIQ: jerarquía plana y riesgo de inanición

PRIQ ordena las colas únicamente por su prioridad, con valores de 0 a 15. No emplea el árbol de subcolas jerarquizadas propio de HFSC o CBQ. Es fácil de interpretar para diferenciar tráfico muy urgente del ordinario, pero una corriente intensa de prioridad elevada puede dejar sin caudal útil a las colas inferiores. La prioridad no equivale a una reserva garantizada de Mb/s.

36.10. CBQ: asignación de clases, prioridad y Borrow

CBQ construye clases y subclases cuya suma presupuestada no debe exceder el caudal del padre. Priority acepta valores de 0 a 7. Borrow from other queues when available permite que una clase hija consuma

capacidad no utilizada por su cola padre, hasta el límite inmediato. No debe confundirse esta función con un cupo independiente por dirección IP; para cuotas de cliente se utilizan limitadores.

36.11. HFSC: curvas de servicio y parámetros m1, d y m2

HFSC ofrece tres nociones: Real Time para garantía temporal de servicio, Link Share para distribución ordinaria y Upper Limit para imponer el máximo. La curva se expresa con m1 (caudal durante el intervalo inicial), d (duración en milisegundos) y m2 (caudal posterior). Netgate indica que, en Real Time, m2 no debe exceder el 30 % del ancho de banda padre. Sin exigencias de ráfaga suele bastar m2, dejando m1 y d vacíos.

Una garantía HFSC no debe establecerse improvisadamente: si los mínimos sumados compiten con una capacidad insuficiente, la cola se comportará de forma poco predecible para el administrador. Documentar las necesidades reales de voz o vídeo y comparar la latencia y las pérdidas bajo carga.

36.12. CoDel y FAIRQ: latencia y equidad

CoDel intenta reducir bufferbloat, que aparece cuando se acumulan paquetes en buffers y aumenta la latencia durante transferencias. Puede configurarse como disciplina ALTQ sobre una interfaz compatible, o emplearse FQ_CODEL dentro de limitadores, que constituye una implementación diferente. FAIRQ reparte de forma más equitativa entre flujos cuando existen múltiples conexiones concurrentes, aunque sus opciones no se configuran desde el wizard.

36.13. By Queue: navegación por nombre, estructura y dependencias

Ruta: Firewall → Traffic Shaper → By Queue. Muestra las colas ALTQ de manera alternativa a By Interface, haciendo más cómoda la localización de qDefault, qInternet y clases de servicio generadas por el wizard. Las operaciones de edición y mantenimiento dependen del árbol que aparezca, que está vacío o incompleto cuando no se ha creado un shaper ALTQ.

Netgate describe estas operaciones: pulsar el nombre para editar, elegir un padre y Add New Queue para añadir, o entrar en una cola para usar Delete This Queue. No debe eliminarse una cola que siga referenciada por una regla: antes, localizar dichas reglas en Firewall → Rules y reorganizar su asignación.

36.14. Campos de las colas ALTQ: Name, Priority, Queue Limit y Default Queue

Campo documentado	Qué controla	Criterio de uso
Name	Nombre de cola (1–15 caracteres, sin espacios).	Preferir nombre estable y reconocible por servicio.
Priority	Orden relativo de envío, según scheduler.	PRIQ 0–15; CBQ 0–7. En HFSC no basar garantía en Priority.
Queue Limit	Número máximo de paquetes en espera.	La documentación indica 50 por defecto; vigilar latencia.
Default Queue	Cola de tráfico que no coincide con otra clasificación.	Debe existir exactamente una cola predeterminada por interfaz.
Bandwidth	Porción absoluta o porcentual de la cola padre.	Las cuotas hijas no deben exceder el presupuesto padre.
Description	Nota administrativa para la cola.	Registrar función y dueño del servicio.

36.15. Opciones de gestión activa de colas: RED, RIO, ECN y CoDel

RED descarta antes de que se llene completamente una cola para advertir de congestión a TCP; RIO mantiene reglas de RED con diferenciación in/out. ECN marca congestión cuando los extremos la reconocen, evitando determinadas pérdidas. CoDel Active Queue se utiliza en el esquema de disciplina correspondiente. Estas opciones no deben activarse indiscriminadamente: su utilidad depende de scheduler, flujos, carga y soporte de extremos.

36.16. Reglas de asignación a colas ALTQ

Las colas no clasifican automáticamente todas las aplicaciones. Las reglas de Firewall → Rules, especialmente Floating con la acción Match, asignan los flujos a colas sin cambiar por sí mismas la

decisión Pass/Block. Una regla Pass de interfaz puede también especificar Queue/Ackqueue en sus opciones avanzadas, según los mecanismos disponibles. El wizard suele generar reglas Floating.

NAT altera direcciones antes de ciertos puntos de evaluación: una regla Floating saliente en WAN puede ver la dirección pública ya traducida, no el origen privado del cliente. Netgate recomienda, cuando proceda, clasificar en la entrada LAN o usar etiquetas de tráfico aplicadas en un punto anterior. Tampoco resulta fiable distinguir aplicaciones modernas sólo por un puerto compartido.

36.17. Limiters: cuándo utilizarlos y qué cambia respecto a ALTQ

Ruta: Firewall → Traffic Shaper → Limiters. Esta pestaña emplea dummynet y ofrece pipes raíz, colas hijas, límites de caudal y máscaras por dirección o subred. Es el recurso adecuado para fijar un máximo a invitados, equipos o tráfico no crítico. Una cuota es un techo, no una reserva mínima garantizada. Puede existir una cola hija con Weight, pero sin un Bandwidth separado: el máximo se define en el pipe padre.

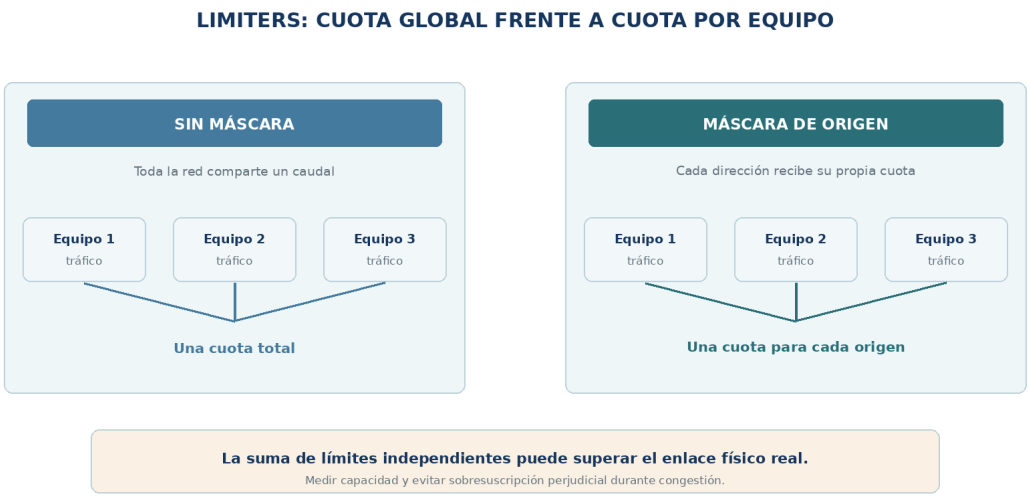


Figura 36.3. Un pipe compartido frente a un pipe con máscara por cliente.

36.18. Vista de Limiters y operaciones de creación

El botón New Limiter crea un pipe raíz; después se puede seleccionar ese pipe y pulsar Add New Queue para añadir colas subordinadas. El árbol resultante puede listar pipes habilitados o deshabilitados. Los controles concretos de edición y borrado dependen de la versión y sólo aparecen cuando existen elementos. Antes de deshabilitar o eliminar un limiter, revisar las reglas que lo referencian.

36.19. Editor de Limiters: campos fundamentales

Campo	Significado técnico	Cuándo ajustarlo
Enable	Habilita o deshabilita el limiter.	Mantener activo sólo cuando se aplica una política aprobada.
Name	Identificador alfanumérico, con - o _.	Usar Up/Down para evitar confusión con In/Out.
Bandwidth / Bw Type	Valor numérico y unidad del caudal.	Ej.: Mbit/s o Kbit/s según velocidad efectiva medida.
Schedule / Add Schedule	Varios techos para horarios diferentes.	Requiere calendarios separados y no solapados.
Mask	None, Source Address o Destination Address.	Compartir un pipe o establecer cuota por IP/subred.
IPv4/IPv6 Mask Bits	Bits de agrupación para máscaras de direcciones.	/32 por IPv4 individual; /128 por IPv6 individual.
Description	Finalidad y alcance administrativo.	Documentar a quién afecta y motivo del límite.

36.20. Limiters avanzados: Delay, Weight, Packet Loss Rate y Queue Size

Opción	Alcance	Advertencia
Delay	Pipe raíz: retardo artificial en milisegundos.	Pensado sobre todo para ensayos; no activar en producción sin motivo.
Weight	Cola hija: ponderación 1–100.	Distribuye prioridad dentro del pipe; no crea una cuota nueva.
Packet Loss Rate	Descartes inducidos, porcentaje como fracción.	0.01 significa 1 %; normalmente se deja vacío.
Queue Size	Slots de cola, por defecto 50 si vacío.	Grandes colas pueden elevar demora y uso de memoria.
Bucket Size	Tamaño de la tabla hash, por defecto 64.	Normalmente dejar vacío; rango documentado 16–65536.

El editor puede exponer Queue Management Algorithm (p. ej., Tail Drop) y Scheduler (p. ej., FQ_CODEL) según el limiter y la versión. Su combinación debe evaluarse con métricas de latencia, CPU, uso de memoria y descartes. Algunos valores y controles avanzados no aparecen hasta guardar o expandir secciones del formulario.

36.21. Máscaras por dirección: cuota total o cuota por abonado

Mask=None crea una capacidad común a todos los flujos coincidentes; Source Address o Destination Address crea instancias por origen, destino o prefijo, según Mask Bits. En una regla entrante de LAN, para subida por equipo se utiliza generalmente una máscara Source y para descarga una máscara Destination. Una máscara /24 agrupa equipos por subred completa; /32 aplica por dirección IPv4 y /128 por dirección IPv6.

Si se aplica un límite de 10 Mbit/s por equipo a treinta equipos, no significa que el enlace disponga de 300 Mbit/s: cada uno puede intentar alcanzar su máximo y la suma quedará restringida por la capacidad real. Probar simultaneidad, colas, jitter y calidad de servicio.

36.22. Asignación de Limiters en reglas: In/Out Pipe

1. Crear dos pipes identificados por función: uno para subida y otro para bajada; guardar y aplicar.
2. Abrir la regla Pass que acepta el tráfico deseado, o una regla Floating debidamente delimitada.
3. Expandir Advanced Options y localizar In / Out Pipe.
4. En una regla de entrada de LAN, seleccionar el pipe de subida en In y el de bajada en Out.
5. Guardar la regla y aplicar los cambios.
6. Abrir sesiones nuevas, medir subida y descarga por separado y revisar Diagnostics → Limiter Info.

Atención al sentido. Si se aplica desde WAN o desde una Floating out, los sentidos cambian. No copiar In/Out de una regla a otra sin razonar la perspectiva del cortafuegos.

36.23. Limiters, IPv6 y políticas Multi-WAN

Netgate documenta que los limiters admiten IPv6, pero puede ser necesario separar reglas IPv4 e IPv6 para su aplicación correcta. En Multi-WAN, los enlaces que no usan la pasarela predeterminada requieren un tratamiento específico mediante reglas Floating en dirección out y la pasarela correspondiente. En escenarios de failover, no asumir que un límite construido para la WAN primaria se adapta por sí solo a las capacidades de una WAN de respaldo.

36.24. FQ_CODEL con Limiters para bufferbloat

FQ_CODEL puede ayudar a reducir la latencia bajo carga sin utilizar ALTQ en el adaptador. La receta oficial configura un limiter y una cola hija para descarga, otro conjunto para subida, Scheduler=FQ_CODEL y Queue Management Algorithm=Tail Drop, además de una regla Floating de salida que asigna los pipes. Netgate sugiere iniciar las pruebas con los valores predeterminados de FQ_CODEL y ajustar el ancho de banda a la capacidad efectiva del enlace.

Los valores de Queue Length utilizados en recetas son orientativos para determinadas velocidades, no una configuración universal. Una red con buen comportamiento de latencia y bajo nivel de bufferbloat puede no

necesitar estos limitadores, y establecer el caudal demasiado bajo desperdiciará capacidad. Medir latencia en reposo y simultáneamente con cargas de subida y bajada.

36.25. Wizards: modalidades disponibles y alcance

Ruta: Firewall → Traffic Shaper → Wizards. Netgate documenta Multiple LAN/WAN (general, una o varias conexiones de cada tipo) y Dedicated Links (emparejamientos concretos entre LAN y WAN). Tras seleccionar el enlace correspondiente del asistente, la GUI solicita recuento de interfaces, selección de redes y velocidad, planificador ALTQ y clasificación de aplicaciones.

Advertencia crítica. Finalizar un wizard puede sustituir las colas y reglas Floating creadas anteriormente por el asistente, incluidas copias derivadas de esas reglas. Guardar respaldo de configuración, inventario de colas y reglas, y comprobar el impacto antes de pulsar Finish.

36.26. Wizards: selección de interfaces, velocidades y planificador

01. Elegir Multiple LAN/WAN salvo que exista un diseño que justifique Dedicated Links.
02. Indicar cuántas WAN y LAN se tratarán; la clasificación WAN/LAN del sistema depende de gateways y tipo de interfaz.
03. Seleccionar las interfaces de cada grupo y un scheduler compatible (PRIQ, CBQ o HFSC).
04. Introducir velocidades reales de upload y download, con unidades consistentes.
05. Aplicar un margen prudente frente a la capacidad medida para que las colas del firewall administren la congestión.
06. Revisar las páginas de aplicaciones y Finish sólo después de evaluar las reglas existentes.

36.27. Wizard: voz IP y tráfico en tiempo real

La fase Voice over IP permite priorizar llamadas mediante Provider (selección de perfil) o Upstream SIP Server (servidor/alias del extremo). Netgate recomienda priorizar el extremo remoto cuando sea posible porque los puertos SIP/RTP pueden coincidir con otros servicios y el NAT modifica direcciones durante el procesamiento. En HFSC/CBQ aparecen campos de garantía de subida y descarga; en PRIQ tales garantías de ancho de banda se dejan en blanco.

36.28. Wizard: Penalty Box y redes P2P

Penalty Box aplica una penalización de caudal máxima a la dirección o alias seleccionados. La etapa Peer-to-Peer permite bajar prioridad al tráfico clasificado y dispone de la modalidad Catch All que trata tráfico no reconocido como P2P: debe emplearse con extremo cuidado, pues puede reducir prioridad a comunicaciones legítimas no clasificadas.

36.29. Wizard: juegos y clasificación de otras aplicaciones

El asistente incluye prioridades de tráfico de juegos y un bloque Raise or Lower Other Applications. Se elige para cada protocolo si tendrá prioridad Higher, Lower o Default. Las categorías disponibles son orientativas, y los protocolos modernos cifrados o de puertos dinámicos pueden no encajar con los perfiles. No atribuir a estos perfiles capacidades de inspección de aplicaciones que Netgate no documenta.

36.30. Wizard: finalización, IPv6 y estados establecidos

Finish crea las colas y reglas de clasificación activadas. Netgate indica que el wizard genera reglas IPv4: para IPv6 deben duplicarse o adaptarse manualmente según necesidad. La asignación de QoS puede quedar asociada a estados creados antes del cambio; para una prueba fiable, generar conexiones nuevas. Reset States vacía toda la tabla y desconecta sesiones; hacerlo sólo con autorización expresa y ventana de mantenimiento.

36.31. Procedimiento: dar prioridad a voz en una red saturada

01. Medir velocidad de subida y latencia mientras existe tráfico de carga.
02. Confirmar interfaz(s) y compatibilidad con ALTQ; elegir un planificador apropiado para el diseño.

03. Con el wizard generar colas y reglas para VoIP tomando como referencia direcciones conocidas del extremo remoto.
04. Revisar reglas Floating, colas predeterminadas, los protocolos y la dirección del tráfico.
05. Probar llamada mientras se transfiere un archivo grande; comparar pérdida, jitter y retraso antes/después.
06. Si la calidad empeora, recuperar la configuración previa y estudiar reglas de coincidencia y capacidad real.

36.32. Procedimiento: tope por usuario en una red de invitados

01. Diseñar un máximo de subida y descarga realistas, sin afectar a la navegación básica.
02. Crear limitadores Up y Down con bandwidth y unidad adecuados.
03. Elegir la máscara de IP origen para subida y destino para bajada desde reglas LAN.
04. Crear o editar una regla Pass restringida a la red de invitados; asignar pipes en Advanced Options.
05. Comprobar que no exista otra regla anterior que capture los flujos sin limitadores.
06. Probar desde varios equipos simultáneos y examinar Diagnostics → Limiter Info.

36.33. Procedimiento: corregir bufferbloat con FQ_CODEL

01. Realizar pruebas de rendimiento y latencia con la QoS deshabilitada; documentar estado inicial.
02. Crear pares de pipes y colas según la receta Netgate de FQ_CODEL.
03. Asignar capacidades conservadoras y las opciones compatibles de cola.
04. Aplicar mediante reglas del sentido correcto y sin duplicar un shaping ALTQ equivalente.
05. Ejecutar tráfico concurrente; medir RTT, jitter, pérdidas, caudal útil y carga del firewall.
06. Ajustar gradualmente o revertir si no existe una mejora verificable.

36.34. Escenario empresarial: WAN principal y enlace de contingencia

En una organización con un enlace principal de alta velocidad y otro secundario más reducido, las políticas de QoS deben considerar las condiciones reales de cada ruta. No limitarse a copiar el Bandwidth del enlace principal a las colas del de respaldo. Tras un failover, comprobar el gateway que utiliza el tráfico, las reglas de asignación, la disponibilidad de la interfaz y las limitaciones Multi-WAN de los Limiters. Dar prioridad a procesos esenciales, no necesariamente al mayor volumen de datos.

36.35. Escenario empresarial: servicios interactivos y transferencias de fondo

La prioridad alta puede reservarse a comunicaciones interactivas o críticas, mientras que las copias y sincronizaciones pueden ocupar capacidad sobrante. Para separar servicios es preferible clasificar por endpoints conocidos y reglas precisas en vez de suponer que un puerto equivale siempre a una aplicación. En enlaces limitados, definir techos para los procesos de fondo suele ofrecer una mejora más verificable que otorgar máxima prioridad a cada aplicación empresarial.

36.36. Comprobación: Status → Queues y Diagnostics → Limiter Info

Status → Queues muestra colas ALTQ: PPS, Bandwidth, Borrows, Suspends, Drops y Length. El aumento de drops durante congestión no significa necesariamente caída de conexiones, pero requiere interpretar latencia, retransmisiones y condiciones de carga. Diagnostics → Limiter Info permite leer valores configurados de pipes/queues y estadísticas de uso, incluyendo instancias enmascaradas por IP.

Indicador	Lectura	Qué comprobar
PPS / Bandwidth	Paquetes/s y bits/s en una cola ALTQ.	Que la cola adecuada procese el flujo de prueba.
Drops	Paquetes descartados por modelado o congestión.	Correlación con latencia y pérdidas visibles.
Length	Ocupación de cola respecto a tamaño.	Aumento sostenido y retardo bajo carga.

Indicador	Lectura	Qué comprobar
Borrows	Capacidad que una cola toma según reglas CBQ.	Que la clase tenga disponibilidad y política válida.
Limiter Info	Actividad de pipe y colas dummynet.	Que reglas In/Out asignen tráfico en el sentido correcto.
CPU/mbufs	Recursos de procesamiento y memoria.	Que la QoS no degrade el throughput crítico.

36.37. Errores frecuentes y diagnóstico paso a paso

Síntoma	Causa habitual	Corrección recomendada
No hay tráfico en la cola	Regla equivoca origen/puerto/dirección; estado antiguo.	Revisar Floating, NAT, coincidencias y conexión nueva.
No actúa limiter	Pipe sin habilitar o regla anterior intercepta.	Comprobar Enable, In/Out y Diagnostics → Limiter Info.
Bajada controlada como subida	In/Out se invirtieron.	Razonar desde perspectiva firewall según pestaña y dirección.
Se reduce demasiado el caudal	Bandwidth por debajo del enlace real.	Medir capacidad y corregir unidades, overhead y valores.
Aumenta jitter pese a QoS	Colas grandes, scheduler impropio o CPU insuficiente.	Revisar tamaño de colas, algoritmo y carga.
Tras cambiar WAN no encaja QoS	Capacidades y pasarela distinta en Multi-WAN.	Política específica por enlace y prueba de failover.
IPv6 no se clasifica	Wizard generó únicamente reglas IPv4.	Construir reglas IPv6 equivalentes y probarlas.
Desaparecen reglas tras wizard	Finish sustituyó objetos generados previamente.	Restaurar copia y revisar reglas antes de nuevo wizard.

36.38. Seguridad, rendimiento y límites de la técnica

- No activar el shaping por rutina si no existe un problema concreto que corregir y medir.
- Priorizar un número reducido de clases para que los cambios sean mantenibles y verificables.
- Evitar IP, redes, nombres internos o topologías reales en documentos de operación publicados.
- Comprobar soporte ALTQ del driver antes de diseñar colas ligadas a ese mecanismo.
- Controlar CPU y memoria: ALTQ puede reducir el caudal máximo; dummynet también tiene coste.
- Reservar acceso de emergencia fuera de cualquier política de tráfico que pueda saturarse.
- No tratar QoS como control de seguridad ni como sustituto de autenticación y firewall.

36.39. Plan de implantación con reversión segura



Figura 36.4. Fases recomendadas para medir, aplicar y validar cambios de QoS.

01. Guardar un backup de configuración y un inventario de reglas y colas actuales.

02. Realizar medición de referencia: velocidad de descarga/subida, RTT, pérdida, carga y estados.
03. Definir un objetivo medible y un conjunto de dispositivos o aplicaciones piloto.
04. Aplicar una sola familia de cambios cada vez (ALTQ o Limiters) y documentar sus referencias.
05. Validar tráfico nuevo, transferencia simultánea y servicios sensibles.
06. Si hay cortes o degradación, retirar asignaciones o restaurar el respaldo; aplicar y verificar.
07. Cerrar la intervención con evidencias y responsable que acepta los resultados.

36.40. Matriz de aceptación y evidencias

Prueba	Criterio mínimo	Registro de evidencia
Accesibilidad	GUI, VPN y servicios administrativos responden.	Lista de comprobación sin direcciones reales.
Clasificación	El servicio pasa por la cola o pipe esperado.	Estado de Status → Queues / Limiter Info anonimizado.
Caudal	El límite coincide razonablemente con el valor objetivo.	Tres ensayos con origen y destino de prueba.
Latencia	Jitter y RTT no empeoran bajo carga respecto a base.	Comparación en reposo y carga simultánea.
Fairness	No existe inanición inesperada de tráfico ordinario.	Pruebas de simultaneidad.
IPv6	El flujo IPv6 recibe el tratamiento previsto.	Comprobación explícita por familia.
Multi-WAN	Durante el cambio de ruta siguen operando las políticas.	Prueba de failover programada.
Rollback	Restitución posible sin pérdida prolongada de gestión.	Procedimiento y validación firmada.

36.41. Glosario esencial

Término	Definición
QoS	Gestión de prioridad, colas y recursos de enlace.
Traffic shaping	Modelado del caudal mediante temporización/descartes.
ALTQ	Subsistema de colas compatible con determinados drivers.
Scheduler	Disciplina de planificación de paquetes: PRIQ, CBQ, HFSC, etc.
Queue / Root Queue	Cola / cola principal con capacidad asignada a una interfaz.
Limiter / Pipe	Entidad dummynet que impone un máximo de transmisión.
Mask Bits	Agrupación del límite por dirección IP o por prefijo.
AQM	Gestión activa de cola para controlar congestión y retardo.
Bufferbloat	Incremento significativo de latencia por buffers saturados.
FQ_CODEL	Planificador/algoritmo de colas orientado a equidad y baja latencia.
In / Out Pipe	Asignación de limitadores en reglas desde perspectiva del firewall.

36.42. Referencias oficiales de Netgate

Traffic Shaper — visión general — https://docs.netgate.com/pfsense/en/latest/trafficshaper/index.html

Advanced Customization — colas y reglas — https://docs.netgate.com/pfsense/en/latest/trafficshaper/advanced.html

ALTQ Scheduler Types — https://docs.netgate.com/pfsense/en/latest/trafficshaper/altq-scheduler-types.html

Limiters — campos, máscaras y reglas — https://docs.netgate.com/pfsense/en/latest/trafficshaper/limiters.html

Using the Shaper Wizard to Configure ALTQ — https://docs.netgate.com/pfsense/en/latest/recipes/traffic-shaper-altq-wizard.html

Configuring CoDel Limiters for Bufferbloat — https://docs.netgate.com/pfsense/en/latest/recipes/codel-limiters.html

Hardware Limitations (ALTQ) — https://docs.netgate.com/pfsense/en/latest/trafficshaper/limitations.html

ALTQ Traffic Shaper Queue Monitoring — https://docs.netgate.com/pfsense/en/latest/monitoring/status/traffic-shaper-queues.html

Troubleshooting Traffic Shaping — https://docs.netgate.com/pfsense/en/latest/troubleshooting/traffic-shaper.html

37 Firewall → Virtual IPs

IP Alias · CARP · Proxy ARP · Other | NAT, publicación y alta disponibilidad

Ruta: Firewall → Virtual IPs. La vista principal consta de una tabla Virtual IP Address con las columnas Virtual IP address, Interface, Type, Description y Actions, junto a Add y un icono de información. La vista de referencia está vacía: esto únicamente indica que no hay VIP enumeradas en esa tabla. Los detalles del formulario Add y los parámetros específicos por tipo se desarrollan a partir de la documentación oficial de Netgate, y su disponibilidad exacta depende de la versión instalada.



Figura 37.1. Criterios para elegir entre los cuatro tipos de dirección IP virtual.

37.1. Objeto y alcance de Virtual IPs

Una dirección IP virtual (VIP) amplía las direcciones que un firewall puede presentar o utilizar, sin alterar obligatoriamente la IP principal configurada en Interfaces. Puede servir para recibir conexiones destinadas a una IP adicional, proporcionar un extremo de servicios, publicar recursos mediante NAT o compartir una identidad de red entre dos nodos de alta disponibilidad.

El concepto no debe confundirse con un alias de Firewall → Aliases: el alias agrupa IP, redes o puertos para referenciarlos en reglas, mientras que una VIP representa una dirección adicional con un comportamiento específico de red. Tampoco significa, por sí misma, que una IP sea accesible desde Internet o que exista un servicio escuchando.

37.2. ¿Cuándo conviene crear una dirección virtual?

- Varias direcciones disponibles en un mismo segmento de red para separar servicios o destinos NAT.
- Un bloque de IP adicionales que un proveedor enruta hasta el firewall, sin exigir ARP por cada dirección.
- Un clúster activo/pasivo cuya pasarela compartida de LAN o WAN debe permanecer estable entre nodos.
- Una infraestructura que necesita IP de enlace para aplicaciones del propio firewall, sin modificar la IP principal.
- Escenarios específicos de laboratorio o migración en los que hay que mantener temporalmente una dirección adicional.

No se crean VIP por rutina para aumentar capacidad, resolver pérdidas de enlace o sustituir un gateway. La condición imprescindible es comprender cómo llega el tráfico al firewall: conexión de capa 2 con ARP/NDP o encaminamiento desde un dispositivo upstream.

37.3. Lectura completa de la pantalla de listado

Control / columna visible	Significado	Acción administrativa
Virtual IP address	Dirección o prefijo registrado en una VIP.	Identificar la dirección sin asumir que sea la IP principal.
Interface	Interfaz vinculada al objeto VIP.	Comprobar pertenencia a segmento, ruteo y estado de enlace.
Type	IP Alias, CARP, Proxy ARP u Other.	Interpretar ARP, servicios locales y failover según tipo.
Description	Texto libre de propósito y titularidad.	Mantener un inventario legible y objetivo.
Actions	Acciones por fila cuando existe un objeto.	Editar o eliminar con revisión de dependencias.
Add	Abre el formulario de creación de una nueva VIP.	Seleccionar tipo e introducir parámetros consistentes.
Información	Icono de ayuda contextual.	Consultar avisos antes de cambios de red.

La tabla vacía no permite deducir el estado de otras configuraciones de NAT, los gateway o las interfaces: son componentes distintos. Los iconos de edición y eliminación aparecen cuando existen filas; su representación puede variar por versión.

37.4. Los cuatro tipos de VIP: comparación técnica

Tipo	Responde a ARP/L2	Servicios en pfSense	NAT	HA
IP Alias	Sí (ARP en IPv4; ND en IPv6)	Sí	Sí	No por sí solo; excepciones al enlazarlo a CARP
CARP	Sí, MAC virtual	Sí, en nodo MASTER	Sí	Sí, identidad compartida
Proxy ARP	Sí, responde ARP	No	Sí	No como VIP sincronizada
Other	No	No	Sí, con ruta upstream	Compatible con subred enrutada a VIP CARP

La respuesta ICMP que emite el firewall por sí solo es posible para IP Alias y CARP si las reglas lo permiten. Proxy ARP y Other no atienden ping localmente: una traducción NAT hacia un equipo interno podría permitir que responda ese equipo. No usar un ping fallido como única prueba de que una VIP está mal configurada.

37.5. Decisión previa: entrega ARP frente a subred enrutada

Si la IP adicional está en un segmento donde un router necesita resolver el destino mediante ARP, el firewall debe contestar al vecino: se consideran IP Alias, Proxy ARP o CARP según se requieran servicios locales y HA. Si el proveedor ha creado una ruta estática que entrega un prefijo adicional a la IP WAN del firewall, normalmente no hace falta responder ARP por cada IP de ese prefijo: Other permite utilizar las direcciones en los selectores de NAT.

Cuidado con la interpretación. Un prefijo público enrutado a un firewall no equivale a un prefijo directamente conectado. Configurar Proxy ARP en el segmento equivocado no sustituye la ruta necesaria en el upstream.

37.6. IP Alias: comportamiento y ventajas

IP Alias añade una IP real a la interfaz del sistema. El propio firewall puede responder al descubrimiento de vecinos, aceptar tráfico hacia ella y utilizarla como dirección de enlace para servicios compatibles. También sirve para alojar más de una red en la misma interfaz, siempre que el diseño de direccionamiento y filtrado sea explícito.

Es apropiado cuando un servicio del firewall debe escuchar en una dirección adicional, o cuando NAT necesita un destino cuya dirección se encuentre realmente asignada. Por motivos de seguridad, revisar la configuración de escucha de GUI, DNS, VPN y otros demonios: un servicio configurado para escuchar en “todas las interfaces” podría quedar también accesible desde un nuevo IP Alias.

37.7. IP Alias: máscara, subred y vínculo a Localhost o CARP

En la misma subred que la interfaz principal, conviene mantener la máscara coherente con la red; Netgate admite también usos específicos con /32. Para IP Alias en una subred distinta, al menos uno de los alias de ese segmento necesita la máscara correcta para establecer la red conectada. Los IP Alias se crean individualmente, no como un rango ampliado automáticamente a direcciones locales.

Un IP Alias puede usar como interfaz padre una VIP CARP, formando un alias apilado. Esto reduce anuncios CARP y permite que varios destinos compartan la misma transición MASTER/BACKUP; esos alias deben pertenecer a la misma subred que el CARP padre. También puede vincularse a Localhost cuando una dirección de un bloque enrutado se requiere para un servicio interno. IP Alias independiente no se sincroniza normalmente vía XMLRPC, para evitar conflictos; los apilados en CARP o asociados a Localhost son excepciones documentadas.

37.8. CARP: dirección compartida y alta disponibilidad

CARP (Common Address Redundancy Protocol) permite que varios nodos coordinen quién debe hacerse cargo de una dirección y de su MAC virtual. El nodo MASTER utiliza la VIP para atender el tráfico; BACKUP permanece preparado mientras recibe los anuncios del principal. El resultado es una identidad de red compartida sin tener que reconfigurar la dirección de puerta de enlace en clientes ante una conmutación correcta.

CARP no sincroniza por sí solo ni estados de conexiones ni el resto de la configuración: la continuidad requiere diseñar también pfsync, sincronización XMLRPC, rutas, reglas, configuración de servicios y pruebas de failover. Puede utilizarse en un solo firewall para preparar una transición futura a un clúster o disponer de una MAC propia por VIP.

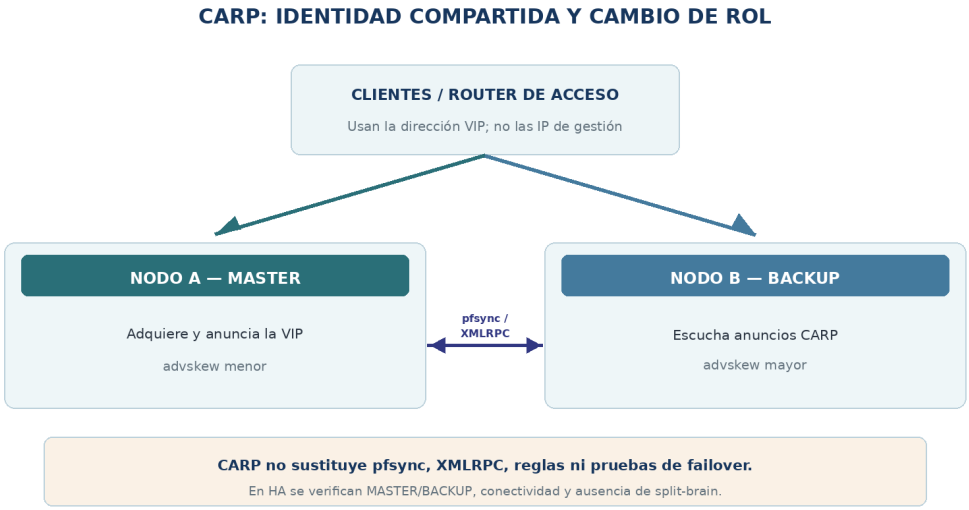


Figura 37.2. Roles MASTER y BACKUP e integración conceptual con sincronización.

37.9. CARP: contraseña compartida y VHID Group

Virtual IP Password protege la autenticidad de los anuncios CARP; los nodos que comparten una misma VIP han de usar la misma contraseña. No escribirla en documentación operativa ni copiarla en capturas. VHID Group identifica el grupo redundante y determina parte de la MAC virtual asociada a la VIP. Cada VHID debe ser único dentro del mismo dominio de capa 2, incluso cuando existan otras instalaciones CARP o VRRP.

Una colisión de VHID puede provocar errores de MAC, pérdida de tráfico o estados MASTER simultáneos. No escoger identificadores sin inventariar primero el segmento. Para IPv4 Netgate cita como convención opcional utilizar el último octeto de la VIP, pero no reemplaza la comprobación de unicidad.

37.10. CARP: Advertising Frequency, Base y Skew

Campo	Función exacta	Recomendación de operación
Base	Intervalo base en segundos entre anuncios.	El valor típico es 1; mantener consistente entre nodos.
Skew	Fracción de 1/256 de segundo que altera la prioridad efectiva.	Primario normalmente 0–1; secundario alrededor de 100.
Frecuencia	Combinación Base/Skew determina anuncios y preferencia.	No ajustar a ciegas para encubrir pérdidas de red.
Sincronización XMLRPC	Puede aumentar automáticamente en 100 el skew de nodo secundario.	No duplicar ajustes sin revisar cómo está habilitada la sincronización.

En CARP, una preferencia de anuncios más rápida permite al nodo preferido asumir el rol MASTER. Diferencias arbitrarias de temporización o un enlace inestable pueden originar oscilación de roles. Verificar primero la entrega de anuncios, la conectividad L2 y el estado real en Status → CARP (failover).

37.11. pfSense Plus: CARP multicast y CARP unicast

La documentación oficial de pfSense Plus describe el control CARP Mode: Multicast o Unicast. Multicast anuncia por el segmento de capa 2 y permite que más de dos posibles participantes escuchen los anuncios, siempre que la red transporte multicast correctamente. Unicast envía directamente al Peer Address y evita la necesidad de multicast extremo a extremo, pero limita el clúster a dos nodos. La GUI de la versión utilizada puede cambiar en localización y presentación de estos campos.

Unicast está orientado a redes especiales —por ejemplo, determinadas infraestructuras cloud o segmentos que no transportan multicast— y no debe adoptarse indiscriminadamente en Ethernet convencional. Netgate advierte sobre posible inundación de tráfico hacia la MAC virtual porque las tramas de anuncio unicast pueden salir con la MAC de interfaz física. El campo Peer Address indica la dirección de comunicación con el otro miembro y requiere verificación bidireccional. La documentación señala que el Peer Address no admite actualmente direcciones IPv6 link-local.

Advertencia de seguridad y rendimiento. No cambiar un clúster operativo de multicast a unicast sólo para “mejorar” la redundancia. Revisar capacidad de switches, aprendizaje de MAC, topología y restricciones del hipervisor, y probar ambos sentidos antes de usarlo en producción.

37.12. Proxy ARP: representación de IP sin asignación local

Una VIP Proxy ARP responde solicitudes ARP para una IP o un conjunto de IP. Las direcciones no se añaden como direcciones locales del sistema operativo: el firewall únicamente atrae a nivel de enlace el tráfico hacia esos destinos, de modo que después NAT pueda redirigirlo. No permite asociar a ellas un servicio del propio pfSense ni responde a ping por sí misma.

Suele emplearse cuando existe un conjunto de direcciones adicionales accesibles en el mismo dominio de capa 2 y todas se utilizarán con NAT. Si la IP adicional se ha enrutado a través del gateway y no requiere ARP, el tipo Other describe mejor el escenario.

37.13. Other: prefijos ya encaminados hasta el firewall

Una VIP Other no instala una dirección local ni responde ARP: sirve para que direcciones de un prefijo enrutado estén disponibles en selectores de NAT. Es una declaración administrativa para NAT, no un anuncio de propiedad de la IP en el segmento. Por ello tampoco habilita automáticamente escucha local ni ping al firewall.

Un caso típico es un proveedor que enruta un bloque público secundario a la IP WAN o a una CARP VIP. El tráfico sólo llegará si upstream conoce la ruta y si el firewall dispone de las reglas NAT y de filtrado correctas. Este método es compatible con escenarios redundantes cuando el prefijo se enruta a la VIP CARP activa.

37.14. Formulario Add: campos comunes documentados

Campo	Qué configura	Disponibilidad y precauciones
Type	Selecciona IP Alias / CARP / Proxy ARP / Other.	Determina qué campos se muestran.

Campo	Qué configura	Disponibilidad y precauciones
Interface	Interfaz padre o CARP VIP para alias apilados.	No confundir interfaz física con etiqueta administrativa.
Address Type	Una dirección o una subred entera.	Documentado para Proxy ARP y Other.
Address(es)	IP y máscara/prefijo CIDR.	Validar pertenencia, ruta, IPv4/IPv6 y solapes.
Expansion	Desglosa subred IPv4 en direcciones en listas de selección.	Sólo ciertos Proxy ARP / Other IPv4; cuidado con prefijos grandes.
Description	Texto del destino o función.	Registrar finalidad sin datos identificativos sensibles.

Los campos del editor dependen del tipo de dirección virtual y de la familia IP elegida. No todos se muestran simultáneamente; comprobar las opciones que corresponden al tipo seleccionado.

37.15. Address Type y Expansion: IP individual frente a subred

Con Proxy ARP y Other, Address Type permite distinguir entre una IP individual y un prefijo que representa múltiples IP. En subredes IPv4, Expansion puede hacer que cada dirección del prefijo se ofrezca por separado en determinados desplegables de NAT. Esto facilita seleccionar una IP concreta, pero puede crear listas enormes y provocar problemas de representación en el navegador.

No utilizar un /16 o un prefijo de gran tamaño como una manera cómoda de “reservar” todas las direcciones visibles: examinar la necesidad real y limitar el número de entradas. La operación no instala una IP por cada elemento cuando el tipo es Other, ni concede propiedad de la subred ante el proveedor.

37.16. IPv4, IPv6, ARP y Neighbor Discovery

En IPv4, la resolución del siguiente salto local suele depender de ARP; en IPv6 la función equivalente se apoya en Neighbor Discovery, no en ARP. Al evaluar una VIP IPv6, diferenciar el tratamiento de la dirección, la publicidad de vecinos, el enrutamiento del prefijo y las reglas de firewall IPv6. La disponibilidad de cada combinación tipo/familia se debe confirmar en la versión instalada, ya que no todos los mecanismos son intercambiables.

CARP permite VIP IPv6 en escenarios compatibles, pero la máscara del CARP debe corresponder al segmento de la interfaz y la red debe permitir su funcionamiento. Evitar suponer que al agregar una VIP IPv6 ya están configurados RA, DHCPv6, rutas del operador y políticas de seguridad.

37.17. Operaciones de listado: Add, edición, borrado y aplicación

01. Abrir Firewall → Virtual IPs e identificar los objetos previamente existentes.
02. Pulsar Add; elegir el Type adecuado según requisitos de ARP, servicios locales y alta disponibilidad.
03. Completar Interface, direcciones y campos condicionales; redactar una descripción técnica.
04. Pulsar Save y, cuando aparezca el aviso, Apply Changes para activar el cambio.
05. Comprobar la aparición en la tabla y verificar ARP/NDP, ruta o estado CARP según el tipo.
06. Antes de editar o eliminar, buscar dependencias en NAT, reglas, servicios, sincronización y rutas; planificar reversión.

Modificar o suprimir una VIP publicada puede cortar sesiones, interrumpir acceso externo o cambiar el miembro que responde a una dirección compartida. En producción, registrar ventana de mantenimiento, backup previo, punto de recuperación y responsables de validación.

37.18. Procedimiento práctico A: IP Alias para servicio del firewall

01. Verificar que la dirección adicional pertenece a una subred autorizada y que no está asignada a otro equipo.
02. En Firewall → Virtual IPs pulsar Add y seleccionar Type=IP Alias.
03. Seleccionar la interfaz adecuada e introducir una IP de ejemplo reservada para documentación con el prefijo correcto.
04. Guardar y aplicar los cambios; verificar que la dirección se presenta en la configuración del firewall.

05. En el servicio local correspondiente, elegir explícitamente la dirección de escucha cuando la aplicación lo permita.

06. Comprobar reglas para el puerto y limitar los orígenes; ensayar acceso desde una red de prueba.

Ejemplo didáctico independiente: IP Alias 192.0.2.20/24 en un segmento de laboratorio 192.0.2.0/24. Es un rango TEST-NET reservado para documentación, no una dirección real ni una recomendación de usarlo en Internet.

37.19. Procedimiento práctico B: Proxy ARP para un destino NAT

01. Comprobar que el destino adicional es alcanzable desde el mismo segmento de enlace y que se requiere una respuesta ARP.

02. Crear Type=Proxy ARP, seleccionar interfaz y elegir Address Type según se utilice una IP o un prefijo.

03. Registrar la descripción, guardar y aplicar.

04. Crear una regla Port Forward o 1:1 NAT hacia un host de pruebas, con traducción y restricciones mínimas.

05. Configurar la regla Pass asociada y comprobar que el upstream aprende la respuesta ARP.

06. Realizar una prueba desde otra red; observar NAT, logs y estados; no diagnosticar únicamente mediante ping a la VIP.

37.20. Procedimiento práctico C: Other para un prefijo enrutado

01. Confirmar documentalmente que el upstream enruta el prefijo adicional hacia la IP WAN del firewall o hacia la CARP VIP pertinente.

02. Crear Type=Other para la dirección o red necesaria; elegir interfaz según el esquema de entrega.

03. No esperar respuesta ARP local de ese objeto Other.

04. Crear NAT de entrada/salida o 1:1 según requisitos, más reglas de acceso explícitas.

05. Verificar desde otra red que la ruta upstream entrega tráfico al firewall y que los contadores de estados avanzan.

06. Si no llegan paquetes, diagnosticar primero la ruta del proveedor antes de modificar otras reglas.

Ejemplo didáctico: una WAN ficticia en 198.51.100.0/24 y un bloque adicional 203.0.113.0/28 enrutado por un router ficticio. Ambos pertenecen a bloques TEST-NET para publicaciones; no representan datos de una red real.

37.21. Procedimiento práctico D: CARP compartido en dos nodos

01. Diseñar interfaces equivalentes y conectar ambos nodos al mismo dominio de capa 2 en cada segmento compartido.

02. Asignar direcciones de gestión individuales diferentes y reservar una dirección compartida distinta para CARP.

03. Configurar sincronización de estados y configuración por los mecanismos soportados, con reglas y acceso de administración.

04. Crear VIP CARP con máscara correcta, contraseña compartida, VHID único y valores Base/Skew coherentes.

05. Guardar, aplicar y verificar en Status → CARP (failover) que hay un MASTER y un BACKUP por VIP.

06. Realizar failover controlado; comprobar que la VIP conmuta, los estados necesarios se mantienen y el acceso vuelve.

07. Restituir el nodo preferido y documentar el resultado, la duración y las incidencias sin publicar datos sensibles.

Máscara CARP. Para una VIP CARP de un segmento directamente conectado se usa la máscara real de la red, coincidente con las IP de interfaz de ese segmento: no introducir /32 por costumbre. Comprobar antes que no existe otro VHID en el mismo dominio de enlace.

37.22. Interacción VIP ↔ NAT ↔ reglas de filtrado



Figura 37.3. Secuencia conceptual de entrega, traducción y decisión de filtrado.

La VIP permite que una dirección sea conocida o seleccionable, pero no sustituye NAT ni la política de filtrado. En Port Forward deben verificarse el destino externo, la traducción a la IP interna, el puerto, la interfaz de entrada y la regla de firewall correspondiente. En 1:1 NAT deben examinarse además los posibles efectos sobre el tráfico de salida y las prioridades frente a Outbound NAT.

Para servicios locales, usar direcciones de enlace compatibles con IP Alias o CARP y limitar los orígenes autorizados. Para Proxy ARP y Other, no intentar vincular directamente un servicio pfSense a una dirección que no está configurada como dirección local del sistema.

37.23. Relación con DNS, certificados y puertos de servicios

Publicar una IP adicional no crea registros DNS ni instala certificados TLS. La resolución externa debe apuntar a la IP accesible, la traducción NAT debe llevar al servidor correcto y el servicio debe responder en el puerto esperado. Comprobar también el cortafuegos del servidor destino, rutas de retorno y posibles traducciones en cascada.

Cuando la VIP se destina a la administración o a servicios locales del propio firewall, valorar expresamente si GUI, SSH, DNS o VPN escucha en esa dirección. Evitar exponer administración en una WAN sólo porque se ha añadido una dirección adicional: la superficie de exposición puede aumentar sin una intención explícita.

37.24. VIP y Multi-WAN: interfaces diferentes no equivalen a rutas válidas

Una VIP depende de la interfaz y de la entrega de red concreta. En Multi-WAN no se debe suponer que una IP pública de un operador se conservará al pasar a otra WAN distinta. Una ruta de salida alternativa tampoco cambia por sí sola la ruta con la que el operador entrega la IP publicada. CARP sólo resuelve la posesión compartida de direcciones dentro del segmento adecuado: no es un mecanismo general de migración de IP públicas entre ISP independientes.

37.25. Sincronización XMLRPC y excepciones relevantes

Tipo	¿Se sincroniza como VIP sin más?	Criterio clave
CARP	Sí, si está configurada sincronización de VIPs.	Revisar VHID, contraseña y skew efectivo por nodo.
IP Alias directo	No normalmente.	Evitar conflicto duplicando una dirección local en ambos nodos.
IP Alias sobre CARP	Sí.	Hereda el movimiento de la VIP padre; misma subred.
IP Alias sobre Localhost	Sí.	No se publica como identidad de L2 en ambos nodos.

Tipo	¿Se sincroniza como VIP sin más?	Criterio clave
Proxy ARP	No.	La duplicación podría provocar conflictos de respuesta ARP.
Other	Compatible con diseños HA, según ruteo.	No requiere ARP; revisar la entrega a CARP y reglas NAT.

La sincronización de objetos no equivale a que el clúster esté sano. Comprobar estado de las VIP, interfaces asignadas, anuncios, pfsync y sincronización XMLRPC en sus apartados correspondientes.

37.26. Estado CARP: MASTER, BACKUP e INIT

Estado	Significado operativo	Verificación inmediata
MASTER	Nodo que responde al tráfico de la VIP.	Comprobar que sólo uno ejerce el rol.
BACKUP	Nodo que observa anuncios y puede asumir la VIP.	Verificar anuncios y camino hacia el peer.
INIT / sin estado	VIP no inicializada o interfaz/proceso no preparado.	Comprobar enlace, configuración y eventos.
DISABLED	CARP deshabilitado por control o mantenimiento.	Comprobar ajustes globales y operación planificada.

Ruta: Status → CARP (failover). Un MASTER en cada nodo para la misma VIP es un síntoma de error grave de coordinación (split-brain), no un éxito de redundancia. Comprobar pérdida de anuncios, VHID, contraseña, multicast/unicast y aprendizaje de MAC. En un entorno virtualizado verificar además las políticas del switch virtual.

37.27. Seguridad de CARP y virtualización

Los adaptadores virtuales y vSwitch deben permitir la MAC virtual y el intercambio de anuncios del modo CARP elegido. En determinadas plataformas pueden requerirse opciones como promiscuous mode, forged transmits o MAC address changes; deben revisarse las instrucciones de Netgate específicas del hipervisor. Permitir indiscriminadamente esas capacidades en todas las redes virtuales no es una buena práctica: limitar su alcance al grupo de puertos pertinente.

Los switches físicos también pueden interferir con multicast por storm control, filtrados o IGMP snooping. Evitar bucles de capa 2. El estado CARP puede cambiar si el nodo recibe sus propios anuncios por una topología incorrecta.

37.28. Comprobaciones: ARP/NDP, captura, estados y servicio

Prueba	Resultado esperado	Si falla
Estado de interfaz	Enlace e IP principal válidos.	Revisar puerto, VLAN y direccionamiento.
ARP/ND	La VIP apropiada responde cuando debe.	Tipo, VLAN, switch y vecindad.
CARP	Un MASTER y un BACKUP.	Anuncios, VHID, máscara, password.
Ruteo upstream	Los paquetes del prefijo llegan al firewall.	Ruta de operador/next-hop.
Port Forward / 1:1	La traducción alcanza destino autorizado.	Reglas, NAT, retorno, estados.
Ping	Respuesta sólo cuando el tipo y reglas lo permiten.	No usar ping en Other/Proxy ARP como único test.
Failover	La VIP cambia de propietario sin conflicto.	pfsync, XMLRPC, switch, estados.

Herramientas: Diagnostics → Packet Capture, Diagnostics → ARP Table / NDP Table (según familia y versión), Diagnostics → States y registros del firewall; para CARP, Status → CARP (failover). Un test exterior real debe proceder de otra red, no únicamente de un equipo que comparte el mismo dominio de broadcast.

37.29. Errores frecuentes y resolución de incidencias

Síntoma	Causa probable	Cómo resolver
VIP no accesible desde fuera	No existe ruta o NAT/regla adecuada.	Verificar si llegan paquetes y completar NAT y Pass.
Other no responde a ARP	Comportamiento previsto de Other.	Validar entrega mediante ruta upstream.
Proxy ARP no responde a ping	No hay IP local que conteste ICMP.	Testear servicio NAT en destino, no ping local.
IP Alias expone GUI inesperada	Servicio escucha en todas las IP.	Revisar bind y reglas de administración.
Dos MASTER en CARP	No se reciben anuncios, VHID/MAC en conflicto.	Revisar L2, clave, máscara, multicast/unicast.
CARP en INIT	Interfaz sin enlace o problema de inicialización.	Verificar estado físico/virtual y logs.
VIP cambia pero sesión se corta	Estados no sincronizados o ruta asimétrica.	Revisar pfsync, NAT y trayectos.
Dropdown NAT inmanejable	Expansion de prefijo demasiado amplio.	Reducir prefijo o desactivar expansión.
VIP desaparece tras sincronizar	Tipo no se replica o reglas XMLRPC incorrectas.	Revisar excepciones IP Alias y dirección padre.

37.30. Buenas prácticas de administración y seguridad

- Planificar qué dirección pertenece a cada interfaz, servicio y reglas antes de crear la VIP.
- No publicar administración, DNS u otros servicios en una VIP sin revisar interfaces de escucha.
- No escribir las contraseñas CARP en libros, tickets o capturas distribuidas.
- Reservar y documentar VHID únicos por dominio de capa 2 y evitar colisiones con VRRP.
- Para prefijos enrutados, comprobar el acuerdo de rutas en upstream antes de elegir Other.
- Preferir cambios discretos con copia de configuración, prueba externa y reversión documentada.
- En HA, ensayar conmutación y retorno al nodo preferido, incluyendo estados y servicios clave.
- No interpretar una VIP como control de seguridad ni habilitación automática de reglas Pass.

37.31. Ficha de implantación y reversión

01. Registrar finalidad, tipo de VIP, interfaz genérica, servicio previsto y requisito ARP/ruta.
02. Verificar autorización de uso de las direcciones e inexistencia de conflictos.
03. Guardar copia de la configuración y registrar NAT, reglas y servicios dependientes.
04. Habilitar acceso administrativo alternativo, especialmente antes de cambios de CARP/HA.
05. Aplicar la VIP y validar conectividad, traducciones y escucha según su tipo.
06. Realizar prueba de retorno o failover, con mediciones y capturas anonimizadas.
07. Revertir eliminando cambios de NAT/reglas asociados y restaurando el estado anterior si aparecen anomalías.

37.32. Matriz de aceptación para puesta en producción

Control	Resultado exigido	Evidencia no sensible
VIP registrada	Tipo/interfaz/prefijo correctos.	Ficha con valores de prueba o inventario restringido.
Entrega de red	ARP/ND o ruta, según VIP, funcionan.	Captura redactada y prueba desde red externa.
Seguridad	Sólo puertos/orígenes previstos llegan al servicio.	Pruebas autorizadas Pass/Block.

Control	Resultado exigido	Evidencia no sensible
NAT	Traducción y retorno simétricos.	Registro de prueba y contador de estados.
Servicio local	Escucha sólo en IP autorizadas.	Comprobación de bind y puertos.
CARP (si aplica)	MASTER/BACKUP, failover y recuperación.	Registro anónimo de transición de estados.
Reversión	Se recupera situación inicial sin errores.	Procedimiento probado y responsable de aceptación.

37.33. Glosario de direcciones virtuales

Término	Definición
VIP	Dirección virtual utilizada para NAT, enlace de servicios o redundancia.
IP Alias	Dirección adicional realmente configurada en una interfaz/local.
CARP	Protocolo de coordinación de identidad VIP en alta disponibilidad.
VHID	Identificador del grupo CARP, relacionado con la MAC virtual.
Base / Skew	Temporización y preferencia de los anuncios CARP.
Proxy ARP	Respuesta ARP a IP que no está asignada localmente.
Other	VIP declarativa para NAT cuando el tráfico ya llega por ruta.
NDP / ND	Descubrimiento de vecinos en IPv6.
XMLRPC	Sincronización de configuración de pfSense entre nodos.
pfsync	Mecanismo de sincronización de estados de firewall.
Split-brain	Situación anómala en que ambos nodos creen ser MASTER.

37.34. Referencias oficiales de Netgate

Virtual IP Addresses — tipos y campos — https://docs.netgate.com/pfsense/en/latest/firewall/virtual-ip-addresses.html

Virtual IP Address Feature Comparison — https://docs.netgate.com/pfsense/en/latest/firewall/virtual-ip-address-comparison.html

Methods of Using Additional Public IP Addresses — https://docs.netgate.com/pfsense/en/latest/firewall/additional-ip-addresses.html

High Availability Configuration Example — https://docs.netgate.com/pfsense/en/latest/recipes/high-availability.html

CARP Status — https://docs.netgate.com/pfsense/en/latest/monitoring/status/carp.html

Troubleshooting High Availability — https://docs.netgate.com/pfsense/en/latest/troubleshooting/high-availability.html

Troubleshooting HA in Virtual Environments — https://docs.netgate.com/pfsense/en/latest/troubleshooting/high-availability-virtual.html

Verifying Failover Functionality — https://docs.netgate.com/pfsense/en/latest/highavailability/test.html

Parte IV Services

38 Services → Introducción general

Asignación de red, nombres, sincronización, acceso y servicios auxiliares

Ruta principal: Services (menú superior de pfSense Plus). El apartado reúne servicios proporcionados por procesos del firewall que trabajan para los dispositivos y aplicaciones de la red. Esta introducción describe el alcance de los dieciséis accesos visibles y sus dependencias; los formularios concretos pueden variar según la versión y el backend seleccionado.

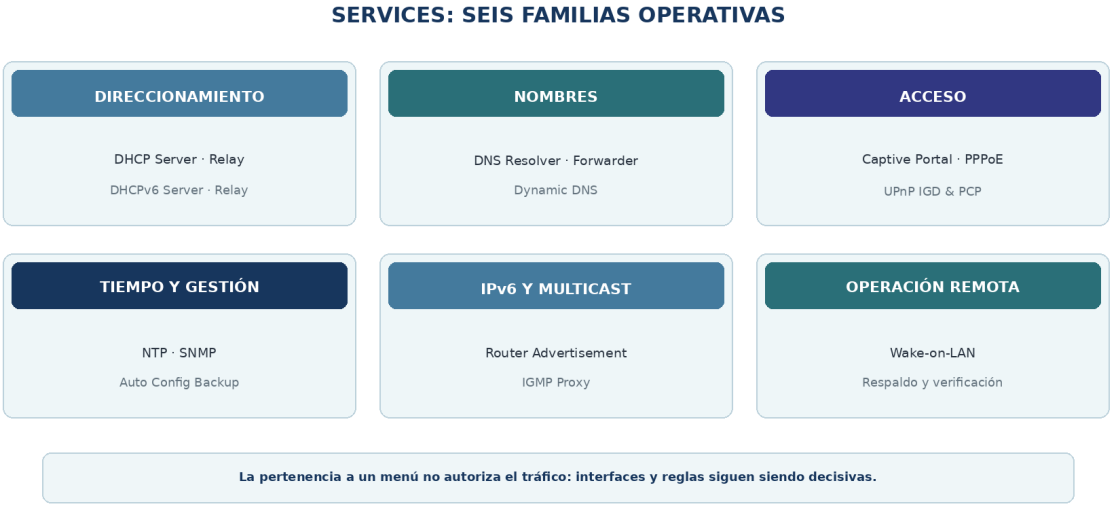


Figura 38.1. Clasificación funcional de las opciones del menú Services.

38.1. Objetivo del apartado Services

El firewall no se limita a filtrar paquetes: puede responder consultas DNS, entregar direcciones IPv4 e IPv6, reenviar peticiones a servidores centrales, sincronizar relojes, ofrecer portales de acceso, publicar telemetría y automatizar tareas de administración. La proximidad de estos mecanismos a las interfaces, al enrutamiento y a las reglas requiere una gestión coordinada.

Cada servicio posee su propia configuración, puede requerir puertos de escucha, interfaces autorizadas, comunicación con servidores externos y registros de funcionamiento. Activarlo no equivale a conceder conectividad universal; las políticas de firewall, el direccionamiento y la topología siguen determinando qué clientes pueden utilizarlo.

38.2. Mapa completo del menú y sus dieciséis entradas

Menú (nombre visible)	Función principal	Dependencia o precaución
Auto Config Backup	Copia cifrada remota de la configuración.	Clave de cifrado, acceso al servicio y restauración comprobada.
Captive Portal	Autenticación o aceptación previa al acceso.	Zonas, reglas, DNS, clientes e incompatibilidad con IPv6.
DHCP Relay	Reenvío DHCPv4 a servidor central.	No coexistir con servidor DHCPv4 local.
DHCP Server	Concesiones y opciones de IPv4.	Pool, gateway, DNS; Kea/ISC.
DHCPv6 Relay	Reenvío DHCPv6 a servicio externo.	No coexistir con servidor DHCPv6 local.
DHCPv6 Server	Entrega de opciones y direcciones IPv6.	Necesita coordinación con RA; no entrega gateway.
DNS Forwarder	Reenvío/caché DNS con dnsmasq.	Conflicto si comparte puerto con resolver.
DNS Resolver	Resolución DNS con Unbound.	ACL, validación DNSSEC, modo resolver/forwarder.

Menú (nombre visible)	Función principal	Dependencia o precaución
Dynamic DNS	Actualización de nombre tras cambiar IP WAN.	Proveedor, IP pública/CGNAT, rutas de retorno.
IGMP Proxy	Retransmisión multicast IPv4.	Un upstream, downstream, reglas multicast.
NTP	Sincronización horaria para la red.	Fuentes horarias y control de consultas.
PPPoE Server	Concentrador PPPoE para clientes locales.	Interfaz, autenticación y direccionamiento.
Router Advertisement	Anuncios de router para IPv6.	SLAAC, DHCPv6 y rutas por defecto.
SNMP	Monitorización remota del equipo.	Control de acceso y credenciales de lectura.
UPnP IGD & PCP	Asignación dinámica de puertos NAT.	Exposición controlada mediante ACL y reglas.
Wake-on-LAN	Envío de paquetes mágicos para despertar equipos.	WOL habilitado en hardware y capa 2.

Alcance de la tabla. Los nombres del menú se toman de la pantalla estudiada. Las funcionalidades y limitaciones se describen a partir de la documentación oficial; no se presupone que todos los servicios estén activados en el dispositivo.

38.3. Modelo de funcionamiento: proceso, interfaz, regla y cliente

El menú Services configura procesos o mecanismos del firewall, pero su funcionamiento está sujeto a cuatro condiciones: un servicio activo y correctamente parametrizado; una interfaz y una dirección donde opera; reglas que permitan los paquetes necesarios; y clientes capaces de utilizarlo. Un quinto factor transversal es la disponibilidad de rutas, resolución DNS, reloj correcto y dependencias de terceros.

Conviene distinguir servicios que escuchan peticiones entrantes (DNS, NTP o DHCP), clientes que ejecutan acciones salientes (Dynamic DNS o copias externas), y funciones que modifican el tránsito de paquetes (Captive Portal o UPnP). Estas funciones tienen perfiles de seguridad muy diferentes.

38.4. Interfaces, VLAN y zonas: dónde funciona cada servicio

Los servicios ligados a segmentos locales deben configurarse en las interfaces correctas. En una red con varias VLAN, la LAN, las redes de invitados y los segmentos de servidores pueden necesitar DHCP y DNS, pero no necesariamente los mismos rangos, resolutores o permisos. La configuración de capa 2 y las asignaciones de interfaces son condiciones previas; no basta con activar una casilla en Services.

Antes de activar una función, responder: ¿qué red genera la petición?, ¿dónde escucha el servicio?, ¿qué protocolo utiliza?, ¿requiere transmisión broadcast/multicast?, ¿existe ruta de retorno? Esta secuencia simplifica incidencias que de otro modo se atribuirían erróneamente al firewall.

38.5. Autenticación, seguridad y privilegio mínimo

La administración de Services debe limitarse a personal autorizado, con registro de cambios y copia de configuración. Los procesos que aceptan conexiones de la red deben escuchar únicamente en las interfaces necesarias cuando el producto lo permita; adicionalmente, las reglas de entrada deben restringir los orígenes. No conviene exponer DNS recursivo, NTP, SNMP ni paneles de administración a Internet de forma indiscriminada.

El Portal cautivo no sustituye segmentación, los servicios DHCP no son mecanismos de autenticación, y UPnP puede abrir puertos dinámicamente. Un servicio técnicamente funcional puede seguir siendo inapropiado desde el punto de vista de seguridad o cumplimiento.

38.6. Relación entre DNS, DHCP, rutas y reloj

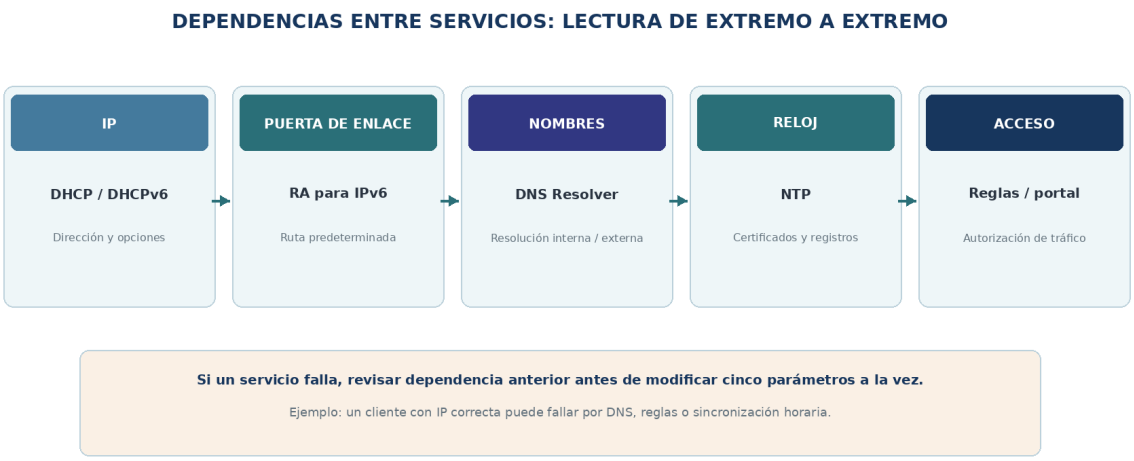


Figura 38.2. Dependencias habituales para que un cliente disponga de conectividad funcional.

Una concesión DHCP válida no implica navegación: un dispositivo puede tener IP pero carecer de ruta correcta, resolución DNS o permiso de paso. Asimismo, una configuración de DNS correcta puede fallar si el propio firewall no tiene conectividad hacia servidores autorizados; y la validación TLS y los registros pueden sufrir si el reloj está desincronizado.

38.7. Auto Config Backup: continuidad de la configuración

Ruta: Services → Auto Config Backup. ACB almacena copias cifradas de la configuración en un servicio remoto de Netgate para facilitar la recuperación ante errores, sustituciones o pérdida del equipo. Su utilidad radica en la independencia respecto del almacenamiento local, aunque requiere proteger adecuadamente la información de recuperación y controlar quién puede restaurarla.

Caso práctico: tras un cambio fallido se conserva una revisión anterior de configuración y se restaura mediante un procedimiento autorizado. Deben registrarse qué copia es válida, su fecha y las dependencias del hardware de destino. La existencia de una copia no demuestra por sí sola que la restauración sea completa ni que el equipo resultante disponga de rutas, certificados o credenciales externas adecuados.

38.8. Captive Portal: control de acceso a redes de usuarios

Ruta: Services → Captive Portal. Permite exigir autenticación, códigos tipo voucher o aceptación mediante un portal antes de autorizar determinados accesos. Puede aplicarse por zonas y utilizar la base local u otros métodos de autenticación. Es habitual en redes de invitados, alojamientos y espacios de acceso temporal, pero no reemplaza un diseño de VLAN y firewall restrictivo.

Punto crítico: la documentación oficial indica que el Captive Portal de pfSense no es compatible con IPv6. Al planificar una zona de invitados deben revisarse los comportamientos de los clientes modernos, los accesos sin portal, los destinos permitidos antes de iniciar sesión y la protección de los datos de autenticación.

38.9. DHCP Relay: centralizar la concesión de IPv4

Ruta: Services → DHCP Relay. La retransmisión permite que clientes de una subred reciban respuestas de un servidor DHCPv4 situado en otra. El firewall recibe las solicitudes en el segmento local y las remite al servidor configurado, superando la frontera habitual de los broadcasts DHCP.

Se utiliza cuando una organización mantiene un sistema DHCP central, por ejemplo para administrar varias VLAN. El relay no sustituye al servidor que asigna direcciones. Netgate indica que el DHCPv4 Relay y el DHCPv4 Server no deben estar activos simultáneamente: antes de migrar, planificar la transición, las rutas hacia el servidor y las reglas que permiten el intercambio.

38.10. DHCP Server: direccionamiento IPv4 automatizado

Ruta: Services → DHCP Server. Proporciona a cada cliente una dirección del rango definido y opciones como máscara, puerta de enlace, DNS, dominio y otras específicas. Cada interfaz con configuración compatible puede tener su propio servicio y sus reservas; los rangos deben pertenecer a la subred apropiada y no solaparse con asignaciones ajenas.

Netgate documenta dos backends: Kea DHCP, recomendado actualmente y mantenido activamente, e ISC DHCP, obsoleto y destinado a desaparecer. Las opciones visibles y las funciones de integración DNS dependen del backend y de la versión. Al introducir Kea es necesario revisar el efecto sobre reservas, DNS y alta disponibilidad; nunca presuponer que una migración es transparente.

38.11. DHCPv6 Relay: retransmisión de solicitudes IPv6

Ruta: Services → DHCPv6 Relay. Reenvía las solicitudes DHCPv6 de los clientes hacia un servidor situado fuera del enlace local. Su objetivo es equivalente al relay IPv4, pero emplea mensajes y multicast IPv6 con estructura distinta. Deben existir rutas IPv6 válidas, permisos adecuados y una configuración de RA compatible con los clientes.

El servicio DHCPv6 Relay no debe funcionar a la vez que el DHCPv6 Server en el firewall. Importa distinguir «recibir dirección IPv6» de «conocer la ruta por defecto»: DHCPv6 no suministra el gateway de los clientes, que se descubre por Router Advertisements.

38.12. DHCPv6 Server: gestión de direcciones y opciones IPv6

Ruta: Services → DHCPv6 Server. Entrega direcciones IPv6 y determinados parámetros de red a los dispositivos que usan DHCPv6. Puede coordinarse con prefijos distribuidos por un proveedor mediante delegación, configuraciones estáticas o modos de anuncio que permitan a los clientes solicitar direcciones.

Hay sistemas que utilizan SLAAC y no un cliente DHCPv6 convencional. Por ello, un diseño IPv6 debe especificar qué se obtiene mediante Router Advertisement y qué se entrega por DHCPv6. Los parámetros de DNS pueden anunciarse en más de un mecanismo; su coherencia debe comprobarse, especialmente en una red con varias plataformas cliente.

38.13. DNS Forwarder: reenvío ligero con caché

Ruta: Services → DNS Forwarder. Basado en dnsmasq, resuelve peticiones locales reenviándolas a servidores DNS configurados u obtenidos dinámicamente y puede mantener una caché. Está orientado al reenvío y no realiza el proceso recursivo completo propio de un resolvedor.

El DNS Forwarder está desactivado por defecto en instalaciones modernas que utilizan DNS Resolver. Ambas funciones no pueden ocupar a la vez el mismo puerto de escucha en las mismas direcciones; cambiar de motor sin planificar los clientes puede producir una interrupción general de resolución de nombres.

38.14. DNS Resolver: resolución recursiva y control DNS

Ruta: Services → DNS Resolver. Utiliza Unbound y es el servicio DNS predeterminado en instalaciones actuales. Puede realizar resolución recursiva consultando servidores raíz y autoritativos, con validación DNSSEC, o funcionar en modo forwarding hacia DNS ascendentes. Permite controlar qué interfaces aceptan consultas y qué redes pueden usarlas.

En empresas puede atender registros locales, consultas de clientes y determinadas necesidades de VPN. Para una conexión multi-WAN, el modo forwarding y los DNS configurados con pasarelas específicas pueden facilitar la continuidad de resolución. No conviene habilitar simultáneamente DNS Resolver y DNS Forwarder en las mismas direcciones y puertos.

38.15. Dynamic DNS: mantener un nombre con WAN cambiante

Ruta: Services → Dynamic DNS. Actualiza registros de un proveedor cuando cambia la IP supervisada de una conexión WAN. Facilita localizar un extremo remoto mediante un nombre estable, por ejemplo para un servicio VPN u otro recurso autorizado, sin depender de memorizar una dirección que puede variar.

El nombre actualizado no crea rutas, puertos abiertos ni conectividad entrante. Si una WAN está detrás de NAT del operador o CGNAT, puede ser imposible aceptar conexiones desde Internet pese a disponer de un

nombre correcto. Al configurar DDNS en multi-WAN, comprobar la IP que publica el proveedor, las interfaces monitorizadas, la caducidad DNS y la ruta de retorno.

38.16. IGMP Proxy: tráfico multicast entre interfaces

Ruta: Services → IGMP Proxy. Permite transmitir suscripciones y tráfico multicast IPv4 entre segmentos cuando un servicio lo necesita, por ejemplo determinadas distribuciones de vídeo IP. Define una interfaz upstream, donde se encuentra la fuente, y una o varias downstream donde están los receptores.

No es un sustituto de enrutamiento unicast, ni basta con añadir una regla Any. Deben revisarse redes permitidas, grupos multicast, TTL, IGMP y reglas apropiadas en la interfaz downstream. Las implementaciones dependen además del comportamiento de los switches y de su gestión multicast.

38.17. NTP: tiempo coherente para operaciones y seguridad

Ruta: Services → NTP. El daemon NTP puede sincronizar el reloj del firewall con fuentes externas y atender a clientes autorizados. Una hora fiable es esencial para correlación de logs, caducidades de certificados, autenticación y tareas programadas. La zona horaria de visualización no equivale a la sincronización del reloj.

Antes de publicar NTP en una red, definir fuentes fiables, interfaces de escucha y restricciones de acceso. Si un cliente no sincroniza, comprobar NTP en el firewall, DNS y conectividad hacia fuentes upstream, reglas UDP/123 y configuración horaria del sistema.

38.18. PPPoE Server: autenticación de sesiones de acceso

Ruta: Services → PPPoE Server. pfSense Plus puede actuar como concentrador PPPoE (servidor), aceptar conexiones de clientes en una interfaz y autenticarlas. Se utiliza en arquitecturas que requieren acceso basado en sesión o validación previa de usuarios, no para configurar la típica conexión PPPoE que el firewall utiliza como cliente hacia un ISP.

Su adopción exige dimensionar sesiones concurrentes, direccionamiento, sistema de autenticación y políticas de firewall. Debe evaluarse el MTU/MSS efectivo y la autenticación antes de activar servicios de producción; una configuración equivocada puede dejar clientes sin conexión o crear un acceso no deseado.

38.19. Router Advertisement: anuncio de rutas IPv6

Ruta: Services → Router Advertisement. Emite anuncios ICMPv6 que informan a los clientes de los routers, prefijos y parámetros de configuración. La documentación detalla modos como Disabled, Router Only, Unmanaged, Managed y Assisted, que definen el uso de SLAAC y DHCPv6. Los clientes suelen aprender su gateway IPv6 mediante RA, no por DHCPv6.

Es un mecanismo crítico para la conectividad IPv6: un RA erróneo puede modificar la ruta por defecto o anunciar un prefijo inapropiado. Conviene separar las redes IPv6 por interfaz, valorar el soporte SLAAC/DHCPv6 de los equipos y comprobar que los switches y políticas de seguridad no bloquean los mensajes ICMPv6 imprescindibles.

38.20. SNMP: supervisar sin conceder administración general

Ruta: Services → SNMP. El demonio integrado bsnmpd expone métricas seleccionadas de CPU, memoria, interfaces, tráfico o recursos disponibles mediante MIB. Los sistemas de monitorización autorizados pueden consultarlo de forma periódica y, según módulos, recibir determinados traps.

El acceso SNMP debe restringirse a la red de monitorización y a sus direcciones concretas. Evitar comunidades triviales, tratar la cadena de lectura como secreto y no asumir que toda versión SNMP proporciona cifrado. La monitorización no sustituye al seguimiento de logs, disponibilidad de gateways y pruebas de aplicación.

38.21. UPnP IGD & PCP: apertura dinámica de puertos

Ruta: Services → UPnP IGD & PCP. Permite que aplicaciones o dispositivos clientes soliciten mapeos de puertos y reglas NAT dinámicas, útil en determinados servicios de comunicación o consolas. PCP puede atender clientes compatibles con NAT-PMP. Es una función distinta a las reglas de Port Forward creadas manualmente.

Es potencialmente arriesgada en una red corporativa porque un cliente puede solicitar exposición entrante sin aprobación manual por cada caso. Si es imprescindible, limitar interfaces internas, aplicar ACL de denegación por defecto, autorizar equipos y puertos específicos y auditar los mapeos resultantes. Detrás de CGNAT no puede garantizarse publicación real por el hecho de activar el servicio.

38.22. Wake-on-LAN: despertar equipos de forma controlada

Ruta: Services → Wake-on-LAN. Envía paquetes mágicos a la dirección MAC de dispositivos compatibles para encenderlos o despertarlos, siempre que su firmware, NIC, alimentación y red lo permitan. Se pueden guardar entradas reutilizables y emitir el paquete al equipo seleccionado.

No constituye una herramienta de encendido universal: no reemplaza un sistema de gestión fuera de banda y depende de la capacidad WoL del destino. El paquete mágico no incorpora autenticación por sí mismo; por ello conviene limitar qué estaciones tienen WoL activo y no exponer mecanismos de activación sin control.

38.23. Arquitecturas DHCP: servidor local frente a relay

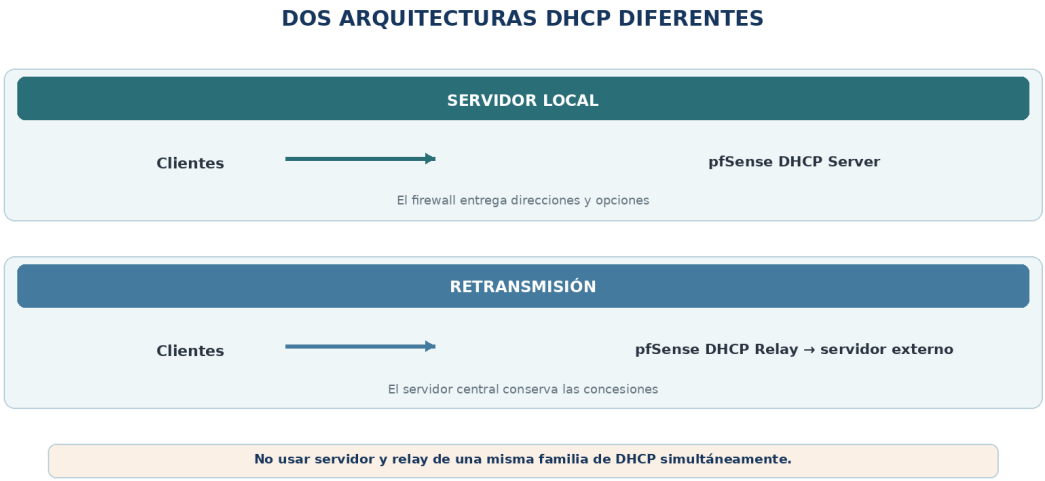


Figura 38.3. Diferencia entre el firewall como servidor DHCP y como retransmisor hacia un servidor central.

La elección de servidor frente a relay afecta a quién almacena concesiones, desde dónde se envían opciones, cómo se administran reservas y qué dependencia introduce la conexión entre segmentos. En redes sencillas suele ser suficiente el DHCP local; en estructuras con directorio y DNS dinámico centralizado puede justificarse el relay. En ambos casos se debe evitar superposición de pools y DHCP no autorizado.

38.24. Puertos y protocolos habituales de servicios

Servicio	Puertos / protocolo típicos	Observación profesional
DHCPv4	UDP 67/68	Broadcast local o relay al servidor.
DHCPv6	UDP 546/547	Multicast y relay de IPv6.
DNS	TCP/UDP 53	No compartir escucha entre motores.
NTP	UDP 123	Restringir a fuentes y clientes autorizados.
SNMP	UDP 161; traps 162	No exponer al exterior ni usar comunidad simple.
PPPoE	EtherType 0x8863 / 0x8864	Protocolo de capa 2; no es TCP/UDP.
RA IPv6	ICMPv6 tipo 134	Necesario para puerta de enlace IPv6.
IGMP	Protocolo IP 2	Control multicast, no puerto TCP/UDP.
UPnP / PCP	UDP 1900/5351; TCP 2189	Descubrimiento y control de mapeos.

Servicio	Puertos / protocolo típicos	Observación profesional
WoL	Magic Packet en enlace local	No depender de un puerto fijo como único criterio.
ACB / DDNS	Conexiones de cliente según proveedor	Comprobar salida y TLS, no publicar servicio.
Advertencia técnica. Las referencias de puertos son habituales, no una plantilla de reglas que deba habilitarse indiscriminadamente. Algunos servicios usan multicast, tráfico de capa 2 o puertos configurables.		

38.25. Caso empresarial A: red de oficina con servicios básicos

01. Definir interfaces y subredes de usuarios, servidores y dispositivos, evitando solapamientos.
02. Configurar DHCP Server sólo en las interfaces que deban proporcionar concesiones locales.
03. Elegir DNS Resolver y comprobar que los clientes reciben la dirección de DNS apropiada.
04. Verificar que el firewall mantiene el reloj sincronizado y que NTP atiende sólo a redes internas autorizadas.
05. Aplicar reglas de interfaz que permitan los servicios necesarios y bloqueen el resto.
06. Probar un alta de cliente: concesión IP, gateway, DNS, acceso a servicios y registro de incidencias.

38.26. Caso empresarial B: DHCP centralizado en varias VLAN

01. Identificar un servidor DHCP central y confirmar que dispone de ámbitos válidos para cada VLAN.
02. Desactivar el servidor DHCPv4 local antes de poner en marcha Relay, según las restricciones del producto.
03. Seleccionar las interfaces de clientes y el destino del servidor de retransmisión.
04. Revisar reglas, rutas y disponibilidad del servidor central durante la puesta en servicio.
05. Probar concesiones y renovación desde cada segmento; registrar tiempos y opciones recibidas.
06. Prever reversión controlada para evitar periodos sin DHCP o dos fuentes de respuesta.

38.27. Caso empresarial C: IPv6 gestionado con RA y DHCPv6

01. Verificar el prefijo IPv6 local, la ruta externa y la delegación si procede.
02. Elegir el modo de Router Advertisement que corresponda a los clientes y a la política de direcciones.
03. Activar DHCPv6 Server únicamente si se precisa y resulta compatible con el modo RA elegido.
04. Definir DNS y verificar que los sistemas exclusivamente SLAAC siguen obteniendo configuración adecuada.
05. Probar ruta por defecto, consultas DNS, acceso IPv6 e ICMPv6 necesarios.
06. Inspeccionar registros y corregir anuncios indebidos antes de añadir reglas de apertura general.

38.28. Caso empresarial D: invitados, supervisión y respaldo

Una red de visitantes puede necesitar Captive Portal con condiciones de acceso, mientras que la monitorización interna obtiene métricas mediante SNMP y el administrador dispone de copias ACB. Conviene separar estas funciones por redes y permisos: los invitados no necesitan alcanzar SNMP, los agentes de monitorización no deben compartir las credenciales de gestión y un portal no debe utilizarse como única barrera de seguridad.

Si el enlace cambia de dirección, Dynamic DNS puede mantener un nombre de acceso. Sin embargo, la accesibilidad entrante dependerá del operador, el NAT, los VIP y las reglas. Antes de considerar el servicio publicado, realizar pruebas externas autorizadas y no sólo desde el mismo segmento.

38.29. Inspección inicial sin modificar la configuración

01. Abrir Services y recorrer las dieciséis entradas para conocer el catálogo disponible.
02. Consultar Status → Services para identificar qué demonios están activos y su estado real.

03. Comprobar qué backend DHCP está seleccionado y si se usa servidor o relay para cada familia IP.
04. Determinar si el DNS del firewall funciona con Resolver o Forwarder y en qué interfaces escucha.
05. Revisar NTP, DDNS, portales, SNMP y otros servicios expuestos únicamente a redes autorizadas.
06. Registrar dependencias entre servicio, interfaz, dirección de escucha, reglas y servidor externo.
07. Conservar un inventario sin credenciales, direcciones operativas ni identificadores únicos.

38.30. Procedimiento general de cambio y reversión

01. Documentar objetivo, alcance, servicio afectado y resultado verificable.
02. Guardar copia de configuración y confirmar acceso administrativo alternativo.
03. Comprobar incompatibilidades: DHCP con Relay, DNS en puertos compartidos, RA y backend IPv6.
04. Modificar un único servicio de cada vez y guardar/aplicar sus cambios según corresponda.
05. Validar el funcionamiento desde un cliente de prueba y revisar registros y estado del demonio.
06. Comprobar que no se ha abierto tráfico adicional ni afectado a otras redes.
07. Si no cumple la aceptación, restaurar los ajustes previos y revalidar DHCP, DNS y acceso.

38.31. Diagnóstico: fallos habituales y comprobaciones

Síntoma	Qué revisar primero	Pista técnica
El cliente no obtiene IPv4	VLAN, interfaz, pool y backend.	Doble DHCP o relay/servidor incompatible.
Recibe IP pero no navega	Gateway, DNS, NAT y reglas.	No todo fallo de conexión es DHCP.
IPv6 sin salida	RA, prefijo, ICMPv6, rutas.	El gateway no se entrega por DHCPv6.
DNS deja de responder	Servicio, puerto 53, ACL, upstream.	Resolver/Forwarder compiten en misma escucha.
Portal no aparece	Zona, DNS, cliente y familia IP.	Portal no compatible con IPv6.
DDNS resuelve, pero no conecta	IP publicada, CGNAT, NAT, reglas.	Un nombre correcto no abre conexiones.
NTP desincronizado	DNS de upstream, fuentes y estado.	Reloj afecta certificados y eventos.
SNMP no responde	ACL, comunidad y puerto UDP.	Verificar origen de monitorización.
Multicast ausente	IGMP, upstream/downstream, reglas.	Comprobar switches y TTL.
WoL no enciende	BIOS/UEFI, NIC, energía y segmento.	El equipo puede no admitir WoL activo.

38.32. Controles de seguridad, rendimiento y continuidad

- Exponer únicamente los servicios necesarios; limitar las interfaces de escucha y las reglas de acceso.
- Usar secretos y credenciales robustos y guardarlos sólo en repositorios autorizados.
- Evitar resolver DNS abierto, SNMP accesible desde Internet y UPnP sin controles de acceso.
- Mantener el backend DHCP dentro de versiones soportadas y documentar migraciones a Kea.
- Verificar IPv4 e IPv6 por separado; revisar clientes que sólo admiten SLAAC.
- Reducir el registro excesivo si compromete recursos, pero mantener trazabilidad suficiente.
- Separar redes de usuarios, servicios, invitados y administración.
- Revisar el impacto de cambios sobre VPN, enlaces de respaldo, DNS y acceso administrativo.
- Mantener copias de configuración y ensayar recuperación antes de una intervención sensible.

Operación segura. Desactivar DHCP o DNS sin una alternativa preparada puede afectar de forma masiva a usuarios, aplicaciones, actualizaciones y VPN. Los cambios en RA pueden hacer que los clientes IPv6 pierdan su puerta de enlace. Planificar ventana y reversión.

38.33. Matriz de aceptación para servicios esenciales

Control	Criterio de aceptación	Prueba documentable
Direccionamiento IPv4	Cliente obtiene IP y opciones correctas.	Liberar/renovar concesión en entorno de prueba.
Direccionamiento IPv6	Prefijo, RA y ruta adecuados.	Consulta de dirección/rutas en cliente.
DNS	Resuelve nombres internos y externos.	Consultas A, AAAA y nombre interno.
NTP	Reloj del firewall sincronizado.	Estado NTP y contraste horario.
Protección de acceso	Sólo redes previstas usan servicios.	Prueba autorizada desde origen permitido/denegado.
Portal / PPPoE	Acceso correcto tras autenticación.	Prueba con usuario de ensayo.
Monitorización	Agente consulta sólo métricas esperadas.	Consulta de prueba con credencial temporal.
Continuidad	Copias y reversión localizadas.	Revisión de una copia y plan ensayado.

38.34. Glosario esencial

Término	Significado
Daemon / servicio	Proceso del firewall que atiende o genera funciones de red.
DHCP / DHCPv6	Protocolos para asignar parámetros en IPv4 o IPv6.
Relay	Retransmisión de solicitudes a un servidor ubicado en otra subred.
Kea	Backend DHCP moderno recomendado por Netgate.
ISC DHCP	Servidor legado DHCP en proceso de retirada.
SLAAC	Autoconfiguración IPv6 a partir de anuncios de router.
RA	Router Advertisement: anuncio IPv6 con información de enrutamiento.
Unbound / dnsmasq	Implementaciones del DNS Resolver / DNS Forwarder.
DDNS	Actualización dinámica de información DNS.
IGMP	Protocolo de gestión de pertenencia a grupos multicast IPv4.
NTP / SNMP	Sincronización de tiempo / monitorización de dispositivos.
UPnP / PCP	Mecanismos de creación dinámica de mapeos y puertos.
WOL	Wake-on-LAN, activación mediante paquete mágico.
ACB	Auto Config Backup, copia externa cifrada de configuración.

38.35. Referencias oficiales de Netgate

Guía de menú Services — https://docs.netgate.com/pfsense/en/latest/menuguide/services.html

Servicios — Índice general — https://docs.netgate.com/pfsense/en/latest/services/index.html

Automatic Configuration Backup — https://docs.netgate.com/pfsense/en/latest/backup/acb.html

Captive Portal y limitaciones — https://docs.netgate.com/pfsense/en/latest/captiveportal/index.html

DHCP — tipos y backend Kea/ISC — https://docs.netgate.com/pfsense/en/latest/services/dhcp/index.html

DHCPv4 & DHCPv6 Relay — https://docs.netgate.com/pfsense/en/latest/services/dhcp/relay.html

DHCPv6 Server — https://docs.netgate.com/pfsense/en/latest/services/dhcp/ipv6.html

DNS Resolver — configuración — https://docs.netgate.com/pfsense/en/latest/services/dns/resolver-config.html

DNS Forwarder — configuración — https://docs.netgate.com/pfsense/en/latest/services/dns/forwarder-config.html

Dynamic DNS — introducción — https://docs.netgate.com/pfsense/en/latest/services/dyndns/index.html

IGMP Proxy — https://docs.netgate.com/pfsense/en/latest/services/igmp-proxy.html

NTP Server Configuration — https://docs.netgate.com/pfsense/en/latest/services/ntpd/server.html

PPPoE Server — https://docs.netgate.com/pfsense/en/latest/services/pppoe-server.html

IPv6 Router Advertisements — https://docs.netgate.com/pfsense/en/latest/services/dhcp/ipv6-ra.html

SNMP — https://docs.netgate.com/pfsense/en/latest/services/snmp.html

UPnP IGD & PCP — https://docs.netgate.com/pfsense/en/latest/services/upnp.html

Wake on LAN — https://docs.netgate.com/pfsense/en/latest/services/wake-on-lan.html

39 Services → Auto Configuration Backup

Copias cifradas, histórico remoto, restauración y verificación operativa

Ruta: Services → Auto Config Backup. El servicio se organiza en tres pestañas: Settings, Restore y Backup Now. AutoConfigBackup (ACB) protege la configuración frente a cambios fallidos, pérdidas del almacenamiento o sustituciones del equipo, pero necesita una estrategia verificable de recuperación.



Figura 39.1. Flujo general de copia, cifrado, envío y validación del respaldo remoto.

39.1. Finalidad y alcance del servicio

AutoConfigBackup es un mecanismo integrado de pfSense Plus para conservar fuera del firewall versiones cifradas de su archivo de configuración. Su activación no crea una imagen completa del disco ni almacena necesariamente el estado transitorio de todos los procesos, archivos externos de paquetes o datos añadidos manualmente fuera de config.xml.

Su aportación principal es disponer de puntos de restauración protegidos contra una pérdida local del equipo. Es especialmente útil antes de modificaciones en NAT, reglas, interfaces, pasarelas, VPN y servicios. Una copia remota no reemplaza un inventario de hardware, el acceso de recuperación, la compatibilidad de software o una copia local independiente.

39.2. Ubicación y estructura de las tres pestañas

Pestaña	Ruta	Finalidad / alcance
Settings	Services → Auto Config Backup → Settings	Activación, periodicidad, identificación, cifrado, retención y presentación.
Restore	Services → Auto Config Backup → Restore	Consultar revisiones remotas; ver, descargar, borrar y restaurar entradas.
Backup Now	Services → Auto Config Backup → Backup Now	Generar una revisión manual con razón identificativa antes o después de cambios.
Nota técnica. La organización en tres pestañas corresponde a las funciones oficiales de AutoConfigBackup. Algunos controles y etiquetas pueden variar ligeramente según la versión instalada.		

Desde el punto de vista operativo, Settings define la política de creación de copias; Restore controla su localización, inspección y recuperación; y Backup Now documenta hitos de mantenimiento. Un equipo responsable de redes necesita permisos de gestión, secretos custodiados y un procedimiento de validación independiente de la persona que ejecutó el cambio.

39.3. Qué guarda ACB y qué no guarda

Elemento	Tratamiento típico	Implicación de administración
config.xml	Base de la configuración y parámetros habituales.	Conservarlo permite reconstruir gran parte del servicio.
Reglas, NAT, gateways y servicios	Se reflejan cuando forman parte de la configuración.	Restaurar puede cambiar rutas, políticas y acceso.
Credenciales, certificados y material VPN	El archivo puede contener información sensible.	No distribuir ni publicar el XML descifrado.
Datos del SO y cambios manuales	No equivalen a una imagen del disco.	Prever instalador y documentación de cambios externos.
Datos ajenos a config.xml	Algunos paquetes pueden requerir procedimientos propios.	Verificar recuperación de cada componente crítico.

Netgate describe ACB como una copia cifrada de la configuración enviada por HTTPS. Es una estrategia de respaldo de configuración, no un servicio de replicación de tráfico, un clúster de alta disponibilidad ni una garantía automática de tiempo de recuperación.

39.4. Arquitectura técnica del mecanismo de respaldo

01. Un cambio relevante, una programación o una orden manual provoca la preparación de una copia.
02. El firewall cifra la configuración localmente con la contraseña indicada por el administrador.
03. La copia cifrada y los metadatos se colocan en una cola local de envío.
04. El proceso revisa periódicamente las entradas pendientes, aproximadamente cada minuto.
05. El equipo envía el respaldo cifrado por HTTPS a los servidores de ACB de Netgate, asociado a su Device Key.
06. En Restore, el administrador puede consultar las revisiones almacenadas y comprobar la fecha y razón.

El cifrado documentado es AES-256-CBC. La contraseña de cifrado se utiliza localmente; el dato de identificación del dispositivo y los metadatos de la revisión son diferentes del contenido cifrado. La comprobación debe atender a la llegada efectiva de la copia, no sólo al mensaje inicial de creación.

39.5. Settings: vista general y alcance exacto

La pestaña Settings agrupa ocho áreas principales: Enable ACB; Backup Frequency; Device Key, con descarga y Change Key; Encryption Password y confirmación; Hint/Identifier; Manual Backup Limit; Descending Date Order; y el botón Save. Cuando se elige la periodicidad programada aparece además un bloque Schedule.

Campo o control	Función	Resultado de modificarlo
Enable ACB	Habilita el mecanismo de copia automática.	La desactivación detiene la creación automática; Backup Now puede no estar accesible.
Backup Frequency	Selecciona cambio relevante o calendario.	Modifica cuándo se producen las revisiones.
Device Key / Change Key	Identifica el conjunto remoto de copias.	Una nueva clave separa los históricos.
Encryption Password / Confirm	Establece secreto para el cifrado local.	Una nueva contraseña impide leer históricos anteriores sin la antigua.
Hint/Identifier	Metadato opcional, no cifrado.	Puede ayudar a Netgate TAC a localizar una clave perdida.
Manual Backup Limit	Reserva histórica de entradas manuales.	Regula retención en el máximo total.
Descending Date Order	Invierte el orden visual del listado.	No modifica el contenido de ninguna revisión.
Save	Guarda los parámetros.	Aplica la nueva política de ACB.

39.6. Settings → Enable ACB

La casilla Enable automatic configuration backups pone en funcionamiento AutoConfigBackup. Activada, el firewall genera respaldos según Backup Frequency; desactivada, no se programan copias automáticas mediante este servicio. La comprobación debe hacerse revisando Restore y los registros, no únicamente observando la casilla marcada.

Antes de habilitar ACB se deben definir la custodia de Device Key y Encryption Password, la política de retención, el acceso de salida HTTPS y la responsabilidad de comprobar las revisiones. En un equipo aislado de Internet, este mecanismo remoto no reemplaza una copia local segura.

39.7. Settings → Backup Frequency: por cambio o por calendario

Modalidad	Funcionamiento	Cuándo conviene
Automatically backup on every configuration change	Genera una copia ante cambios significativos; se pueden ignorar modificaciones menores.	Cambios relativamente poco frecuentes y necesidad de granularidad.
Automatically backup on a regular schedule	Usa una planificación tipo cron; no crea copia duplicada si nada cambió.	Equipos con cambios muy frecuentes o política operativa periódica.

La modalidad por cambio no es un sistema de auditoría de cada pulsación de la GUI. La programada simplifica el volumen de revisiones, pero puede dejar fuera un cambio problemático realizado poco antes del siguiente horario. Los respaldos manuales antes y después de una actuación importante complementan ambas opciones.

39.8. Settings → Schedule: opciones que aparecen al elegir horario

Netgate documenta los controles Minute, Hour, Day of Month, Month y Day of Week, basados en expresiones cron. La configuración predeterminada equivale a una revisión diaria durante la hora de medianoche, con minuto aleatorio inicial hasta guardar. Si el archivo no se ha modificado, el ciclo puede no generar una entrada nueva.

Componente	Significado	Recomendación
Minute	Minuto de ejecución dentro de cada hora.	Escalonar equipos para evitar picos simultáneos.
Hour	Hora de ejecución.	Escoger ventana con conectividad remota.
Day of Month	Día del mes o comodín.	Evitar cron complejos sin comprobación.
Month	Mes del año o comodín.	Ajustar únicamente si lo justifica la retención.
Day of Week	Día semanal o comodín.	Verificar interpretación cron y zona horaria.
Ritmo recomendado. La documentación de Netgate sugiere normalmente una copia diaria; en general, no incrementar innecesariamente la frecuencia. Si se necesitan respaldos frecuentes, suele ser más adecuado el modo por cambio.		

39.9. Settings → Device Key: identidad de las revisiones

Device Key es una clave de identificación única para buscar, asociar y gestionar los respaldos remotos de un dispositivo. No es la contraseña que cifra el contenido: el valor permite localizar el histórico, mientras la contraseña permite descifrarlo. La clave se considera secreta, porque su conocimiento puede permitir manipular las copias asociadas.

La página muestra la clave, un icono para descargarla y el botón Change Key. Su valor nunca debe incorporarse a manuales, capturas de difusión ni documentación sin protección. Guardar una copia segura fuera del propio firewall es imprescindible para una recuperación tras pérdida completa del almacenamiento.

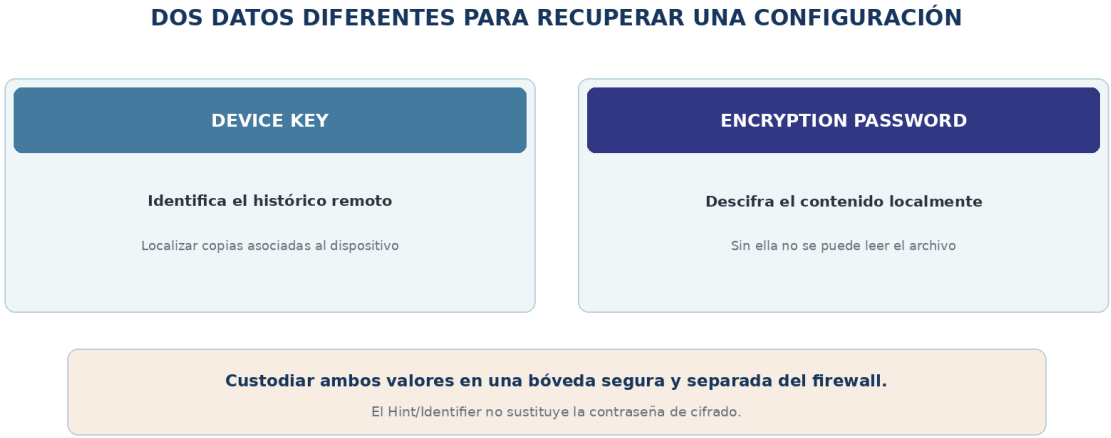


Figura 39.2. Identificación de respaldos y descifrado: secretos independientes y complementarios.

39.10. Settings → Change Key: procedimiento y riesgos

Change Key abre la página específica para cambiar el identificador del dispositivo. Netgate exige una nueva clave de 64 caracteres hexadecimales si se introduce manualmente y ofrece Generate New Key. El procedimiento presenta una advertencia que se debe aceptar antes de poder seleccionar Update Key.

01. Inventariar las copias remotas existentes y registrar su fecha de último respaldo.
02. Descargar y custodiar Current Device Key y, si existe, Legacy Device Key.
03. Abrir Change Key y generar una clave nueva o introducir una válida de 64 caracteres hexadecimales.
04. Leer la advertencia, confirmar la aceptación y seleccionar Update Key.
05. Conservar la clave antigua para recuperar el histórico anterior y proteger la nueva en bóveda.
06. Producir y verificar una nueva revisión asociada a la clave actual.

Riesgo de pérdida de histórico. Cambiar Device Key no transforma ni migra automáticamente las copias antiguas: el histórico anterior se consulta usando la clave antigua y la contraseña correspondiente. No sustituir este procedimiento por pruebas improvisadas.

39.11. Settings → Encryption Password y confirmación

Encryption Password define la contraseña que utiliza ACB para cifrar y descifrar las copias. El segundo campo confirma su escritura para evitar errores. Netgate indica cifrado AES-256-CBC en el equipo y aclara que esta contraseña no se transmite a sus servidores como una credencial de acceso.

La contraseña debe ser larga, robusta y única; su custodia ha de incluir un segundo custodio o procedimiento empresarial autorizado. Perderla impide recuperar el contenido de las copias cifradas con ella. Cambiarla modifica el cifrado de las copias futuras; para consultar anteriores será necesario restablecer la contraseña antigua según el procedimiento de recuperación previsto.

39.12. Settings → Hint/Identifier: utilidad y exposición

Hint/Identifier admite una referencia opcional para distinguir un dispositivo ante incidencias. El texto se envía y almacena como metadato en claro, visible para Netgate TAC según la documentación oficial. Su misión posible es facilitar que soporte identifique una clave perdida, sin garantía de recuperación.

No incluir nombres personales, información interna de sedes, IP, dominios privados, teléfonos ni credenciales. Puede elegirse una etiqueta genérica o dejarse vacío. No confundir este campo con un mecanismo de autenticación o con un sustituto de la contraseña.

39.13. Settings → Manual Backup Limit y retención remota

Netgate documenta un máximo de 100 respaldos por Device Key. Dentro de ese total, pueden conservarse hasta 50 entradas manuales protegidas frente a la sustitución por respaldos automáticos; cuando se supera el límite de manuales establecido, se eliminan las entradas manuales más antiguas.

Concepto	Límite documentado	Consecuencia
Histórico remoto por Device Key	Hasta 100 entradas.	Las nuevas revisiones desplazan las que sobrepasen el máximo.
Entradas manuales protegidas	Hasta 50 entradas dentro de esas 100.	No son inmunes a exceder su propio límite.
Manual Backup Limit	Número de revisiones manuales que se desea preservar.	Establece la política de retención de respaldos etiquetados.

La retención no equivale a almacenamiento ilimitado ni sustituye el archivado corporativo. Es importante extraer de forma segura revisiones extraordinarias que deban mantenerse a largo plazo y verificar el cumplimiento de políticas de privacidad y conservación.

39.14. Settings → Descending Date Order y Save

Descending Date Order hace que Restore muestre primero los respaldos más nuevos. Si se deja desmarcada, el orden predeterminado es del más antiguo al más reciente. La casilla no altera ni cifra los respaldos: sólo cambia su presentación en el listado.

Save registra las opciones elegidas. Debe comprobarse después el efecto: revisar que ACB sigue activado, que la cadencia coincide con la política, que se ha conservado la contraseña de descifrado en el lugar previsto y que aparece una entrada nueva en Restore cuando corresponda.

39.15. Restore: estructura y propósito

La pestaña Restore permite consultar respaldos asociados a la clave seleccionada. Según la documentación de Netgate, incluye sección Device Key, lista Automatic Configuration Backups, búsqueda de otra clave y herramientas para revisar, descargar, eliminar o restaurar revisiones. Al cambiar la clave consultada no se cambia necesariamente el identificador configurado en Settings.

Columna del listado	Qué representa	Precaución
Local Date/Time	Fecha de la revisión adaptada a la zona horaria del firewall.	El servidor almacena referencias temporales en UTC.
Configuration Change	Motivo de cambio o razón de copia manual.	No presuponer que describe todos los cambios.
Actions	Restaurar, inspeccionar, descargar o eliminar.	Las acciones destructivas requieren control de cambios.

39.16. Restore → Device Key, Search y Reset

Device Key muestra el identificador en uso para consultar el histórico. El icono de descarga permite conservarlo de forma segura. Introduciendo otro identificador y pulsando Search puede visualizarse temporalmente su histórico, por ejemplo durante la sustitución de hardware; Reset devuelve la consulta a la clave original.

En equipos que conservan una Legacy Device Key puede aparecer un control para alternar entre el histórico legado y el actual. Las opciones disponibles dependen de la existencia de esa clave heredada y de la versión de ACB.

39.17. Restore → acciones de las revisiones

Control	Función documentada	Recomendación operativa
Restore (flecha de retorno)	Descarga, descifra y restaura la entrada seleccionada.	Revisar impacto y acceso alternativo.
View / Details	Abre Revision con metadatos y contenidos.	Tratar el XML descifrado como secreto.
Download this revision	Descarga una copia XML de la revisión.	Conservarla en repositorio cifrado autorizado.
Delete	Elimina la revisión remota seleccionada.	Confirmar que no es la última copia íntegra.
Hosted / Staged count	Muestra entradas alojadas y, si procede, pendientes.	Distinguir cola local y respaldo confirmado.

39.18. Restore → Revision: lectura de detalles

La vista Revision puede mostrar Service Date/Time (UTC), Local Date/Time, Revision Reason, SHA256 Summary, Encrypted config.xml y Decrypted config.xml, además de botones de Restore y Download this revision. El resumen SHA-256 sirve para contrastar la integridad de datos, pero no demuestra que el backup sea compatible ni funcional en el equipo de destino.

Información sensible. Nunca pegar en tickets, documentación o mensajería un config.xml descifrado. Puede incluir contraseñas, material de VPN, certificados, información de redes y otros secretos incluso cuando el dispositivo tenga accesos de usuario correctamente protegidos.

39.19. Restore → procedimiento seguro para revertir cambios

01. Registrar síntoma, revisión actual, impacto y ventana de intervención.

02. Garantizar un respaldo actual verificable, preferentemente también una copia local independiente.

03. Identificar una revisión anterior consistente y revisar fecha y motivo; examinar diferencias cuando se disponga de medios seguros.

04. Confirmar que se conoce la contraseña necesaria y que la conectividad con Netgate funciona.

05. Seleccionar Restore en la entrada elegida y aceptar la confirmación sólo tras verificar su identidad.

06. Atender el aviso de reinicio: si la revisión modifica más que reglas NAT/firewall, preparar el reinicio recomendado por Netgate.

07. Comprobar tras la recuperación la GUI, interfaces, DHCP, DNS, rutas, VPN, NAT y servicios críticos.

08. Registrar el resultado y conservar un camino de retorno si la recuperación no alcanza el objetivo.

En cambios que afectan exclusivamente a reglas de firewall o NAT, pfSense puede recargar la configuración sin reiniciar automáticamente. En cambios de interfaces u otros componentes se requiere reinicio para aplicar toda la configuración restaurada. No efectuar estas operaciones sin acceso de consola o vía alternativa cuando una pérdida de conectividad sea plausible.

39.20. Restore → recuperación tras avería completa del dispositivo

01. Instalar una versión y plataforma de pfSense Plus compatibles con la configuración que se desea recuperar.

02. Obtener conectividad mínima de gestión y salida hacia el servicio ACB; si WAN exige parámetros especiales, configurarlos temporalmente.

03. Acceder a Settings e introducir la contraseña de cifrado correspondiente al respaldo antiguo.

04. Entrar en Restore, introducir la antigua Device Key y seleccionar Search.

05. Localizar la revisión válida, verificar contexto y confirmar Restore.

06. Aceptar el reinicio cuando se solicite y verificar asignación de interfaces y direccionamiento tras el arranque.

07. Revisar conectividad LAN/WAN, VLAN, VPN, gateways, DNS, DHCP, reglas y paquetes dependientes.

Restaurar en hardware distinto puede cambiar nombres de adaptadores, mapeo de puertos o funcionalidades especiales. Además, la compatibilidad depende de la revisión del formato de configuración y de la versión de destino. Si existe riesgo, ajustar las interfaces desde la consola y comprobar la compatibilidad antes de poner el equipo en producción.



Figura 39.3. Secuencia de recuperación operativa tras un fallo de configuración o de hardware.

39.21. Backup Now: crear una entrada manual

Backup Now está orientada a registrar un punto de recuperación deliberado con una descripción administrativa. Netgate documenta el campo Revision Reason, la comprobación de Device Key y el botón Backup. Esta pestaña no se ofrece cuando ACB está deshabilitado.

Campo / botón	Función	Uso recomendado
Revision Reason	Etiqueta que explica por qué se crea la revisión.	Indicar una razón funcional sin datos sensibles.
Device Key	Identificador bajo el que se guardará el backup.	Confirmar que corresponde al historial deseado.
Backup	Prepara la copia cifrada para subida.	Comprobar resultado en Restore tras el proceso.

39.22. Backup Now → procedimiento antes de una actuación importante

01. Confirmar que ACB está habilitado y se dispone de la clave y la contraseña custodiadas.
02. Acceder a Backup Now y redactar una razón inequívoca, por ejemplo «Estado validado previo a mantenimiento».
03. Verificar Device Key sin copiar ni difundir su valor en registros ajenos al proceso.
04. Pulsar Backup y comprobar que no existen avisos de error.
05. Tras al menos un minuto, entrar en Restore y confirmar que aparece la revisión etiquetada.
06. Anotar el identificador de revisión y la evidencia de verificación en el registro interno de cambios.

Al terminar las modificaciones y verificar que los servicios funcionan, crear una segunda revisión manual identificada como «Estado validado posterior a mantenimiento». Así quedan dos puntos de retorno reconocibles para un procedimiento con varias modificaciones.

39.23. Diferencias entre copia automática, programada y manual

Criterio	Por cambio	Programada	Manual
Disparador	Cambio significativo	Calendario configurado	Decisión del operador
Nombre o motivo	Generado por el sistema	Cambio registrado	Revision Reason explicativo
Utilidad principal	Granularidad	Regularidad	Hitos de mantenimiento
Riesgo operativo	Múltiples revisiones	Intervalo sin respaldo	Depende de la disciplina

39.24. Diagnóstico: confirmar que la copia llegó al destino

01. Abrir Restore y verificar que existe la entrada con la hora esperada y el motivo correcto.

02. Distinguir entradas alojadas en el servidor de copias todavía staged para subir.
03. Consultar Status → System Logs → System/General y buscar mensajes ACB de preparación, envío, éxito o error.
04. Verificar DNS, salida HTTPS, reloj del firewall y conectividad hacia el servicio oficial cuando existan fallos de subida.
05. Si el listado es correcto, descargar de modo controlado una revisión y comprobar que tiene el contenido esperado.
06. Ensayar una restauración en entorno autorizado cuando sea posible; documentar el resultado.

Los respaldos se procesan mediante una cola revisada aproximadamente una vez por minuto. Por ello, una revisión recién creada puede tardar en aparecer en el listado remoto. No deducir una avería instantánea sólo por no verla inmediatamente después de pulsar Backup.

39.25. Errores frecuentes y acciones correctivas

Síntoma	Causa posible	Comprobación y corrección
No se crean respaldos	ACB deshabilitado; calendario no alcanzado; cambio ignorado.	Revisar Settings, cadencia y registros de eventos.
Backup Now no aparece	ACB inactivo.	Habilitar servicio y guardar Settings.
Copia en espera	Cola pendiente o conectividad de salida.	Esperar proceso y revisar HTTPS, DNS y logs.
Histórico ausente	Device Key distinta o consulta de histórico legado.	Buscar con clave antigua custodiada.
No se descifra la revisión	Contraseña cambiada, errónea o extraviada.	Recuperar contraseña correspondiente desde bóveda.
Cambió el historial tras Change Key	Nueva clave identifica conjunto distinto.	Conservar y consultar clave anterior.
Reinicio necesario tras Restore	Interfaces y otros servicios no recargados por completo.	Planificar reinicio y prueba funcional.
Faltan datos de paquete	Algunos elementos se guardan fuera de config.xml.	Revisar guía de backup del paquete o servicio.

39.26. Seguridad, privacidad y cadena de custodia

- Custodiar Device Key y Encryption Password en almacenamiento seguro con controles de acceso y plan de sustitución de responsables.
- Aplicar MFA y control de privilegios en los sistemas donde se guarden copias o instrucciones de recuperación, cuando estén disponibles.
- No incluir información sensible en Hint/Identifier ni en Revision Reason, que pueden formar parte de metadatos visibles.
- Restringir la descarga del XML descifrado y eliminar copias temporales tras un proceso autorizado.
- Evitar restauraciones durante la producción sin coordinación; el contenido puede sustituir usuarios, contraseñas y políticas vigentes.
- Conservar documentación de versión, licencia y asignación genérica de interfaces para evitar depender solamente de una copia cifrada.

39.27. Recomendaciones de resiliencia y política de copias

Adoptar una política combinada: ACB remoto con frecuencia ajustada al ritmo de cambios, copia local cifrada desde Diagnostics → Backup & Restore en hitos significativos, control de retención y ensayos periódicos. Mantener separado el almacenamiento de las claves respecto a los archivos y al equipo protegido.

La retención debe priorizar revisiones estables y aprobadas. Una serie larga de cambios triviales puede desplazar puntos antiguos por el máximo de 100 entradas; la reserva de manuales ayuda a proteger hitos, pero no sustituye un plan de archivo y conservación externo.

39.28. Escenario empresarial A: cambio delicado de reglas y NAT

Se debe introducir una política de publicación de servicio y modificar traducciones. Antes del cambio, el responsable crea una copia manual con revisión descriptiva, registra las reglas actuales y comprueba la subida. Una vez aplicadas y validadas las reglas, crea un segundo backup. Si las comprobaciones externas fallan, dispone del punto anterior para revertir.

39.29. Escenario empresarial B: sustitución de un firewall averiado

Tras un fallo irrecuperable de almacenamiento, el equipo de soporte despliega hardware compatible, restaura la conectividad de gestión mínima y recupera una revisión desde ACB usando Device Key y Encryption Password previamente custodiadas. La tarea no termina cuando arranca el sistema: se revisan mapeos físicos y VLAN, rutas, VPN, servicios de red y accesos de usuarios.

39.30. Escenario empresarial C: cambios frecuentes con backups programados

Una organización que realiza muchas actualizaciones al día decide ejecutar el respaldo remoto en una franja estable para evitar una gran cantidad de revisiones consecutivas. Se comprueba que la programación incluye los campos cron correctos y que el resultado es visible. Antes de actuaciones de alto riesgo, se usa Backup Now para no depender exclusivamente de la siguiente ejecución programada.

39.31. Prueba de restauración periódica y reversión

01. Seleccionar un entorno o ventana de mantenimiento donde una recuperación no afecte indebidamente a la operación.
02. Documentar la revisión base, credenciales custodiadas y acceso de consola o alternativa.
03. Crear un respaldo manual y verificar su almacenamiento remoto.
04. Aplicar un cambio reversible y conocido, verificando que queda registrado.
05. Restaurar una revisión anterior autorizada, reiniciar si procede y comprobar que el cambio posterior ha desaparecido.
06. Ejecutar pruebas de conectividad y aplicaciones, y registrar capturas neutras de resultados sin datos sensibles.
07. Restablecer estado operativo y elaborar acta del ensayo con responsables y hallazgos.

39.32. Matriz de aceptación del sistema AutoConfigBackup

Comprobación	Criterio de aceptación	Evidencia recomendada
ACB activo	Settings habilitado y guardado.	Registro de revisión de configuración.
Cifrado	Contraseña larga custodiada y confirmada.	Control documental sin valor secreto.
Identidad	Device Key disponible en custodia autorizada.	Registro de ubicación en bóveda.
Subida	Entrada visible en Restore tras el envío.	Fecha y motivo genérico.
Histórico	Listado y límites de retención supervisados.	Verificación periódica.
Restauración	Ensayo completado sin interrupciones inesperadas.	Acta de prueba y plan de reversión.
Copia alternativa	Archivo local protegido independiente disponible.	Inventario de soporte y ubicación.

39.33. Glosario operativo

Término	Definición práctica
ACB	AutoConfigBackup, servicio de respaldos remotos cifrados de configuración.
Device Key	Identificador secreto que agrupa y permite consultar revisiones remotas.

Término	Definición práctica
Encryption Password	Secreto local requerido para cifrar y descifrar el archivo de configuración.
Revision Reason	Descripción administrativa que identifica el motivo de una copia manual.
Staged Backup	Entrada preparada localmente pero aún pendiente de envío confirmado.
Config.xml	Archivo XML con gran parte de los parámetros de pfSense.
Bare Metal Recovery	Reconstrucción del firewall en instalación o hardware nuevo.
Cron	Sistema de especificación periódica de fechas y horas para tareas.

39.34. Referencias oficiales de Netgate

Servicio y funcionamiento general: https://docs.netgate.com/pfsense/en/latest/backup/acb.html

Funcionamiento interno y retención: https://docs.netgate.com/pfsense/en/latest/backup/acb-info.html

Opciones Settings (todos los campos): https://docs.netgate.com/pfsense/en/latest/backup/acb-config.html

Cambio y custodia de Device Key: https://docs.netgate.com/pfsense/en/latest/backup/acb-changekey.html

Restore, Revision y recuperación bare metal: https://docs.netgate.com/pfsense/en/latest/backup/acb-restore.html

Respaldo manual con Backup Now: https://docs.netgate.com/pfsense/en/latest/backup/acb-manual.html

Pruebas y registros del servicio: https://docs.netgate.com/pfsense/en/latest/backup/acb-status.html

Compatibilidad y restauración de copias: https://docs.netgate.com/pfsense/en/latest/backup/restore.html

Estrategia general de backup: https://docs.netgate.com/pfsense/en/latest/backup/index.html

39.35. Síntesis para el administrador

AutoConfigBackup es una pieza central de la continuidad operativa de pfSense Plus si sus tres acciones esenciales se mantienen bajo control: crear copias útiles, conservar los secretos que permiten recuperarlas y probar la restauración. La presencia de un archivo en el servicio remoto es el principio de la recuperación, nunca su final. La gestión de cambios, el control de acceso y las pruebas periódicas convierten el respaldo en una capacidad real de recuperación.

40 Services → Captive Portal

Zonas, autenticación, acceso de invitados y gestión de sesiones

Ruta: Services → Captive Portal. La vista inicial presenta el inventario de zonas y Add. Tras crear o editar una zona se accede a sus opciones de configuración, métodos de autenticación, excepciones, vouchers y recursos del portal. Los controles disponibles dependen de la versión y del modo de autenticación.

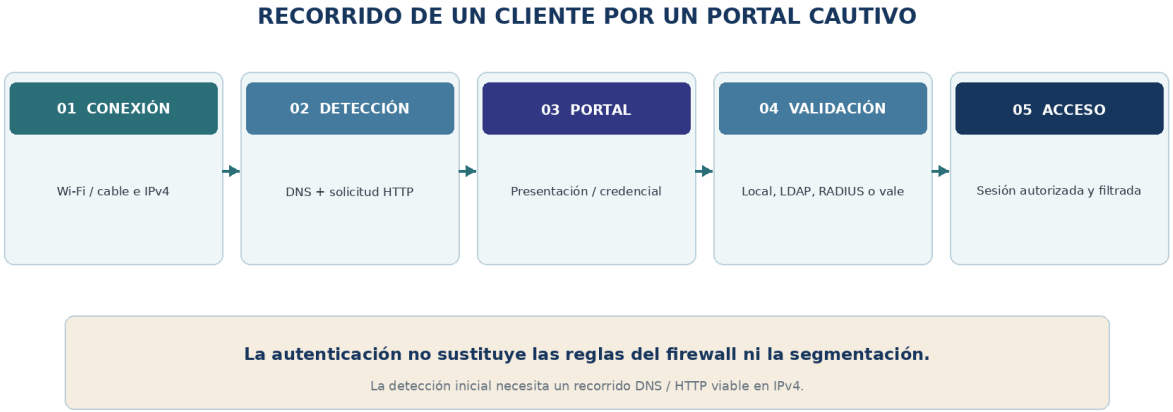


Figura 40.1. Esquema conceptual de detección, autenticación y autorización de acceso.

40.1. Objeto, alcance y funcionamiento

Un portal cautivo condiciona el acceso a la red a la presentación de una página de aceptación, a una autenticación o a un código de acceso temporal. Es frecuente en redes de visitas, aulas, espacios públicos y zonas empresariales separadas. El firewall identifica el cliente y decide cuándo puede alcanzar destinos fuera de la zona, pero la autorización de portal es un control distinto de las políticas habituales de firewall y NAT.

El acceso puede ser libre tras un clic de aceptación, autenticado contra usuarios locales, LDAP o RADIUS, o habilitado con vouchers. Las opciones de cada zona se gestionan por separado. La pantalla de inicio puede estar vacía sin que ello indique fallo: significa que aún no hay zonas configuradas.

40.2. Navegación y organización de las zonas

Services → Captive Portal presenta la tabla Captive Portal Zones, con los encabezados Zone, Interfaces, Number of users, Description y Actions. Add crea una zona nueva; el icono de ayuda abre la documentación contextual. Para configurar una zona existente se utiliza su acción de edición.

Columna / control	Qué expresa	Cómo interpretarlo
Zone	Identificador funcional de la zona del portal.	Permite localizar el conjunto independiente de opciones.
Interfaces	Interfaces incluidas dentro del portal.	Una misma interfaz no se puede asignar a dos zonas.
Number of users	Indicador de usuarios de la zona que presenta la GUI.	No confundirlo sin comprobación con el total histórico de accesos.
Description	Texto descriptivo administrativo.	Conviene describir la finalidad de la zona.
Actions	Controles por fila de edición y eliminación.	Comprobar dependencias antes de eliminar.
Add / ayuda	Creación de zona y acceso a la ayuda.	Tras crear, se configuran las opciones individuales.

40.3. Concepto de zona y pertenencia de interfaces

Una zona agrupa una o varias interfaces sometidas a la misma lógica de portal. Cada zona mantiene sus propios parámetros, HTML, servidores de autenticación, excepciones de MAC/IP y vouchers. Una interfaz

solo puede pertenecer a una zona; intentar reutilizarla genera un error de validación. Las interfaces WAN no son destinos válidos para una zona de portal.

Cuando se utiliza un bridge, Netgate indica que la interfaz asignada a la zona debe ser el propio bridge con dirección IP configurada, no una selección arbitraria de puertos miembros. Antes de activar el portal, identificar la interfaz real por la que entra el tráfico del usuario.

Precaución de acceso. Nunca habilitar sin ensayo un portal en la interfaz utilizada para administrar el firewall o para servicios críticos: un error de zona, DNS o autenticación puede impedir gestionar el equipo desde esa red.

40.4. Crear una zona: Zone Name y Zone Description

Al pulsar Add, Netgate documenta Zone Name y Zone Description como los primeros datos de creación. Zone Name admite letras, números y guion bajo; no deben utilizarse espacios ni otros caracteres especiales. Zone Description es opcional y debe facilitar la operación. El botón Save & Continue guarda esta identidad y abre el editor del portal.

01. Entrar en Services → Captive Portal y pulsar Add.
02. Introducir un nombre neutro y técnico, por ejemplo PORTAL_VISITAS, sin datos personales ni ubicaciones reales.
03. Añadir una descripción funcional que distinga el alcance de la zona.
04. Pulsar Save & Continue para crear la zona.
05. Configurar la interfaz y las condiciones de autenticación antes de habilitar el servicio en producción.

40.5. Acciones del listado: editar, eliminar y comprobar usuarios

El icono de lápiz abre la edición y las pestañas de una zona creada. El icono de papelera elimina una zona tras confirmación; puede afectar al acceso de clientes activos y a sus excepciones, configuración visual o vouchers. El número de usuarios de la tabla sirve como referencia rápida, pero la comprobación efectiva de sesiones se realiza desde Status → Captive Portal → Active Users.

40.6. Editar una zona: Enable, Description e Interface

Parámetro	Efecto al habilitar o cambiarlo	Criterio recomendado
Enable	Activa el control de portal sobre las interfaces seleccionadas.	Probar antes en una red aislada, con consola alternativa.
Description	Actualiza la identificación administrativa.	Redacción breve y no sensible.
Interface	Determina qué interfaces de usuario controla la zona.	Excluir WAN y redes de gestión; validar bridges y VLAN.

Al desmarcar Enable, el portal deja de aplicar su flujo de autorización en la zona. Eso no concede acceso por sí mismo: siguen siendo necesarias las reglas convencionales de firewall, las rutas, DHCP y DNS. Cambiar la interfaz puede desplazar el control de acceso a otra red y cortar sesiones existentes.



Figura 40.2. Capas diferenciadas de identidad, sesión, excepciones y presentación.

40.7. Maximum concurrent connections: protección del portal web

Este campo limita las conexiones simultáneas a la página web del portal por dirección IP, no el número total de personas autenticadas. La referencia de Netgate indica un valor habitual por defecto de 4. Su objetivo es evitar que un único equipo, por error o abuso, agote recursos del servidor del portal. Aumentarlo solo cuando clientes legítimos lo necesiten y exista capacidad suficiente.

40.8. Idle timeout y Hard timeout

Campo	Comportamiento	Riesgo a considerar
Idle timeout	Desconecta al usuario tras los minutos de inactividad definidos.	Una sesión inactiva pierde autorización; no impide autenticarse otra vez.
Hard timeout	Cierra la sesión tras un tiempo máximo, aunque exista actividad.	Puede interrumpir una transferencia o videollamada.
Relación con DHCP	Los timeout configurados deben ser menores que la concesión DHCP.	Evita que una sesión permanezca asociada a una IP reasignada.

La duración de un voucher y la vida de una sesión no son necesariamente equivalentes. Comprobar la interacción entre temporizadores, caducidad de credenciales, sesión actual y renovación DHCP.

40.9. Traffic Quota: cuota acumulada de sesión

Traffic Quota define el tráfico máximo que una sesión puede transferir, sumando subida y bajada. Al superar el umbral, el portal desconecta al cliente. Si las credenciales continúan siendo válidas, el usuario podría volver a iniciar sesión; no equivale necesariamente a una cuota persistente por identidad. En entornos RADIUS pueden aplicarse atributos de cuota específicos.

40.10. Pass-Through Credits: accesos temporales sin autenticación

Los créditos de paso permiten a una MAC acceder cierto número de veces antes de exigir autenticación. Están relacionados con el período de espera de recuperación y funcionan mejor cuando se definen límites de sesión. No equivalen a una identidad robusta: las MAC pueden variar o suplantarse. Configurar con cautela en redes donde se necesita trazabilidad.

Control	Función	Efecto práctico
Pass-through credits allowed per MAC	Cantidad de accesos de cortesía.	Consumidos, se exige autenticación.
Waiting period to restore credits	Horas para recuperar créditos tras el uso inicial.	Permite un nuevo ciclo de accesos.
Reset waiting period on attempted access	Reinicia la espera si el cliente reintenta sin créditos.	Evita reintentos continuos para eludir la espera.

40.11. Redirecciones previas y posteriores al acceso

Pre-authentication redirect URL envía al cliente a una página informativa antes de la autenticación. Ese destino puede necesitar una excepción en la zona para ser accesible sin iniciar sesión, además de un retorno correcto al portal. After authentication Redirection URL determina el destino tras completar el acceso; si no se define, se intenta continuar hacia el sitio originalmente solicitado. Blocked MAC address redirect URL permite ofrecer un destino para dispositivos expresamente bloqueados.

Seguridad de redirección. Utilizar destinos conocidos y controlados. Si una página externa incorpora recursos adicionales, comprobar sus nombres y direcciones antes de crear excepciones; no abrir de forma general redes enteras para solucionar un error de carga.

40.12. Preserve user database y Concurrent user logins

Preserve user database intenta conservar la información de usuarios conectados cuando el firewall reinicia. Concurrent user logins controla cómo se trata la reutilización simultánea de una identidad o vale, no constituye por sí mismo un límite general de usuarios de la zona.

Modo	Comportamiento del usuario / voucher
Disabled	No permite inicios concurrentes para una misma identidad.
Multiple	Permite varias conexiones simultáneas; opción general predeterminada.
Last Login	Conserva el inicio más reciente y desconecta los anteriores.
First Login	Admite el primer inicio y deniega los intentos posteriores mientras siga activo.

40.13. MAC filtering y paso automático de MAC

La opción MAC filtering, tal como la describe Netgate, desactiva el filtrado MAC del portal al marcarla: conviene leer la etiqueta y la ayuda antes de asumir la dirección de su efecto. Puede necesitarse cuando varios clientes se encuentran detrás de otro router y el portal no identifica MAC individuales. Esa modalidad es incompatible con RADIUS MAC Authentication.

Pass-through MAC automatic additions incorpora automáticamente a una lista de excepciones los dispositivos que ya se autenticaron; la variante with username conserva el nombre relacionado. Una vez añadidos, esos dispositivos pueden evitar nuevas autenticaciones hasta retirar la excepción. Netgate advierte incompatibilidad con determinadas modalidades de RADIUS MAC y con la ventana de cierre de sesión.

40.14. Límites de velocidad predeterminados por usuario

Default download y Default upload fijan límites orientativos en kilobits por segundo para usuarios del portal. Dejarlos en blanco o en 0 supone ausencia de límite definido por esos campos. RADIUS puede suministrar restricciones individuales que prevalezcan sobre el valor base. Conviene combinarlo con capacidad real, número de concurrentes, colas existentes y comprobaciones de latencia.

40.15. Página de inicio: personalización sencilla

Sin Use Custom Captive Portal Page, se ofrecen controles simples para Display Custom Logo Image, Logo Image, Display Custom Background Image, Background Image y Terms and Conditions. El texto de condiciones debe ser comprensible y revisado por el responsable correspondiente; la aceptación por clic no equivale a una autenticación de identidad ni garantiza cumplimiento normativo por sí sola.

40.16. Use Custom Captive Portal Page y recursos de presentación

La personalización avanzada habilita HTML Page Contents para crear una experiencia diferenciada. Existen páginas principales según autenticación, vouchers y variantes, más una página de error y otra de salida. En los formularios deben respetarse los nombres de campos esperados por pfSense. Las páginas pueden incorporar PHP; este código se ejecuta en el firewall y debe ser auditado como software sensible, no como mero contenido visual.

Elemento	Utilidad	Observación de seguridad
Portal page contents	Página principal de entrada y autenticación.	Comprobar campos y navegación completa.
Authentication error page contents	Presentación de autenticaciones fallidas.	No revelar detalles internos de validación.
Logout page contents	Interfaz de salida cuando está habilitada.	Algunos navegadores bloquean ventanas emergentes.
View / Download / Restore Default	Consultar, descargar o eliminar páginas personalizadas.	Mantener una versión revisada y plan de retorno.

40.17. Authentication Method: tres familias de acceso

Modalidad	Qué solicita	Uso adecuado / restricción
None, don’t authenticate users	Clic en Continue / aceptación; sin credenciales.	Invitados de bajo riesgo con filtrado y limitación de tiempo.

Modalidad	Qué solicita	Uso adecuado / restricción
Use an Authentication backend	Usuario y contraseña de base local, LDAP o RADIUS; admite vouchers.	Control individual o accesos temporales.
Use RADIUS MAC Authentication	Identidad basada en MAC y secreto del servidor.	Requiere ver MAC; no reemplaza seguridad fuerte.

En los tres casos sigue existiendo una fase de presentación o envío del formulario del portal. La ausencia de autenticación no significa permitir acceso antes de que el cliente acepte la página configurada.

40.18. Authentication Server y fuente secundaria

Authentication Server permite seleccionar la base local o uno o varios servidores externos. Los servidores primarios se prueban según su orden si uno no responde. Secondary Authentication Server configura un mecanismo independiente con sus propios campos; no debe confundirse con la conmutación automática de servidores dentro del grupo primario. Verificar de antemano la disponibilidad de DNS, rutas y puertos de autenticación desde el propio firewall.

40.19. Local Database y privilegio de acceso

Con Local Database, los usuarios se crean bajo System → User Manager. La opción Allow only users/groups with “Captive portal login” privilege set restringe el acceso a quienes posean ese privilegio, directa o indirectamente por grupo. Es recomendable separar las cuentas de portal de las cuentas administrativas del cortafuegos y revisar caducidad y bajas de usuarios.

40.20. LDAP: autenticación contra directorio

Al seleccionar un servidor LDAP configurado en pfSense, el portal lo utiliza para validar credenciales. Antes del despliegue, comprobar certificados, conectividad con el directorio, permisos, formato del usuario y procedimientos de fallo. La elección de LDAP no convierte por sí sola la zona de invitados en parte de la red interna: aplicar restricciones mediante reglas independientes.

40.21. RADIUS: autenticación, NAS e integración empresarial

RADIUS permite centralizar usuarios y, según el sistema, controlar políticas por respuesta. Los campos documentados comprenden NAS Identifier, Reauthentication y opciones específicas de límites. Reauthentication puede remitir peticiones de validación periódicas; combinarla sin cuidado con controles de concurrencia puede rechazar sesiones legítimas. Mantener sincronización horaria y recursos de conectividad con el servidor.

Atributo de respuesta	Influencia posible
Session-Timeout / Idle-Timeout	Duración máxima e inactividad de una sesión.
WISPr / ChilliSpot Bandwidth	Límites de subida y bajada por usuario.
pfSense-Max-Total-Octets	Cuota global de tráfico de la sesión.
WISPr-Redirection-URL	Destino de navegación posterior a la autorización.
Acct-Interim-Interval	Periodicidad de actualizaciones de accounting.

40.22. RADIUS MAC Authentication: formato y fallback

RADIUS MAC Secret se utiliza como contraseña al presentar la MAC como identificador de usuario. MAC address format transforma la representación para coincidir con los registros del servidor (pares con dos puntos, con guiones, grupos con punto o sin separadores). Login Page Fallback envía al formulario de credenciales si la autenticación de MAC falla. No documentar MAC reales ni el secreto de autenticación.

40.23. RADIUS Accounting y trazabilidad de sesiones

Accounting Server identifica el destino de los registros de sesión. Send Accounting Updates permite No updates, Stop/start, Stop/start (FreeRADIUS) e Interim. El modo Interim añade actualizaciones periódicas que mejoran la información ante reinicios imprevistos, con coste de mensajes y almacenamiento. Accounting Style puede invertir el punto de vista de los contadores y Idle Time Accounting cambia el cálculo de tiempo cuando hay cierre por inactividad.

40.24. HTTPS login, nombre DNS y certificado

La opción Login sirve la página del portal mediante HTTPS cuando existe un certificado TLS válido. HTTPS server name debe coincidir con el nombre del certificado y resolver desde la red de clientes. SSL Certificate selecciona el certificado gestionado en pfSense. Disable HTTPS Forwards impide intentar redirigir conexiones HTTPS de terceros hacia el portal, reduciendo errores de certificado; la detección inicial dependerá entonces de HTTP y del mecanismo propio del sistema operativo.

No interceptar HTTPS de manera engañosa. No es recomendable sustituir la identidad TLS de un destino externo ni instruir al usuario para ignorar alertas de certificado. Mantener HTTPS legítimo para la página de login y un recorrido HTTP de detección cuando se requiera.

40.25. Pestañas auxiliares tras crear una zona

El editor de zona ofrece controles de MAC, direcciones IP permitidas, hostnames permitidos, vouchers y File Manager. Las pestañas se consultan después de abrir una zona concreta. Sus etiquetas y visibilidad pueden variar con la revisión de pfSense Plus.

Área	Propósito	Precaución
MACs	Pass o Block por dirección MAC.	Una MAC puede suplantarse.
Allowed IP Addresses	Tráfico exento con dirección y sentido determinados.	Limitar al destino y sentido imprescindible.
Allowed Hostnames	Excepciones basadas en resolución DNS periódica.	CDN y servicios múltiples pueden requerir varios nombres.
Vouchers	Códigos y rolls de duración limitada.	Custodiar claves y códigos en circulación.
File Manager	Archivos gráficos, CSS y recursos del portal.	Revisar contenidos y límites de tamaño.

40.26. MACs: Pass, Block y control por dispositivo

En la pestaña MACs, Action determina Pass (bypassa el portal sin autenticación) o Block (deniega el acceso). Se configuran MAC address, Description y, si se desea, Bandwidth up/down. Los controles de edición y eliminación alteran la excepción. Un dispositivo autorizado mediante MAC no equivale a un usuario individual autenticado: la dirección de hardware puede cambiar, aleatorizarse o falsificarse.

40.27. Allowed IP Address: excepciones por dirección y sentido

Esta zona permite excepciones explícitas para recursos necesarios antes de la autenticación, por ejemplo el servidor de una página de bienvenida. Evaluar el sentido To, From o Both según corresponda, los prefijos y las reglas de firewall. Una excepción de portal no debe utilizarse para abrir libremente la conectividad administrativa. Las direcciones permitidas son distintas de las reglas NAT y no sustituyen controles L3/L4.

40.28. Allowed Hostnames y walled garden

Los nombres permitidos se resuelven periódicamente a direcciones IP, por lo que su alcance puede variar si cambia el DNS. La documentación permite Direction (To, From, Both), Hostname, Description y opcionalmente Bandwidth up/down. Un portal con página externa puede requerir permitir nombres adicionales de estilos o contenido; autorizar dominios amplios puede abrir más tráfico del previsto.

40.29. Vouchers: códigos y rolls de acceso temporal

Los vouchers son códigos emitidos por lotes llamados rolls; cada roll se crea con una duración establecida. El temporizador comienza al primer uso y no se detiene por cerrar la sesión. Si otro equipo reutiliza el mismo vale, la sesión anterior puede quedar interrumpida. No son cuentas permanentes ni sustituyen la revisión de acceso de recursos sensibles.

El módulo incluye Enable, claves RSA pública/privada, conjunto de caracteres y parámetros de bits, así como mensajes para códigos inválidos o caducados. Netgate advierte que alterar las claves o parámetros después de generar rolls puede invalidar vouchers existentes. La generación de lotes y su exportación deben quedar sujetas a custodia y a una política de entrega.

40.30. File Manager: recursos y límites del portal

File Manager acepta elementos usados por el portal, como imágenes y CSS. La documentación indica un límite total de 1 MB por zona y el prefijo automático captiveportal- para los nombres subidos. Los ficheros aparecen como recursos relativos del servidor del portal. No cargar código PHP o JavaScript no revisado: los recursos se incorporan a la configuración del propio firewall.

40.31. Estado y monitorización: Active Users y vouchers

Status → Captive Portal → Active Users muestra sesiones activas y permite seleccionar la zona. Según el tipo de autenticación, puede presentar dirección IP, MAC, nombre de usuario o código de voucher y hora de inicio de sesión. Una acción de eliminación cierra la sesión seleccionada, lo que obliga a autenticarse de nuevo. En las pestañas de vouchers se consultan roll usage, códigos activos y pruebas de validez.

40.32. Procedimiento 1: portal de aceptación sin credenciales

01. Crear una zona neutra y revisar que la interfaz seleccionada corresponde únicamente a la red de invitados.
02. Configurar DHCPv4, DNS y una regla que permita la conexión HTTP inicial necesaria para detectar el portal.
03. Elegir None, don’t authenticate users y definir el contenido de aceptación o página simple.
04. Establecer Idle y Hard timeout acordes al tipo de visita y menores que la concesión DHCP.
05. Habilitar el portal en la zona y guardar.
06. Conectar un cliente de pruebas, comprobar redirección, pulsar Continue y verificar la navegación permitida.
07. Validar que no se accede a redes internas salvo excepciones explícitas y justificadas.

40.33. Procedimiento 2: portal de usuarios locales

01. Crear usuarios no administrativos y asignarles acceso al portal cuando el modo lo exija.
02. Seleccionar Use an Authentication backend y Local Database.
03. Activar la limitación por privilegio cuando sea necesaria, y definir concurrencia y temporizadores.
04. Preparar la página de autenticación con campos correctos y mecanismo HTTPS válido.
05. Iniciar sesión desde un cliente de prueba y verificar su aparición en Active Users.
06. Intentar una cuenta sin autorización y confirmar el rechazo sin pérdida de acceso administrativo.

40.34. Procedimiento 3: portal centralizado con RADIUS

01. Configurar un servidor RADIUS en el sistema, con secretos custodiados y conectividad validada.
02. Elegir Authentication Server con la entrada RADIUS apropiada y revisar NAS Identifier.
03. Seleccionar método de accounting, límites individuales y políticas de reautenticación si están soportadas.
04. Ensayar autenticaciones válidas e inválidas, y verificar los registros del servidor RADIUS.
05. Simular indisponibilidad controlada del servidor para estudiar el comportamiento del portal.
06. Comprobar RADIUS accounting y que ningún privilegio de administración se derive de forma involuntaria.

40.35. Procedimiento 4: vouchers con caducidad

01. Crear una zona con Authentication Method compatible con vouchers.
02. Abrir Vouchers, activar Enable y establecer las claves y parámetros antes de emitir códigos.
03. Crear un roll de duración reducida en una red de pruebas.
04. Exportar los códigos mediante un procedimiento de custodia restringida.
05. Iniciar sesión con un voucher de prueba y observar su temporizador.

06. Validar la caducidad, el comportamiento al reutilizar el código y la trazabilidad de uso.

40.36. Integración de red: VLAN, DHCP, DNS, NAT y reglas PF

Una red de invitados sólida normalmente separa sus clientes en VLAN o interfaz específica, asigna IPv4 mediante DHCP, resuelve DNS y restringe con reglas de firewall el acceso a redes internas. Captive Portal añade control de sesión, pero no soluciona errores de capa 2, rutas, NAT o DNS. La dirección de respuesta del portal y el nombre HTTPS deben ser alcanzables desde los clientes.

En pfSense Plus 22.05 y posteriores, Netgate documenta el uso de reglas PF de capa 2 con ether para el mecanismo de portal. En diagnóstico avanzado se pueden inspeccionar los anchors de Captive Portal, pero las modificaciones manuales del ruleset no son una vía normal de administración ni deben persistirse fuera de la GUI.

40.37. Limitaciones conocidas y compatibilidad IPv6

La documentación oficial establece que Captive Portal no es compatible con IPv6 y tampoco funciona como un portal inverso para conexiones entrantes desde Internet. Debe planificarse el comportamiento de IPv6 en la red de invitados para evitar errores de conexión o vías de acceso ajenas al portal, y verificarlo en una prueba controlada. Algunos navegadores modernos priorizan HTTPS y no permiten una redirección visible desde cualquier URL.

Limitación crítica. La mera presencia de una página de portal no demuestra que todo el tráfico de la red esté condicionado por ese proceso. Comprobar IPv4/IPv6, reglas, excepciones, clientes con DNS alternativo y sistemas de detección automática.

40.38. Riesgos operativos: cierres de sesión y cambios en producción

La activación, desactivación, cambio de interfaz o modificación del método de autenticación puede cortar sesiones de visitas, afectar a integraciones con directorio y modificar accesos preautorizados. No utilizar la misma interfaz para invitados y administración si el diseño exige independencia. Prever consola, una ruta alternativa y una copia de configuración verificable antes de grandes cambios.

40.39. Diagnóstico: el portal no aparece

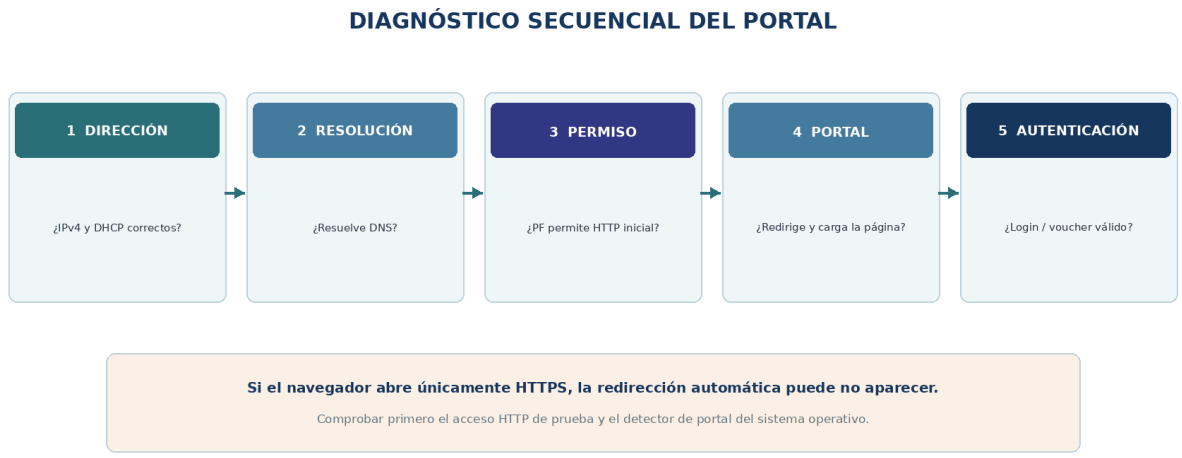


Figura 40.3. Secuencia de verificación desde IPv4 y DNS hasta la autenticación.

Síntoma	Causa probable	Acción correctiva
No muestra la página	DNS no resuelve o tráfico HTTP bloqueado.	Revisar DNS en interfaz, resolución y reglas PF.
El navegador da error TLS	HTTPS de tercero; certificado de portal no coincide.	Probar URL HTTP de detección y certificado FQDN válido.
Autenticación rechazada	Credenciales, privilegios, LDAP o RADIUS.	Revisar usuarios, ACL y logs de servidor.
El login funciona pero no navega	Faltan rutas, reglas o NAT posterior.	Comprobar política L3/L4 de invitados.

Síntoma	Causa probable	Acción correctiva
Cliente no accede a un recurso permitido	Excepción incompleta, dependencia CDN o DNS cambiante.	Revisar sentidos, nombres e IP resueltas.
Sesión se corta antes de lo esperado	Hard/Idle timeout, voucher o RADIUS.	Revisar todos los temporizadores y atributos.

40.40. Comprobación funcional y matriz de aceptación

Prueba	Resultado que debe verificarse	Evidencia sugerida
Aislamiento	Sin acceso lateral a redes no autorizadas.	Pruebas desde cliente de invitados.
Detección	Se abre portal desde HTTP o detección del sistema.	Registro de flujo y observación local.
Acceso autorizado	Autenticación válida genera sesión activa.	Status → Captive Portal.
Rechazo	Acceso erróneo o voucher caducado no permite navegación.	Captura neutral de mensaje.
Caducidad / cierre	La sesión termina según política.	Hora de finalización y nueva solicitud.
Continuidad	Servicios críticos fuera de zona siguen operativos.	Ficha de monitorización.
Reversión	Restauración documentada revierte cambios.	Registro de cambio y comprobación.

40.41. Recomendaciones de seguridad y operación empresarial

- Diseñar una red de invitados separada, con reglas de mínimo privilegio, sin compartir la administración del firewall.
- Controlar cuidadosamente las excepciones MAC/IP/hostname: cada una modifica el alcance del requisito de autenticación.
- Custodiar vouchers, secretos RADIUS y certificados; no incluirlos en inventarios públicos ni documentos del libro.
- Preferir TLS válido y formularios simples auditados; evitar páginas con PHP no revisado.
- Alinear tiempos de sesión con DHCP, conservar eventos relevantes y establecer un plan de atención a fallos.
- Medir carga, ancho de banda, número de usuarios y capacidad de backend antes de desplegar múltiples zonas.

40.42. Plan de reversión ante una implantación fallida

01. Registrar el cambio y crear una copia de configuración anterior validada.
02. Mantener acceso de administración por una vía ajena a la zona.
03. Si falla el portal, revisar primero DNS, HTTP, interfaz y backends sin modificar reglas indiscriminadamente.
04. Si la incidencia afecta a usuarios, deshabilitar temporalmente la zona solo después de evaluar las reglas restantes.
05. Si el acceso administrativo queda afectado, emplear consola o restauración controlada.
06. Verificar navegación, aislamiento, DHCP/DNS y cierre de sesiones tras la reversión.

40.43. Glosario breve

Término	Definición
Captive Portal	Control de acceso basado en presentación y autorización previa a la navegación.
Zone	Conjunto de interfaces y ajustes de portal independientes.

Término	Definición
RADIUS / LDAP	Servicios externos de identidad y validación.
Voucher / Roll	Código temporal de acceso / lote de vouchers con parámetros comunes.
Walled garden	Conjunto restringido de recursos accesibles antes de iniciar sesión.
Idle / Hard timeout	Desconexión por inactividad / por duración total de sesión.
Accounting	Registros de inicio, fin y consumo de sesiones en RADIUS.

40.44. Referencias oficiales de Netgate

Captive Portal — visión general — https://docs.netgate.com/pfsense/en/latest/captiveportal/index.html

Captive Portal Zones — https://docs.netgate.com/pfsense/en/latest/captiveportal/zones.html

Zone Configuration Options — https://docs.netgate.com/pfsense/en/latest/captiveportal/configuration.html

Common Captive Portal Scenarios — https://docs.netgate.com/pfsense/en/latest/captiveportal/common-scenarios.html

MAC Address Control — https://docs.netgate.com/pfsense/en/latest/captiveportal/mac-address-control.html

Allowed Hostnames — https://docs.netgate.com/pfsense/en/latest/captiveportal/allowed-hostnames.html

Vouchers — https://docs.netgate.com/pfsense/en/latest/captiveportal/vouchers.html

File Manager — https://docs.netgate.com/pfsense/en/latest/captiveportal/file-manager.html

Captive Portal Status — https://docs.netgate.com/pfsense/en/latest/monitoring/status/captiveportal.html

Troubleshooting Captive Portal — https://docs.netgate.com/pfsense/en/latest/troubleshooting/captiveportal.html

41 Services → DHCP Relay

Agente de reenvío DHCPv4, servidor central, opción 82 y alta disponibilidad

Ruta: Services → DHCP Relay. La pantalla presenta el aviso de incompatibilidad con DHCP Server, los parámetros de reenvío, las interfaces receptoras, la dependencia opcional de CARP y los servidores ascendentes. El capítulo relaciona estos controles con el funcionamiento del protocolo y los procedimientos de verificación.

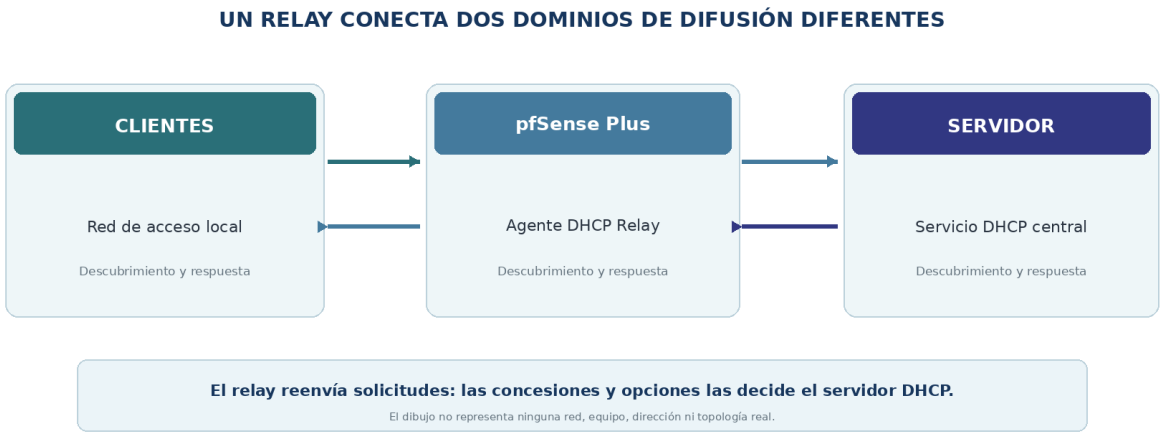


Figura 41.1. Estructura lógica de un agente DHCP Relay entre clientes y servidor central.

41.1. Objeto del servicio y razón de utilizar DHCP Relay

DHCP Relay permite que clientes situados en una red de difusión local reciban configuración IPv4 de un servidor DHCP ubicado en otra red. El cliente suele iniciar el proceso con un mensaje de difusión que no atraviesa enrutadores por sí mismo; el agente de reenvío escucha en la interfaz de los clientes y transmite la solicitud hacia un servidor remoto. Así se centralizan las reservas, los rangos y las opciones sin desplegar servidores DHCP independientes en cada red.

El firewall actúa como intermediario, no como autoridad que concede la dirección. La concesión, tiempo de arrendamiento, dirección del router y servidores DNS siguen siendo políticas del servidor remoto. El relay tampoco sustituye al enrutamiento, a las reglas de acceso o a la disponibilidad del servidor central.

41.2. Cuándo se utiliza y cuándo conviene evitarlo

Situación	¿Relay adecuado?	Razonamiento
Múltiples VLAN con DHCP central	Sí, si la red y las rutas están preparadas.	Consolida ámbitos y reservas en un servidor.
Una sola LAN pequeña	Opcional; a menudo innecesario.	El servidor local reduce dependencias externas.
Clientes y servidor en la misma VLAN	Normalmente no.	No es necesario superar un límite de difusión.
Dependencia crítica de un enlace WAN/VPN	Depende de la continuidad requerida.	Una caída del enlace puede impedir concesiones nuevas.
Red con servidor DHCPv4 local activo en pfSense	No simultáneamente.	Hay que decidir entre servir y reenviar DHCPv4.

41.3. Ruta y composición de la pantalla

Services → DHCP Relay contiene el bloque DHCP Relay Configuration, Enable, Append circuit ID and agent ID to requests, Downstream Interfaces, CARP Status VIP, Upstream Servers, Add Upstream Server y Save. La ayuda contextual permite contrastar la configuración. El servicio DHCPv6 se administra por separado.

Campo o control	Función verificable	Comportamiento general
Enable DHCP Relay	Activa el agente de reenvío IPv4.	Sin marcar, el relay no envía solicitudes.
Downstream Interfaces	Selecciona las redes que alojan clientes DHCP.	Permite más de una interfaz de clientes.
CARP Status VIP	Vincula la ejecución al estado de una VIP CARP.	MASTER activo; BACKUP detenido.
Append circuit ID and agent ID	Añade identificación de agente/segmento.	Requiere coordinación con el servidor.
Upstream Servers	Direcciones IPv4 de servidores DHCP destino.	Add Upstream Server añade otra entrada.
Save	Guarda los parámetros introducidos.	Verificar después que el servicio funciona.

41.4. Aviso rojo de incompatibilidad: alcance real

El aviso «DHCP Relay cannot be enabled while DHCP Server is enabled on any interface» significa que pfSense no admite simultáneamente el servidor DHCPv4 integrado y el relay DHCPv4. Netgate especifica que el servicio de servidor DHCPv4 debe deshabilitarse en todas las interfaces para poder habilitar el relay, no únicamente en la interfaz que se desea reenviar. Esto afecta a cualquier segmento que dependiera del servidor local.

ADVERTENCIA CRÍTICA. Si se desactiva el DHCP local sin que el servidor remoto tenga ámbitos y conectividad correctos, los clientes podrían quedarse sin dirección al renovar o reiniciar. Mantener una vía de administración con IP estática, acceso alternativo o consola y una ventana de cambio con plan de reversión.

41.5. Enable: activación del agente DHCP Relay

Al marcar Enable DHCP Relay, el firewall intenta iniciar el servicio con las interfaces de clientes y los destinos configurados. Desmarcarlo detiene el reenvío del agente; no desactiva el servicio DHCP remoto ni convierte automáticamente el firewall en servidor DHCP. La validez de las direcciones ya concedidas depende de sus tiempos de arrendamiento y de las renovaciones futuras.

Enable activa o desactiva el relay local. Que la casilla esté desmarcada no informa por sí solo del funcionamiento de otros servidores DHCP presentes en la red.

41.6. Downstream Interfaces: elección correcta de redes receptoras

Selecciona una o varias interfaces del firewall conectadas a segmentos donde se encuentran los clientes DHCP. En el control solo figuran interfaces con dirección IPv4, tal como indica el texto de ayuda. La selección se efectúa en una lista múltiple; cada interfaz elegida participa en la recepción y el reenvío.

Que una interfaz aparezca en la lista no implica que deba seleccionarse: una WAN puede ser técnicamente elegible pero no debe tratarse como red de usuarios sin una justificación de diseño. Es crucial diferenciar «downstream» (lado de los clientes) y «upstream» (destino del servidor), que no son opciones intercambiables.

41.7. Selección múltiple, interfaces VLAN y prerrequisitos

En instalaciones con VLAN asignadas, cada VLAN de usuarios ha de existir como interfaz del firewall, disponer del direccionamiento de capa 3 apropiado y ser accesible desde el cliente. La dirección de la interfaz ayuda a identificar la red de origen ante el servidor remoto mediante la información de relay. Las políticas y el servidor deben conocer el ámbito DHCP correspondiente a cada segmento.

01. Documentar las redes de clientes previstas con nombres neutros y sin exportar identificadores reales.
02. Comprobar que cada interfaz seleccionable tiene IPv4 y que las VLAN y puertos asociados funcionan.
03. En Downstream Interfaces elegir exclusivamente los segmentos que deben usar el relay.
04. Verificar que no existe un segundo relay o servidor DHCP no autorizado que responda en el mismo segmento.

41.8. CARP Status VIP: funcionamiento y objetivo

CARP Status VIP permite seleccionar una dirección virtual CARP para condicionar la ejecución del relay al rol del nodo: cuando esa VIP está en MASTER, el servicio funciona; cuando está en BACKUP, se detiene. La opción resulta útil en clústeres de alta disponibilidad porque evita que ambos nodos envíen solicitudes duplicadas hacia el servidor.

El valor none significa que no se ha elegido una VIP de control. En despliegues sin CARP puede ser apropiado; en un clúster es necesario valorar la coordinación de ambos nodos y confirmar visualmente el estado en Status → CARP (failover).

41.9. CARP en alta disponibilidad: precondiciones y cautelas

Para usar CARP Status VIP se requiere una VIP CARP previamente configurada y estable, sincronización coherente de la configuración y una estrategia documentada de conmutación. Durante una transición a MASTER puede existir una breve pausa antes de que el servicio quede disponible. Si ambos nodos creen ser MASTER se deben investigar primero problemas de CARP y capa 2; cambiar el relay de forma improvisada puede agravar la incidencia.

No confundir redundancias. El control CARP de pfSense regula si el agente relay está activo; no crea por sí mismo alta disponibilidad del servidor DHCP central, ni garantiza que las concesiones sobrevivirán a toda avería.

41.10. Append circuit ID and agent ID to requests: opción 82

Al activar esta casilla se adjunta información de identificación de origen a los mensajes relayed, habitualmente relacionada con la opción 82 de DHCPv4 (Relay Agent Information). Netgate describe el circuit ID como el número de interfaz del firewall y añade también un agent ID. La finalidad es ayudar al servidor remoto a conocer el punto de procedencia de la solicitud, aplicar políticas o mantener registros de red.

La opción debe habilitarse cuando el servidor DHCP y las políticas del entorno la requieran o acepten. Si el servidor rechaza la opción, no identifica el formato esperado o hay equipos intermedios que la transforman, pueden fallar las concesiones. Es recomendable comenzar con la casilla desmarcada salvo que exista un requisito documentado.

41.11. Consecuencias de activar y desactivar los identificadores

Estado	Efecto	Cuándo usarlo
Desactivado	El relay no añade esos identificadores desde esta opción.	Servicios simples que distinguen subredes por el contexto de relay.
Activado	Añade circuit ID y agent ID según el agente.	Servidor con reglas o auditoría basadas en el punto de acceso.
Se cambia con usuarios activos	Las siguientes solicitudes pueden verse afectadas.	Probar renovaciones controladas y revisar trazas del servidor.

41.12. Upstream Servers: dirección del servicio central

En Upstream Servers se introducen las direcciones IPv4 de los servidores a los que el relay enviará las solicitudes. Deben ser direcciones alcanzables mediante el enrutamiento del firewall, no direcciones de interfaz de los clientes ni nombres ambiguos. Netgate permite múltiples destinos utilizando Add Upstream Server. La pantalla no muestra un campo de puerto personalizado para cada destino.

La presencia de varios destinos no debe interpretarse automáticamente como un balanceador o una reserva coordinada. Cada servidor requiere ámbitos, configuración y comportamiento de respuesta compatibles; se debe probar expresamente cómo responde el conjunto cuando uno falla.

41.13. Add Upstream Server y Save: botones

Add Upstream Server incorpora una nueva casilla de dirección IPv4. Se utiliza cuando existe más de un servidor central previsto. Save guarda la configuración de la pantalla. Antes de guardar deben revisarse los segmentos seleccionados, la disponibilidad de los destinos, la relación con DHCP Server y la opción 82.

Tras guardar no se debe considerar implantado hasta completar una adquisición DHCP desde cada red de clientes.

41.14. Qué ocurre en un intercambio DHCPv4

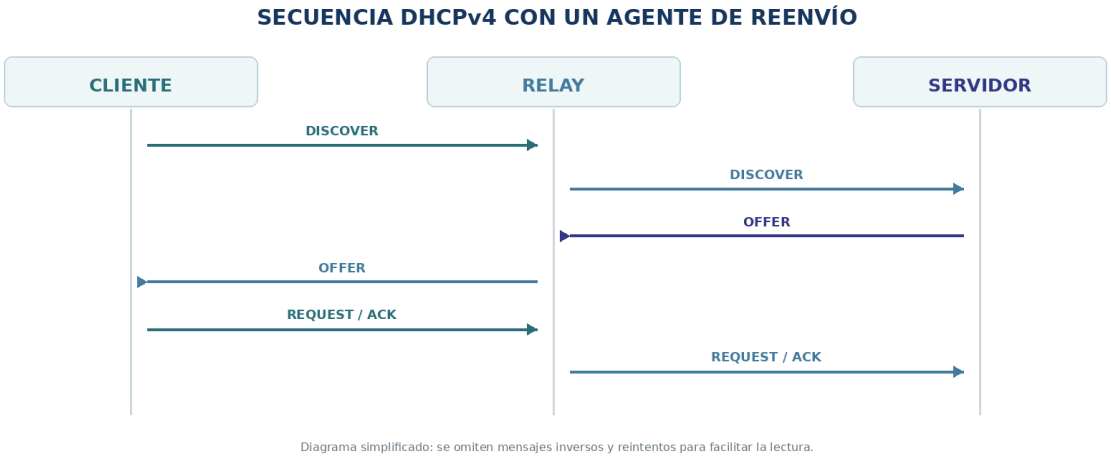


Figura 41.2. Resumen de los mensajes entre cliente, relay y servidor (DORA).

La secuencia básica contiene DISCOVER, OFFER, REQUEST y ACK. El cliente puede emitir inicialmente DHCPDISCOVER como broadcast local, usando UDP 68 hacia UDP 67. El relay recibe la petición y la comunica al servidor remoto. La respuesta debe regresar al relay y luego al cliente; la asignación solo culmina cuando el cliente recibe y acepta la configuración. El diagrama agrupa algunos mensajes para explicar la lógica sin simular una captura real.

41.15. Relay y campo giaddr: selección del ámbito de clientes

El protocolo DHCPv4 contempla el campo giaddr (gateway IP address), usado por los agentes de reenvío para indicar al servidor la red desde la que procede la solicitud y cómo devolver la respuesta. Un servidor central suele elegir el ámbito basándose en el contexto de relay y, en configuraciones avanzadas, también puede usar datos de opción 82. El administrador debe comprobar que el ámbito del servidor corresponde a la subred del cliente, no a la subred del servidor DHCP.

41.16. Puertos de red, difusión y retorno

DHCPv4 utiliza UDP 67 y 68. La difusión inicial del cliente opera dentro de su VLAN; el relay se comunica con el servidor central mediante paquetes encaminables, y el retorno ha de alcanzar al relay. Si el servidor está en otro segmento o atravesando una VPN, comprobar el enrutamiento de ida y vuelta, los filtros en ambos extremos y el diseño del túnel. No abrir UDP 67/68 en Internet ni permitir orígenes arbitrarios para “resolver” un fallo.

Tramo	Punto de verificación	Fallo típico
Cliente → interfaz de acceso	Tramas DHCP y VLAN correctas.	Broadcast no llega por etiquetado o puerto equivocado.
Firewall → servidor DHCP	Ruta válida y UDP pertinente permitido.	Destino sin ruta o firewall intermedio bloquea.
Servidor → relay	Ruta de retorno y servicio activo.	Oferta no vuelve o se envía a nodo incorrecto.
Relay → cliente	Recepción de OFFER/ACK en su red.	Cliente sigue sin concesión por aislamiento o filtrado.

41.17. Ejemplo genérico: red de usuarios con servidor central

Supóngase una red de prácticas 192.0.2.0/24 y un servidor de laboratorio accesible en 198.51.100.10, ambos pertenecientes a bloques de documentación. La finalidad del ejemplo es mostrar relaciones lógicas: la interfaz del relay identifica el segmento local; el servidor remoto aloja un ámbito coherente con esa red y entrega el router y DNS apropiados. No copiar estas direcciones a un sistema operativo: son rangos reservados para documentación.

El diseño correcto debe especificar qué VLAN aloja al cliente, cómo llega al servidor, qué entidad mantiene el ámbito y cuál es la política de recuperación si el servidor central o el enlace de tránsito fallan.

41.18. Procedimiento de implantación inicial

01. Hacer una copia de configuración del firewall y documentar el método de reversión.
02. Mantener acceso administrativo independiente de DHCP mediante dirección estática o consola.
03. Preparar en el servidor remoto un ámbito por red de clientes, con máscara, router, DNS y exclusiones adecuados.
04. Comprobar desde el firewall la ruta hacia cada servidor central y la ruta de retorno.
05. Deshabilitar DHCP Server de pfSense en todas las interfaces, verificando el impacto en las demás redes.
06. Entrar en Services → DHCP Relay y activar Enable.
07. Seleccionar las Downstream Interfaces correspondientes a clientes y completar Upstream Servers.
08. Ajustar CARP Status VIP y Option 82 solo cuando el diseño lo justifique y el servidor esté preparado.
09. Guardar y forzar una renovación controlada desde un equipo de pruebas por cada segmento.
10. Documentar las concesiones, los resultados y la disponibilidad del servicio después del cambio.

41.19. Procedimiento de migración desde DHCP Server local

Una migración exige un inventario previo de los ámbitos atendidos por el servidor local, reservas, exclusiones, opciones, concesiones vigentes y dependencias de DNS. El servidor remoto debe estar listo antes de desactivar el local. El cambio puede producir ventanas en las que los clientes actuales aún conservan la dirección y los nuevos no reciben ninguna; por eso la comprobación debe incluir una solicitud inicial y una renovación, no solo un ping desde un equipo que ya tenía dirección.

01. Exportar de forma segura los datos de configuración necesarios al entorno autorizado sin incorporarlos al libro.
02. Recrear en el servidor central todos los ámbitos de las redes afectadas, incluidas las opciones de router y DNS.
03. Programar ventana de mantenimiento y acceso alternativo de gestión.
04. Desactivar el servidor DHCPv4 de pfSense donde esté habilitado y activar relay.
05. Validar una concesión por segmento y verificar que proviene del servidor correcto.
06. Observar renovaciones posteriores, resolver incidencias de reservas y registrar aceptación.

41.20. Escenario de varias VLAN: un relay para varios ámbitos

Si el firewall enruta varias VLAN de usuarios, puede seleccionarlas conjuntamente como downstream, siempre que cada una disponga de dirección IPv4 y el servidor tenga ámbitos separados. La separación en VLAN no se elimina por compartir servidor DHCP; las reglas entre segmentos siguen dependiendo del firewall. No seleccionar por comodidad interfaces ajenas al alcance del servicio, como enlaces WAN no destinados a clientes.

41.21. Escenario de enlace entre sedes o túnel VPN

Un relay es útil cuando el servidor DHCP central se alcanza a través de un enlace enrutado o una VPN, siempre que el flujo UDP del relay al servidor y su respuesta sean compatibles con las políticas y rutas. No se trata de transportar indiscriminadamente los broadcasts DHCP a través del túnel: el relay transforma la comunicación en un intercambio encaminable. El servidor remoto debe tener ámbitos correctos y una ruta de vuelta al relay.

41.22. Escenario de servidores ascendentes múltiples

Puede configurarse más de una dirección de servidor ascendiente. Antes de hacerlo es necesario decidir si son servidores con ámbitos independientes, un mecanismo de alta disponibilidad compatible o un diseño de asignación coordinado. Si varios servidores responden sin coordinación se arriesgan concesiones

inconsistentes o duplicadas. No asumir que Add Upstream Server reparte carga, ofrece failover garantizado o sincroniza arrendamientos.

41.23. Escenario de dos firewalls mediante CARP

En una pareja HA con CARP, seleccionar el mismo criterio de VIP de control en la configuración apropiada permite que solo el nodo que se encuentre en MASTER mantenga el relay activo. Las rutas, la configuración del servidor central y la sincronización del conjunto deben revisarse en ambos nodos. Al ensayar una conmutación, observar Status → CARP (failover), comprobar la activación del nuevo relay y solicitar una concesión DHCP desde un cliente de prueba.

41.24. DHCPv4 frente a DHCPv6 Relay

La pantalla documentada corresponde a DHCPv4. El servicio Services → DHCPv6 Relay es una función distinta para reenviar solicitudes DHCPv6; tiene su propia configuración y no debe suponerse que la casilla Enable de DHCP Relay IPv4 habilite automáticamente IPv6. En redes IPv6 también deben revisarse los anuncios de router (RA), prefijos y requisitos del servidor DHCPv6. El papel de DHCPv6 no sustituye de forma universal al de RA.

41.25. DHCP Relay frente a DHCP Server y otras alternativas

Servicio	Quién asigna direcciones	Consideración de diseño
DHCP Server en pfSense	El firewall ofrece concesiones directamente.	Menor dependencia externa; no coexistir con DHCPv4 Relay local.
DHCP Relay en pfSense	Servidor DHCP situado en otra red.	Requiere rutas y disponibilidad del servidor central.
DHCPv6 Relay	Servidor DHCPv6 remoto, si está configurado.	Separado de la pantalla y el flujo DHCPv4.
Servidor DHCP local externo	Equipo dedicado en el mismo segmento.	Si responde directamente, el relay puede ser innecesario.

41.26. Limitaciones y consideraciones de seguridad

- Habilitar el relay solo en las interfaces que deben recibir clientes; evitar exponer su servicio en zonas externas no previstas.
- Verificar que el servidor remoto no entregue gateways incorrectos ni DNS fuera de la política corporativa.
- Revisar la posibilidad de servidores DHCP falsos y el uso de DHCP snooping en los switches cuando se disponga de esa función.
- Entender que Option 82 aporta contexto administrativo, pero no constituye por sí misma autenticación criptográfica del dispositivo.
- Restringir el acceso a UDP 67/68 según origen/destino realmente necesarios y evitar reglas universales.
- Vigilar la disponibilidad del servidor central y del camino de red, pues el relay no conserva una base propia de concesiones.

41.27. Verificación desde los clientes DHCP

En un equipo de ensayo con conectividad segura de recuperación, solicitar una concesión inicial y confirmar dirección, máscara, puerta de enlace, DNS, tiempo de concesión y servidor que la proporciona. Verificar también la renovación y la obtención de dirección tras reconectar la interfaz. Las pruebas deben repetirse por cada VLAN incluida en Downstream Interfaces.

Validación	Resultado esperado	Evidencia de laboratorio
Concesión inicial	Cliente obtiene datos del ámbito correcto.	Salida saneada de la configuración de red.
Router por DHCP	Coincide con la puerta de enlace de la VLAN.	Tabla de rutas y prueba de conectividad.
Resolución DNS	Consulta normal a servidores autorizados.	Consulta de nombre de prueba sin datos sensibles.

Validación	Resultado esperado	Evidencia de laboratorio
Renovación	El cliente puede renovar al vencer T1/T2.	Evento de DHCP y temporizadores anonimizados.
Red adicional	Cada VLAN recibe su propio ámbito.	Prueba por segmento y control de máscara.

41.28. Comprobación en el firewall: servicio, registros y capturas

La ruta Status → Services permite comprobar servicios disponibles y su estado. Status → System Logs, pestaña DHCP, reúne eventos del subsistema DHCP; algunas revisiones y backends pueden mostrar más o menos detalles. El instrumento más concluyente para aislar el punto de fallo es Diagnostics → Packet Capture: capturar UDP 67/68 primero en la interfaz de clientes y luego en la interfaz utilizada para alcanzar al servidor, evitando guardar PCAP con datos reales en documentación pública.

Una captura demuestra lo que entra y sale por una interfaz, no necesariamente que una regla de firewall haya permitido ese paquete. Se deben contrastar el resultado de la captura, los registros del firewall y la respuesta del servidor.

41.29. Diagnóstico secuencial de fallos

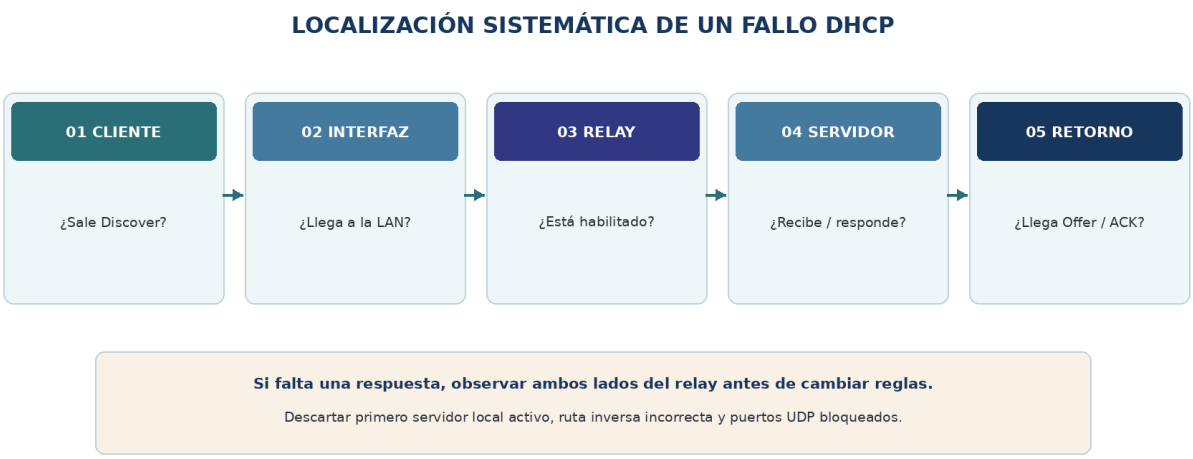


Figura 41.3. Secuencia de comprobación por cliente, relay, servidor y camino de retorno.

Síntoma	Hipótesis principal	Comprobación y corrección
La casilla Enable no puede activarse	DHCP Server local sigue activo.	Deshabilitar servidor DHCPv4 en todas las interfaces, tras planificar el cambio.
No se ve Discover en interfaz	VLAN incorrecta, enlace o equipo cliente.	Revisar puerto, etiquetado, captura en entrada y NIC.
Discover entra, no sale hacia servidor	Relay apagado, interfaz no seleccionada o ruta.	Comprobar Enable, downstream, destino y tabla de rutas.
Servidor recibe, no ofrece	Ámbito incorrecto, política o Option 82.	Revisar logs del servidor y su tratamiento de giaddr/Option 82.
Hay Offer remoto, pero cliente no lo recibe	Ruta inversa, bloqueo o problema local.	Capturar en ambos extremos y revisar reglas.
Falla solo en nodo HA de reserva	Estado CARP o selección de VIP.	Confirmar MASTER/BACKUP y conmutación.
Concesión válida, sin Internet	Router, DNS o políticas posteriores.	Comprobar opciones del servidor, gateway y firewall.

41.30. Pruebas con captura: qué observar

01. En Diagnostics → Packet Capture seleccionar la interfaz de clientes de la prueba.
02. Aplicar un filtro restringido a UDP 67 y 68, con un límite moderado de paquetes.
03. Solicitar una concesión y verificar que aparece DHCPDISCOVER.

04. Capturar en la interfaz de tránsito o consultar el servidor central para confirmar la solicitud reenviada.
05. Comprobar las respuestas DHCPOFFER y DHCPACK, y si regresan al segmento cliente.
06. Borrar y custodiar adecuadamente las capturas: pueden mostrar MAC, nombres de equipo y opciones internas.

41.31. Errores de arquitectura frecuentes

Son especialmente comunes la selección de una WAN por confusión con el término upstream, la ausencia de ámbito para una VLAN nueva, la falta de ruta de retorno del servidor, el uso de Option 82 sin coordinación, la presencia de un segundo servidor DHCP no autorizado y la activación de DHCP Relay sin haber preparado el cambio desde DHCP Server. Las causas se distinguen capturando mensajes a cada lado del relay, no modificando todas las reglas simultáneamente.

41.32. Rendimiento y continuidad del servicio

El relay intercambia tráfico de control relativamente pequeño; su impacto suele ser bajo frente a los datos de usuario. La prioridad de continuidad es la disponibilidad del servidor y la latencia del enlace. Los clientes con concesiones aún válidas pueden seguir comunicándose, pero altas nuevas y renovaciones pueden verse afectadas por la indisponibilidad del servidor central. Monitorizar el camino, los tiempos de respuesta y el agotamiento de ámbitos, además del estado del propio relay.

41.33. Plan de reversión seguro

01. Tener copia de configuración verificada y un usuario de administración con dirección IP estática.
02. Si el relay falla, comprobar rutas, servidor y capturas antes de activar un segundo DHCP.
03. Si debe volver a DHCP Server, detener primero DHCP Relay y recuperar los ámbitos originales.
04. Habilitar DHCP Server en las interfaces pertinentes solo cuando los rangos y reservas estén validados.
05. Solicitar concesiones nuevas desde un cliente de laboratorio y comprobar que no hay servidores duplicados.
06. Registrar la causa del fallo, la duración y la configuración recuperada.

41.34. Lista de aceptación y documentación operativa

Prueba	Criterio de aceptación	Estado de revisión
No coexistencia	DHCP Server local desactivado al usar relay.	Conforme / pendiente
Interfaces	Solo se seleccionaron redes cliente necesarias.	Conforme / pendiente
Ámbitos	Servidor conoce todas las subredes atendidas.	Conforme / pendiente
Opciones	Router, DNS y tiempos de concesión correctos.	Conforme / pendiente
Option 82	Activado solo si existe requisito y prueba positiva.	Conforme / pendiente
CARP	El agente sigue el estado de la VIP si hay HA.	Conforme / pendiente
Fallos	Hay evidencia de captura y procedimiento de reversión.	Conforme / pendiente

41.35. Glosario de DHCP Relay

Término	Definición operativa
DHCP Relay	Agente que reenvía tráfico DHCP entre redes distintas.
Downstream	Interfaz donde se encuentran los clientes que solicitan configuración.
Upstream Server	Servidor remoto que mantiene el ámbito y emite concesiones.

Término	Definición operativa
DORA	Discover, Offer, Request, Acknowledge; intercambio DHCPv4 clásico.
giaddr	Campo del mensaje DHCPv4 relacionado con el agente de reenvío.
Option 82	Información añadida por relay para identificar el contexto de llegada.
CARP MASTER/BACKUP	Estados de una VIP utilizados para decidir el nodo activo.

41.36. Fuentes y documentación oficial de Netgate

DHCPv4 & DHCPv6 Relay — https://docs.netgate.com/pfsense/en/latest/services/dhcp/relay.html

DHCPv4 Server — https://docs.netgate.com/pfsense/en/latest/services/dhcp/ipv4.html

DHCPv6 Server — https://docs.netgate.com/pfsense/en/latest/services/dhcp/ipv6.html

DHCP — índice de servicios — https://docs.netgate.com/pfsense/en/latest/services/dhcp/

CARP Status — https://docs.netgate.com/pfsense/en/latest/monitoring/status/carp.html

Status → Services — https://docs.netgate.com/pfsense/en/latest/monitoring/status/services.html

Packet Capture GUI — https://docs.netgate.com/pfsense/en/latest/diagnostics/packetcapture/webgui.html

DHCP Logs — https://docs.netgate.com/pfsense/en/latest/monitoring/logs/dhcp.html

Troubleshooting Network Connectivity —
https://docs.netgate.com/pfsense/en/latest/troubleshooting/connectivity.html

Los controles y procedimientos deben contrastarse con la documentación de Netgate correspondiente a la versión instalada. Los escenarios son didácticos y no representan una infraestructura identificable.

42 Services → DHCP Server

Kea DHCPv4 · Configuración global y servidor por interfaz LAN

Ruta: Services → DHCP Server → Settings / LAN. Este capítulo estudia los dos formularios visibles y diferencia sus campos de las opciones complementarias que Netgate documenta para las pantallas de Kea DHCP. Las ilustraciones son nuevas, neutras y conceptuales; las pantallas operativas y sus valores no forman parte del libro.



Figura 42.1. Relación entre parámetros globales y el servicio DHCPv4 de una interfaz.

42.1. Qué es DHCP Server y qué función cumple en pfSense Plus

Dynamic Host Configuration Protocol (DHCP) proporciona automáticamente a los equipos una dirección IPv4 y, habitualmente, la máscara de red, la puerta de enlace predeterminada, los servidores DNS, el dominio y los tiempos de concesión. Centralizar este proceso reduce la configuración manual y ayuda a administrar redes con decenas o cientos de equipos.

Kea es el backend DHCP moderno disponible en pfSense Plus. El servicio DHCPv4 se configura por interfaz con dirección IPv4 estática; la pestaña Settings contiene ajustes compartidos de Kea, mientras que LAN define el ámbito y la política de ese segmento concreto. No se debe confundir DHCPv4 Server, DHCPv6 Server y DHCP Relay.

42.2. Ventajas y aplicaciones prácticas del servicio

Ventaja	Aplicación empresarial	Precaución
Asignación automática	Puestos, equipos de trabajo, redes de visitantes.	No entregar direcciones ya reservadas o usadas.
Gestión centralizada	Políticas de DNS, gateway y vigencia coherentes.	Revisar compatibilidad con aplicaciones internas.
Pools por segmento	Separar equipos de oficina y dispositivos especiales.	Un pool no representa otra VLAN.
Mapeos estáticos	Equipos que requieren una dirección predecible.	Evitar solapes con las asignaciones dinámicas.
Alta disponibilidad Kea	Dos nodos coordinados ante averías.	Requiere sincronización, rutas y pruebas.

42.3. Alcance de las pantallas de configuración y documentación adicional

La primera vista muestra Settings, con General Settings, High Availability y Custom Configuration. La segunda vista muestra LAN, con General Settings, Primary Address Pool, Server Options y únicamente la cabecera de Other DHCP Options al final. Por tanto, los campos de Other DHCP Options, reservas y funcionalidades ampliadas se explican a partir de la documentación oficial, pero no se presentan como observados en la captura.

42.4. Ruta de acceso, pestañas y prerrequisitos

01. Abrir Services → DHCP Server desde la interfaz administrativa de pfSense Plus.
02. Seleccionar Settings para ajustar las opciones de Kea que se aplican globalmente.
03. Seleccionar LAN para configurar el servidor DHCPv4 de esa interfaz.
04. Comprobar que LAN dispone de dirección IPv4 estática, máscara coherente y acceso de administración.
05. Verificar que no está activo DHCPv4 Relay en el firewall y que no hay otro servidor DHCP no coordinado en el mismo dominio de difusión.

ADVERTENCIA — SERVIDOR Y RELAY pfSense no admite DHCPv4 Server y DHCPv4 Relay activos simultáneamente. Cambiar de uno a otro exige planificar el servicio de todas las interfaces, no solo LAN.

42.5. Cómo trabaja DHCPv4: secuencia DORA

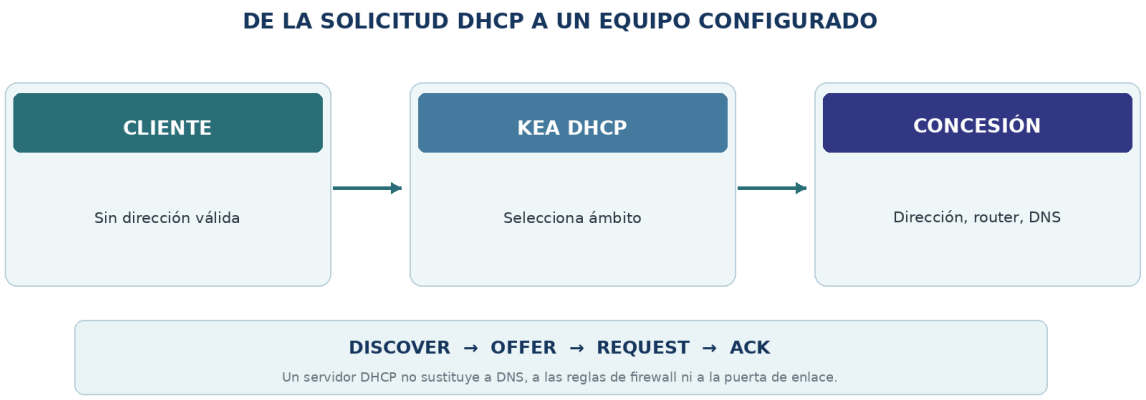


Figura 42.2. Resumen didáctico del intercambio DHCPv4 entre cliente y servidor.

El intercambio habitual comprende DHCPDISCOVER, DHCPOFFER, DHCPREQUEST y DHCPACK; utiliza UDP 67 en el servidor y UDP 68 en el cliente. La configuración se concede por un tiempo limitado y el cliente intentará renovarla antes del vencimiento. La obtención de una dirección válida no garantiza por sí misma que DNS, enrutamiento y reglas de firewall funcionen.

42.6. Pestaña Settings: visión general

Settings agrupa ajustes globales del backend Kea. DNS Registration y Early DNS Registration establecen la política por defecto para las interfaces; High Availability controla la coordinación entre nodos; TLS protege el intercambio HA; JSON Configuration permite ampliar la configuración del motor. El botón Save conserva las modificaciones introducidas.

Bloque visible	Opciones de la pantalla	Función principal
General Settings	DNS Registration; Early DNS Registration.	Registros de nombres en DNS Resolver.
High Availability	Enable; Node Role; Local/Remote Name y Address; Port; Display Advanced.	Conmutación de servicio y sincronización de concesiones.
TLS Transport	Enable TLS transport.	Protege la comunicación de Kea HA.
Custom Configuration	JSON Configuration.	Incorpora parámetros avanzados de Kea.
Acciones	Save; ayudas contextuales.	Guardar y ampliar información de cada parámetro.

42.7. Settings → DNS Registration: registro dinámico en DNS Resolver

Al activar Enable DNS registration, Kea registra de forma predeterminada los nombres de host recibidos en concesiones DHCP, para que los clientes que consultan el DNS Resolver del firewall puedan resolverlos.

Desactivarlo impide ese registro automático por defecto, sin deshabilitar la entrega de direcciones. Kea actualiza los datos del Resolver sin reiniciar Unbound.

La opción global es heredable, no absoluta: cada interfaz puede utilizar Track server, Enable o Disable. En entornos con DNS propio, Active Directory u otros mecanismos de nombres, el administrador debe definir quién mantiene los registros y evitar expectativas de registro externo no configurado.

42.8. Settings → Early DNS Registration: reservas conocidas desde el arranque

Enable early DNS registration registra anticipadamente con el DNS Resolver los nombres definidos en mapeos DHCP estáticos, sin esperar a que el cliente solicite una concesión. Puede resultar útil para dispositivos que deben resolverse por nombre aun cuando están apagados o no renuevan DHCP. Sin marcar, el registro se realiza al solicitarse la concesión, si corresponde.

También admite una excepción por interfaz. Un nombre anticipado disponible en DNS no demuestra que el dispositivo exista o esté conectado: verificar por separado su conectividad real.

42.9. Settings → High Availability: Enable y funcionamiento hot-standby

Enable high availability activa el servicio de alta disponibilidad de Kea, en el que un nodo primario concede direcciones en condiciones normales y un nodo standby sincroniza los datos de concesiones y supervisa al primero. Si el primario falla y se cumplen las condiciones HA, el secundario puede atender nuevos clientes y renovaciones.

Esta casilla no crea automáticamente un clúster completo de firewall. CARP, pfsync, XMLRPC, conectividad de sincronización y las reglas de paso forman parte de la arquitectura HA general, pero cumplen funciones distintas.

42.10. Settings → Node Role: Primary y Standby

Selección	Qué implica	Consecuencia de configuración incorrecta
Primary	Nodo que sirve concesiones normalmente.	Dos primarios sin coordinación generan comportamiento anómalo.
Standby	Nodo preparado para asumir cuando el principal no está disponible.	Si nunca alcanza estado HA correcto, puede no atender clientes.
Cambio de rol	Debe acompañarse de revisión de ambos nodos.	Evitar cambios unilaterales en horario de producción.

42.11. Settings → Local Name y Remote Name

Local Name identifica el propio nodo Kea en el intercambio HA; Remote Name identifica al nodo asociado. Deben ser nombres únicos, coherentes entre extremos y válidos con formato similar a un hostname. No son necesariamente los nombres de la LAN, los identificadores de usuario ni los nombres mostrados al cliente DHCP.

La información puede sincronizarse con intercambio de perspectiva entre primario y secundario mediante XMLRPC, según la documentación de Netgate. Antes de habilitar el servicio es necesario verificar qué valores corresponden a cada nodo desde su propio punto de vista.

42.12. Settings → Local Address, Remote Address y Port

Local Address define la dirección IP donde escucha el nodo local para datos de HA; Remote Address indica el destino del par. Habitualmente se usan direcciones de la interfaz dedicada de sincronización. El puerto mostrado junto a las direcciones especifica el puerto de comunicación del servicio; el valor predeterminado oficial de Kea HA para DHCPv4 es TCP 8765.

Distinguir claramente las direcciones de sincronización de las direcciones entregadas a clientes y de la VIP CARP del gateway. Verificar reglas de firewall, rutas, resolución local y conectividad bidireccional del puerto configurado.

42.13. Settings → Display Advanced: parámetros adicionales de HA

El botón Display Advanced expande los parámetros de sincronización que documenta Netgate. No están desplegados en la captura; por eso la siguiente tabla describe su función oficialmente documentada, no un estado visto en pantalla.

Parámetro de Netgate	Valor predeterminado	Función / cautela
Heartbeat Delay	10 000 ms	Intervalo de comprobación del otro nodo.
Max Response Delay	60 000 ms	Tiempo hasta considerar interrumpida la comunicación; mayor que heartbeat.
Max Ack Delay	60 000 ms	Tiempo relacionado con solicitudes de cliente sin respuesta.
Max Unacked Clients	0	Umbral previo a partner-down; un valor excesivo puede retrasar la atención.
Max Rejected Updates	10	Umbral de rechazos de actualización que conduce a estado terminado.

42.14. Settings → TLS Transport y Enable TLS transport

Enable TLS transport permite cifrar los latidos y los datos de concesiones transmitidos por Kea HA. La documentación describe además Server Certificate y Mutual TLS / Client Certificate cuando están disponibles. La seguridad real depende de certificados válidos, confianza compartida y acceso restringido al enlace de sincronización.

Los ajustes TLS no se sincronizan mediante XMLRPC y se deben preparar manualmente en ambos dispositivos. Activar TLS solo en un extremo o elegir certificados que el otro no confía puede impedir la sincronización. No incrustar certificados ni claves privadas en documentación operativa.

RIESGO DE DISPONIBILIDAD Las modificaciones HA/TLS deben ejecutarse desde un canal de gestión alternativo, con copia de configuración, ventana de mantenimiento y prueba de retorno a servicio.

42.15. Settings → JSON Configuration: propósito y alcance

JSON Configuration recibe un objeto JSON que se fusiona con la sección Dhcp4 del fichero de configuración Kea generado por pfSense. Debe estar bien formado, sin incluir de nuevo la clave superior “Dhcp4”. Permite utilizar ajustes que la interfaz gráfica aún no expone o ajustar parámetros existentes.

No es un editor libre del archivo completo, ni debe copiarse aquí la salida íntegra de Kea. Los fragmentos se guardan en config.xml y viajan con las copias de configuración. Netgate indica que pfSense valida el resultado antes de iniciar Kea y, si el fragmento provoca una configuración inválida, avisa e intenta iniciar sin ese bloque personalizado.

42.16. Settings → criterios de seguridad para JSON y Save

- Mantener vacío JSON Configuration cuando el caso de uso pueda resolverse con controles nativos.
- Validar sintaxis y semántica, evitar claves duplicadas o cambios que contradigan la configuración generada.
- No insertar contraseñas, claves API, secretos o rutas internas en ejemplos de publicación.
- Mantener copia previa y procedimiento para retirar el bloque JSON en caso de fallo.
- Guardar, revisar avisos de pfSense y comprobar la concesión y renovación desde un cliente controlado.

42.17. Pestaña LAN: visión general y secciones visibles

La pestaña LAN configura un servidor DHCPv4 específico para esa interfaz. En el material mostrado figuran General Settings, Primary Address Pool, Server Options y el encabezado Other DHCP Options. La vista identifica el backend Kea, la posibilidad de habilitar el servicio y dos ajustes DNS que pueden seguir la política global o sustituirla.

42.18. LAN → DHCP Backend y Enable

DHCP Backend es informativo: muestra qué motor presta el servicio y no se modifica desde esta línea. El backend global se elige en System → Advanced → Networking. Enable DHCP server on LAN interface activa o desactiva la entrega de concesiones en esa interfaz concreta; desmarcarlo afecta a las nuevas asignaciones y renovaciones que dependen de ese servidor, aunque algunos equipos con concesión vigente continúen temporalmente conectados.

Antes de deshabilitarlo, asegurar que existe otro mecanismo válido para configurar los clientes y conservar acceso a la administración del firewall. La pestaña LAN se corresponde con una red L3, no con cualquier puerto físico que lleve la etiqueta LAN.

42.19. LAN → Deny Unknown Clients: tres políticas posibles

Opción	Comportamiento	Uso recomendado
Allow all clients	Cualquier cliente válido puede solicitar una concesión del pool.	Redes de trabajo comunes o invitadas con controles adicionales.
Allow known clients from any interface	Solo equipos con mapeo estático definido en alguna interfaz.	Inventario gestionado en múltiples segmentos.
Allow known clients from only this interface	Solo equipos conocidos por mapeos de esta interfaz.	Segmentos más controlados, con mantenimiento cuidadoso.

El control se aplica al pool: un pool adicional puede aplicar otra política. No equivale a una autenticación de red: un usuario podría fijar manualmente una dirección o suplantar una MAC. Para protección efectiva considerar 802.1X, DHCP snooping, ACL de switch y segmentación.

42.20. LAN → Ignore Client Identifiers (UID)

Do not record a unique identifier (UID) evita que el servidor tenga en cuenta el identificador DHCP de cliente en los datos de concesión cuando se facilita; puede corregir situaciones en que el mismo hardware arranca sistemas distintos con identificadores diferentes. Netgate advierte que este comportamiento contradice la especificación DHCP y debe reservarse a problemas bien identificados.

No debe emplearse como primera solución a duplicidad de direcciones. Antes, revisar concesiones, cambios de hardware, suplantación de MAC, dos servidores activos y los mensajes del motor Kea.

42.21. LAN → DNS Registration: Track server, Enable y Disable

Valor	Efecto práctico
Track server	Hereda la política establecida en Settings → DNS Registration.
Enable	Activa registro de nombres DHCP con el DNS Resolver para esta interfaz.
Disable	Desactiva ese registro para esta interfaz, aunque globalmente esté activo.

42.22. LAN → Early DNS Registration: tres opciones

La lista Track server / Enable / Disable funciona igual que el ajuste anterior, pero afecta a los nombres definidos en mapeos estáticos y a su pre-registro en DNS Resolver. Track server evita una política redundante; Enable fuerza la disponibilidad anticipada, y Disable impide el pre-registro en esta interfaz.

42.23. LAN → Primary Address Pool: Subnet y Subnet Range

Subnet muestra la subred IPv4 de la interfaz (solo lectura). Subnet Range indica como orientación el intervalo de hosts utilizables, sin excluir por sí mismo todas las direcciones administrativamente ocupadas, como la interfaz del firewall o VIP adicionales. El administrador debe calcular las exclusiones y no interpretar este rango de referencia como un pool ya asignable completo.

El rango disponible depende de la dirección y máscara configuradas en Interfaces → LAN. Si se cambia dicha interfaz, habrá que verificar la coherencia del ámbito DHCP; modificar una máscara puede provocar solapes, pérdida de acceso o concesiones inválidas.

42.24. LAN → Address Pool Range: From y To

From especifica la primera IPv4 que Kea podrá conceder y To la última. Ambos extremos se incluyen. Deben pertenecer a la subred de la interfaz, estar correctamente ordenados y no coincidir con direcciones estáticas, gateways, VIP ni rangos adicionales. Los campos no representan direcciones asignadas a un equipo concreto: describen el intervalo de concesión.

EJEMPLO CONCEPTUAL En documentación puede representarse un pool mediante las variables [INICIO_POOL] y [FIN_POOL]. Para una configuración real hay que introducir direcciones válidas de la subred autorizada; no copiar direcciones de redes publicadas como ejemplos.

42.25. LAN → Additional Pools: Add Address Pool

Add Address Pool permite definir un segundo tramo de direcciones dentro de la misma subred. Es adecuado para reservar huecos entre bloques, disponer de un pool de ampliación o aplicar políticas distintas a una clase de equipos. En general, las opciones no definidas en el pool adicional heredan las del ámbito principal.

Un pool adicional no crea una red VLAN independiente, no añade un segmento enrutado y no corrige un diseño de direccionamiento insuficiente. Antes de crear uno, validar que no se superpone al principal ni a otros pools de la interfaz.

42.26. LAN → Server Options: WINS Servers

WINS Servers permite comunicar hasta dos servidores de Windows Internet Name Service, mecanismo histórico de resolución NetBIOS. Únicamente conviene configurarlo si existe una dependencia heredada específica. En un entorno moderno que no utilice WINS, dejarlos vacíos evita distribuir servicios innecesarios.

42.27. LAN → Server Options: DNS Servers

DNS Servers entrega a los clientes hasta cuatro direcciones de servidores DNS. Si se dejan en blanco, pfSense puede anunciar su propio DNS Resolver/Forwarder o los DNS generales del firewall, según la configuración. Si la red utiliza Active Directory u otro DNS interno autoritativo, los clientes suelen necesitar las direcciones DNS de ese entorno para resolver correctamente nombres corporativos.

No se debe introducir por costumbre un DNS público si el cliente necesita resolver zonas internas. En HA con DNS local, Netgate recomienda anunciar la dirección virtual CARP del servicio para mantener resolución durante la conmutación.

42.28. Other DHCP Options: opciones adicionales documentadas por Netgate

En la captura solo se ve la cabecera de Other DHCP Options; no se visualizan sus campos. Netgate documenta dentro de la página DHCPv4 opciones de gateway, dominios, arrendamientos, control MAC, NTP, TFTP, arranque por red y mapeos estáticos. Su ubicación exacta y visibilidad pueden variar según backend y versión; estas opciones no se consideran confirmadas visualmente en el ejemplo descrito.

Parámetro documentado	Propósito	Criterio de uso
Gateway	Router predeterminado enviado a clientes.	Vacío si corresponde usar el firewall; CARP VIP en HA.
Domain Name / Search List	Dominio y sufijos DNS de búsqueda.	Mantener consistencia con DNS interno.
Default / Maximum Lease Time	Duración normal y máxima de concesión.	Equilibrar estabilidad y rotación de equipos.
NTP / TFTP	Tiempo y aprovisionamiento de clientes.	Activar solo cuando lo requiera el parque.
Network Booting / PXE	Archivos y servidor para arranque remoto.	Verificar BIOS/UEFI y rutas de arranque.
Static Mappings	Asignación preferente y política de clientes conocidos.	Auditar MAC, IP elegida y exclusiones.

42.29. Other DHCP Options → Gateway y dominios: funcionamiento

Gateway anuncia la puerta de enlace que utilizarán los clientes. Si el propio firewall es el router de esa LAN, en general puede dejarse vacío para que el sistema lo determine. En clústeres HA el valor debe corresponder a la VIP CARP accesible por ambos nodos, no a la IP exclusiva de uno de ellos.

Domain Name determina el sufijo DNS; Domain Search List proporciona una lista de sufijos (opción DHCP 119) para completar nombres cortos. Los clientes pueden tratar de forma diferente esta última opción según su sistema operativo, por lo que se debe verificar desde un equipo Windows, Linux o macOS representativo.

42.30. Other DHCP Options → tiempos de concesión

Default lease time determina la duración asignada cuando el cliente no pide otra; Maximum lease time limita la duración solicitada. Netgate documenta como valores habituales 7 200 y 86 400 segundos, respectivamente. No confundir duración de lease con el período de renovación: los clientes suelen intentar renovar antes de la expiración.

Una concesión demasiado corta eleva renovaciones y puede afectar a sedes con conectividad inestable; una excesivamente larga retrasa la recuperación de direcciones cuando cambian los clientes. La elección depende de tamaño de pool, movilidad, continuidad y control operativo.

42.31. Other DHCP Options → reservas y mapeos estáticos

Static Mappings permite definir una preferencia de IP asociada a MAC y, opcionalmente, un Client Identifier, hostname y descripción. Netgate explica que el mapeo no debe entenderse como una exclusividad absoluta de la dirección ante uso manual o conflictos; la práctica de la GUI es situar el mapeo fuera de los pools dinámicos. También es posible registrar solo una MAC como cliente conocido en políticas restrictivas.

En sistemas críticos, una reserva DHCP no sustituye la documentación del direccionamiento. Verificar que ninguna dirección quede compartida entre una reserva, un equipo estático o una VIP.

42.32. Other DHCP Options → NTP, TFTP, PXE y configuraciones específicas

Las opciones NTP permiten indicar servidores de hora a clientes; TFTP suele utilizarse para terminales y dispositivos que necesitan archivos de configuración. Network Booting incorpora opciones de Next Server y ficheros de arranque para diversas arquitecturas. Estas opciones son útiles en despliegue automatizado, pero deben rellenarse según las características del dispositivo y nunca suponiendo que un valor genérico funciona para todos los equipos.

Netgate diferencia opciones dependientes del backend: por ejemplo, OMAPI, Failover Peer IP y determinadas funciones heredadas de ISC aparecen documentadas como “ISC Only” y no deben tratarse como opciones activas de Kea.

42.33. Relación entre DHCP Server, DNS Resolver y firewall

DHCP asigna parámetros al dispositivo; DNS convierte nombres en direcciones; las reglas de firewall permiten o bloquean comunicaciones. Activar DNS Registration no hace que el DNS Resolver funcione si está deshabilitado, ni habilita automáticamente el acceso a DNS a través de una regla denegada. Debe comprobarse cada etapa de forma independiente.

En un entorno con servidor DNS externo es necesario decidir si se publicarán nombres mediante el mecanismo local de Kea o si la infraestructura DNS se actualizará por otro procedimiento controlado.

42.34. Seguridad: clientes conocidos, servidores no autorizados y segmentación

- Comprobar que no haya dos servidores DHCP no coordinados respondiendo en la misma VLAN.
- No interpretar “Deny Unknown Clients” como control de acceso total: es posible configurar IPv4 manualmente.
- Mantener los rangos libres de direcciones estáticas, VIP y duplicados.

- Aplicar seguridad L2 mediante DHCP snooping, control de puertos o 802.1X cuando el equipamiento lo permita.
- Restringir el acceso administrativo al firewall y no guardar identificadores reales de clientes en documentos públicos.
- Observar las concesiones y los registros antes de aumentar el tamaño del ámbito o alterar identificadores.

42.35. Procedimiento paso a paso: configurar un DHCPv4 LAN básico

01. Realizar una copia de la configuración de pfSense y disponer de acceso alternativo al firewall.
02. Comprobar la subred IPv4 real de la interfaz y la ausencia de DHCPv4 Relay activo.
03. Abrir Services → DHCP Server → Settings y decidir la política de registro DNS global.
04. Mantener deshabilitado High Availability si no existe un par Kea configurado.
05. Guardar Settings y pasar a la pestaña LAN.
06. Activar Enable DHCP server on LAN interface.
07. Seleccionar la política Deny Unknown Clients apropiada para el entorno.
08. Elegir DNS Registration y Early DNS Registration de acuerdo con la política global.
09. Definir From y To dentro de la subred, sin solapes con direcciones reservadas.
10. Rellenar DNS y otras opciones solo cuando la configuración automática no sea la esperada.
11. Guardar los cambios; conectar un cliente de laboratorio y comprobar dirección, gateway, DNS, lease y navegación permitida.

42.36. Procedimiento: habilitar el registro DNS de concesiones

01. Verificar que DNS Resolver esté activo y escuche para los clientes autorizados.
02. En Settings activar DNS Registration y, cuando proceda, Early DNS Registration.
03. En LAN dejar Track server o seleccionar Enable si se requiere excepción local.
04. Crear o revisar un mapeo estático de prueba con nombre no identificativo y guardar.
05. Solicitar o renovar una concesión en el cliente de prueba.
06. Consultar el nombre mediante el DNS Resolver esperado y comprobar la respuesta sin confundirla con conectividad del equipo.

42.37. Procedimiento: incorporar un pool adicional

01. Revisar el mapa autorizado de direcciones y los rangos ya usados.
02. Acceder a LAN → Additional Pools → Add Address Pool.
03. Definir un intervalo independiente dentro de la misma subred.
04. Establecer, si procede, la política de clientes o sus opciones específicas.
05. Guardar y probar concesiones con un cliente controlado destinado a ese pool.
06. Verificar en Status → DHCP Leases que los rangos se emplean conforme al diseño.

42.38. Procedimiento: alta disponibilidad Kea con TLS

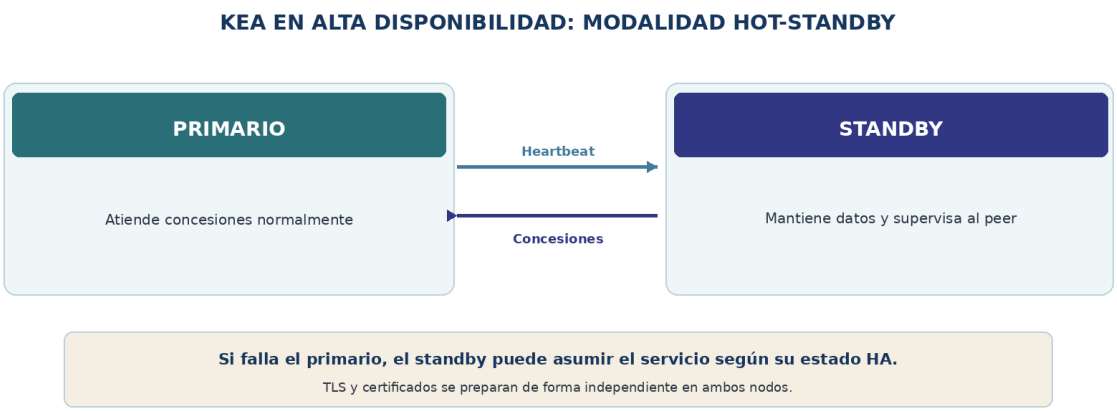


Figura 42.3. Comportamiento lógico primario/standby del servicio DHCPv4 con Kea.

01. Preparar primero la arquitectura HA de pfSense (interfaces Sync, reglas, CARP, configuración sincronizada y hora correcta).
02. Activar Kea como backend en ambos nodos.
03. Configurar un único Primary y un único Standby, con nombres locales y remotos coherentes.
04. Indicar direcciones de sincronización y puertos alcanzables en ambas direcciones.
05. Mantener los parámetros Advanced por defecto salvo requisito documentado.
06. Si se activa TLS, configurar manualmente certificados y confianza en ambos nodos.
07. Sincronizar y verificar los estados de HA desde Status → DHCP Leases.
08. Ensayar una conmutación controlada, obtener y renovar concesiones y validar el retorno del primario.

42.39. Diagnóstico estructurado de problemas DHCP

Síntoma	Causa probable	Prueba dirigida
No hay dirección IPv4	DHCP desactivado, VLAN incorrecta o servicio no alcanzable.	Captura de UDP 67/68 y revisión del estado del daemon.
Dirección inesperada	Servidor DHCP no autorizado, ámbito equivocado.	Comprobar identificador de servidor en concesión.
Dirección correcta, sin DNS	DNS Servers erróneos o DNS Resolver no operativo.	Consultas DNS directas y comprobación de reglas.
Dirección correcta, sin salida	Gateway o reglas/NAT ajenos a DHCP.	Examinar router anunciado y ruta de paquetes.
Nombre DHCP no resuelve	Registro deshabilitado o política por interfaz.	Comprobar DNS Registration y Resolver.
Standby no toma el relevo	HA sin sincronizar, firewall o TLS mal configurado.	Revisar heartbeats, estados HA y conexión TCP.
Concesiones duplicadas	Solapes, servidores no coordinados, direcciones fijas.	Auditar pools, mapeos y tráfico de OFFER.

42.40. Verificación desde Windows, Linux y pfSense

En Windows, ipconfig /all permite comprobar servidor DHCP, dirección, máscara, router, DNS y vencimiento. En Linux se puede utilizar el gestor de red del sistema, journalctl para el servicio correspondiente o herramientas DHCP disponibles. En pfSense, Status → DHCP Leases refleja el inventario y el estado del pool; Diagnostics → Packet Capture permite observar DISCOVER, OFFER, REQUEST y ACK durante una prueba acotada.

No debe ejecutarse una liberación masiva de concesiones en una red productiva. El borrado de toda la base de leases es una operación disruptiva y no forma parte de una comprobación ordinaria.

42.41. Indicadores operativos y capacidad del pool

Indicador	Interpretación	Acción preventiva
Porcentaje de pool usado	Capacidad real disponible para nuevas solicitudes.	Ampliar con criterio o revisar duración de leases.
OFFER sin ACK	El cliente no culmina la solicitud.	Captura del intercambio y análisis de filtros/L2.
Solicitudes repetidas	Cliente sin respuesta, red inestable o servidor duplicado.	Inspeccionar enlaces y estado de Kea.
DNS no coherente	Opciones entregadas no corresponden al DNS esperado.	Verificar la política DNS de la interfaz.
Heartbeats HA irregulares	Conectividad o certificación del peer degradada.	Probar Sync/TLS antes de fallos reales.

42.42. Plan de reversión ante un cambio fallido

01. Mantener una copia reciente y un equipo de administración con IP fija, fuera del rango DHCP afectado.
02. Registrar parámetros previos de Settings y LAN y guardar evidencia en un repositorio privado.
03. Si un cambio de rango falla, restaurar From/To y las opciones de gateway/DNS previas.
04. Si falla HA, revisar rol, direcciones, puerto, reglas de Sync y TLS en ambos nodos antes de cambiar otra opción.
05. Retirar el último fragmento JSON si está relacionado con el error y comprobar avisos del motor.
06. Validar una concesión nueva y una renovación controlada antes de cerrar la incidencia.

42.43. Escenarios empresariales representativos

Escenario	Diseño razonable	Comprobación final
Oficina con una LAN	Pool único, DNS local o corporativo según necesidad.	Clientes renuevan y alcanzan recursos permitidos.
LAN con equipos fijos	Reservas fuera de pool; nombres controlados.	IP y DNS previstos tras reinicio del equipo.
Red de visitantes	Ámbito segregado, política de firewall restrictiva.	Sin acceso a redes internas no autorizadas.
Red con expansión	Pool adicional sin solapes; inventario de direcciones.	Consumo y agotamiento monitorizados.
Clúster de firewall	Kea HA con peer sincronizado y VIP CARP.	Prueba de fallo y recuperación de concesiones.

42.44. Matriz de aceptación técnica

Comprobación	Criterio de aceptación	Registro
Backend y servicio	Kea activo; DHCP por interfaz según diseño.	Conforme / pendiente
Relación con relay	No existe DHCPv4 Relay simultáneo.	Conforme / pendiente
Ámbitos	Pools íntegros en subred y sin solapes.	Conforme / pendiente
Opciones cliente	Gateway, DNS y lease coherentes.	Conforme / pendiente
Registro DNS	Política global/local y resolución verificadas.	Conforme / pendiente
HA (si aplica)	Peer sincronizado; TLS correcto; conmutación validada.	Conforme / pendiente
Seguridad	Servidor no autorizado descartado; gestión protegida.	Conforme / pendiente
Reversión	Copia comprobada y procedimiento de retorno probado.	Conforme / pendiente

42.45. Glosario esencial

Concepto	Significado
Kea DHCP	Motor moderno de servicio DHCP disponible en pfSense Plus.
Lease / concesión	Asignación temporal de configuración de red a un cliente.
Scope / Pool	Intervalo del que se ofrecen direcciones IPv4.
DORA	Discover, Offer, Request y Acknowledge.
DNS Registration	Registro dinámico de nombres DHCP en DNS Resolver.
Early DNS Registration	Registro anticipado de hostnames de mapeos estáticos.
Static Mapping	Asociación administrada entre identificación del cliente y dirección preferente.
CARP VIP	IP virtual compartida para continuidad de servicio del clúster.
Hot Standby	Secundario sincronizado que asume cuando el primario falla.
XMLRPC	Mecanismo de sincronización de configuración entre nodos pfSense.

42.46. Referencias oficiales de Netgate y criterios de versión

Kea Settings Tab — https://docs.netgate.com/pfsense/en/latest/services/dhcp/kea-settings.html

DHCPv4 Server — https://docs.netgate.com/pfsense/en/latest/services/dhcp/ipv4.html

DHCP — índice de servicios — https://docs.netgate.com/pfsense/en/latest/services/dhcp/

DHCPv4 Status y concesiones — https://docs.netgate.com/pfsense/en/latest/monitoring/status/dhcp-ipv4.html

Troubleshooting High Availability DHCP Failover — https://docs.netgate.com/pfsense/en/latest/troubleshooting/ha-dhcp-failover.html

High Availability Configuration Example — https://docs.netgate.com/pfsense/en/latest/recipes/high-availability.html

Static Mappings Inside DHCP Pools — https://docs.netgate.com/pfsense/en/latest/services/dhcp/mappings-in-pools.html

High Availability Cluster — https://docs.netgate.com/pfsense/en/latest/solutions/reference/highavailability/

Disponibilidad de las opciones. Los controles de las dos pestañas y sus formularios pueden variar según la edición o versión de pfSense Plus y el backend activo. Las referencias oficiales permiten contrastar las opciones adicionales. Los esquemas y datos de ejemplo son genéricos.

43 Services → DHCPv6 Relay y DHCPv6 Server

Reenvío de solicitudes · Kea Settings · LAN · Router Advertisements

Rutas de gestión: Services → DHCPv6 Relay; Services → DHCPv6 Server → Settings; Services → DHCPv6 Server → LAN. Se estudian tanto los controles principales como las opciones documentadas de Kea, las reservas, la delegación de prefijos y su coordinación con los anuncios de router.

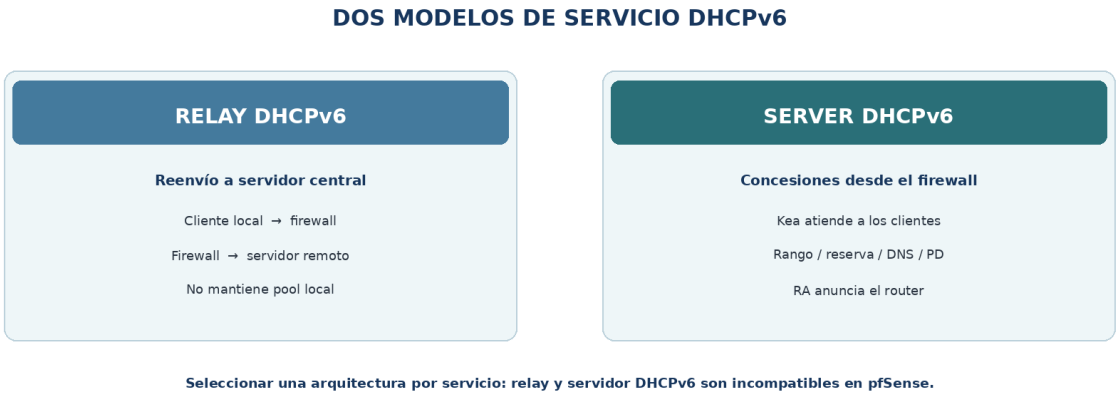


Figura 43.1. Relay frente a servidor local: dos arquitecturas alternativas para la distribución IPv6.

43.1. Objetivo y alcance de los servicios DHCPv6

DHCPv6 permite a los clientes IPv6 obtener direcciones administradas y parámetros como servidores DNS; también permite delegar prefijos a routers descendentes. En pfSense Plus hay dos enfoques excluyentes: DHCPv6 Relay reenvía las solicitudes a un servidor situado en otra red, mientras que DHCPv6 Server entrega las opciones desde el propio firewall con el backend configurado, habitualmente Kea.

Los dos mecanismos no sustituyen ICMPv6 Router Advertisement (RA). Para que un cliente localice su router predeterminado requiere anuncios RA adecuados o una configuración manual; DHCPv6 no incorpora una opción de “gateway” equivalente a DHCPv4.

43.2. Ventajas, aplicaciones y criterio de elección

Escenario	Servicio preferido	Condición operativa
Servidor central corporativo	DHCPv6 Relay	Conectividad IPv6 y políticas hacia servidor upstream.
Sucursal autónoma	DHCPv6 Server	Prefijo IPv6 válido, Kea y RA configurados.
Dos firewalls con HA	Kea HA o relay condicionado por CARP	Diseño consistente de VIP, sincronización y router RA.
Terminales que solo usan SLAAC	Router Advertisement	No obligar al cliente a obtener dirección por DHCPv6.
Router downstream que necesita subredes	Server con Prefix Delegation	Bloque delegado enrutado y dimensionado.
DECISIÓN DE ARQUITECTURA No activar DHCPv6 Server y DHCPv6 Relay a la vez en el mismo pfSense. La GUI advierte que el servicio relay no puede habilitarse mientras el servidor DHCPv6 esté activo en cualquier interfaz.		

43.3. Mapa funcional: DHCPv6, SLAAC, RA y DNS

Componente	Responsabilidad	No debe confundirse con
DHCPv6 Server	Concesiones, DNS, opciones y delegación de prefijos.	Anuncio de puerta de enlace.
DHCPv6 Relay	Reenvío de mensajes entre segmentos.	Servidor de concesiones local.

Componente	Responsabilidad	No debe confundirse con
RA / radvd	Anunciar router y políticas de autoconfiguración.	Servidor DHCPv6.
SLAAC	Direcciones generadas por el cliente a partir de RA.	Reserva DHCPv6 controlada por DUID.
DNS Resolver	Resolución de nombres y registros de leases Kea.	Servidor de direccionamiento.

43.4. Rutas, prerrequisitos y operaciones seguras

01. Verificar que el firewall dispone de un prefijo IPv6 válido y enrutado hacia las redes internas previstas.
02. Decidir si se utilizará relay hacia un servidor central o servidor local Kea; documentar la elección.
03. Comprobar Interfaces → LAN (IPv6 estática o Track Interface) y el funcionamiento de ICMPv6.
04. Revisar Services → Router Advertisement, DNS y reglas de firewall antes de cambiar el servicio.
05. Obtener una copia de la configuración y disponer de consola o acceso alternativo por si se interrumpe la red.

43.5. DHCPv6: secuencia de mensajes y transporte

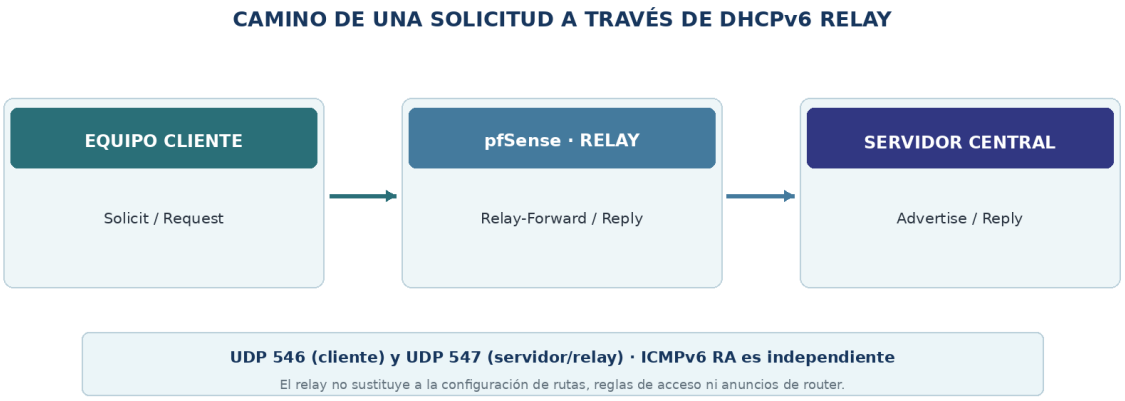


Figura 43.2. Intercambio conceptual entre cliente, relay y servidor remoto.

DHCPv6 utiliza UDP 546 en el cliente y UDP 547 en el servidor o agente relay. Las etapas pueden incluir Solicit, Advertise, Request y Reply; con relay aparecen mensajes Relay-Forward y Relay-Reply. El ciclo concreto varía con el modo de operación y los parámetros del cliente.

No deben bloquearse indiscriminadamente los mensajes ICMPv6 de descubrimiento de vecinos o RA: IPv6 necesita funciones de ICMPv6 para descubrir routers, vecinos y parámetros del enlace. Los servidores upstream deberán ser alcanzables por rutas y reglas apropiadas.

43.6. DHCPv6 Relay: descripción y advertencia principal

Ruta: Services → DHCPv6 Relay. El formulario reúne un aviso de incompatibilidad, Enable, Downstream Interfaces, CARP Status VIP, una opción para añadir identificadores de circuito/agente, Upstream Servers, Add Upstream Server y Save. Si no aparece ninguna interfaz en la lista inferior, se debe revisar su estado IPv6: solo aparecen interfaces elegibles con dirección IPv6.

La pantalla puede impedir activar el relay cuando el servidor DHCPv6 está habilitado en cualquier interfaz. El administrador no debe interpretar la lista vacía o un control deshabilitado como un error del navegador sin antes revisar las condiciones de elegibilidad.

43.7. Relay → Enable y exclusión mutua con DHCPv6 Server

Enable DHCPv6 Relay activa el demonio de retransmisión de mensajes DHCPv6. Desmarcarlo detiene el reenvío, de modo que los clientes nuevos o que necesitan renovar dejan de alcanzar por esa vía al servidor remoto. Una concesión todavía válida no garantiza continuidad indefinida.

Antes de activar Enable, deshabilitar DHCPv6 Server donde esté activo, revisar la supervisión del servicio y comprobar que el servidor central responde desde las redes clientes. El control no crea automáticamente rutas ni reglas de paso a los servidores destino.

43.8. Relay → Downstream Interfaces

Downstream Interfaces es una selección múltiple de las interfaces que reciben las solicitudes originadas por clientes. Deben ser segmentos IPv6 habilitados con dirección válida; una interfaz no disponible puede deberse a direccionamiento ausente o a una configuración no elegible.

Seleccionar únicamente interfaces de acceso a clientes. No se debe seleccionar por rutina una interfaz WAN o de tránsito que no necesita distribuir DHCPv6, para evitar retransmisión accidental desde redes no confiables.

43.9. Relay → CARP Status VIP

CARP Status VIP permite escoger una IP virtual CARP como indicador de la condición operativa del relay: en MASTER el servicio se ejecuta; en BACKUP se detiene. El valor none no vincula el arranque a un VIP CARP. La función sirve para evitar respuestas duplicadas en un clúster, pero depende de que CARP y las reglas de estado funcionen correctamente.

La selección de CARP no vuelve redundante por sí sola al servidor upstream. Se debe diseñar la HA de extremo a extremo y comprobar que un cambio de MASTER provoca el comportamiento esperado del relay.

43.10. Relay → Append circuit ID and agent ID to requests

Esta casilla añade identificadores del circuito o interfaz de origen y del agente relay a los mensajes, para que el servidor ascendente pueda distinguir de qué segmento procede la solicitud. Solo conviene usarla cuando el servidor de destino o la política de provisión exijan esa información.

La incorporación de identificadores puede ser incompatible con políticas existentes del servidor central. Validar previamente el formato esperado y comprobar el intercambio de mensajes con captura de paquetes si la asignación falla.

43.11. Relay → Upstream Servers y Add Upstream Server

Upstream Servers recoge las direcciones IPv6 de los servidores DHCPv6 centrales que recibirán las solicitudes retransmitidas. Add Upstream Server añade otro campo de destino cuando hay varios servidores; no implica necesariamente balanceo, reparto de concesiones o conmutación controlada entre ellos.

Utilizar direcciones de servidor específicas y enrutables, comprobar que pertenecen al destino previsto y evitar introducir gateways, DNS o direcciones de cliente por error. La redundancia del backend DHCP debe configurarse en sus propios servidores.

43.12. Relay → Save, validación y reversión

01. Comprobar que DHCPv6 Server se encuentra deshabilitado en todo el firewall.
02. Elegir Downstream Interfaces que realmente alojan clientes y comprobar direcciones IPv6.
03. Definir un servidor upstream verificable; añadir servidores adicionales solo si procede.
04. Si existe HA, seleccionar CARP Status VIP y comprobar roles MASTER/BACKUP.
05. Activar Relay y guardar. Revisar avisos y estado del servicio.
06. Desde un cliente de pruebas, solicitar configuración DHCPv6 y verificar la concesión en el servidor central; capturar tráfico si falla.

ADVERTENCIA — CAMBIO DE MODELO Deshabilitar un servidor local para habilitar relay cambia dónde se generan y mantienen las concesiones. Planificar la transición para no interrumpir estaciones, telefonía o equipos que dependan de direcciones dinámicas.

43.13. DHCPv6 Server: Settings y LAN

Ruta: Services → DHCPv6 Server. Con Kea hay una pestaña Settings para la política global y pestañas por interfaz, entre ellas LAN, para servir concesiones en subredes específicas. La configuración se administra por separado respecto a DHCPv4, aunque los controles de Kea Settings son análogos.

Solo se ofrecen pestañas para interfaces con direccionamiento IPv6 estático o que siguen un prefijo delegado válido (Track Interface). Si LAN no aparece, verificar primero Interfaces → LAN y la obtención de Prefix Delegation en WAN, si aplica.

43.14. Server Settings → DNS Registration

Enable DNS registration habilita como política global que Kea registre automáticamente en DNS Resolver los nombres de los clientes con concesiones DHCPv6. Es útil para resolver nombres internos desde otros equipos que usan el resolver del firewall. El registro no equivale a una autenticación de cliente ni a la validación de su presencia permanente.

Puede sustituirse por interfaz con Track Server, Enable o Disable. Kea actualiza los datos DNS sin reiniciar de forma disruptiva DNS Resolver, y respeta las reglas de selección de dominio de la configuración DHCP correspondiente.

43.15. Server Settings → Early DNS Registration

Enable early DNS registration permite preinscribir en DNS Resolver los nombres de mapeos estáticos DHCPv6 al arrancar el servicio, sin esperar a una solicitud de concesión. Es útil para sistemas inventariados, pero un nombre publicado anticipadamente no garantiza que el dispositivo se encuentre conectado.

La decisión global también admite excepción por interfaz. No habilitar registro DNS de forma indiscriminada cuando otra plataforma es autoritativa para los nombres del mismo dominio; definir límites y evitar registros contradictorios.

43.16. Server Settings → High Availability: Enable y Node Role

Enable high availability activa el mecanismo Kea Hot Standby, coordinando concesiones y estado entre dos nodos. En funcionamiento normal, Primary atiende solicitudes y Standby mantiene información sincronizada para asumir el servicio ante pérdida del primario. No debe haber dos nodos primarios mal coordinados.

Este mecanismo no sustituye alta disponibilidad del firewall, de las rutas, de las direcciones virtuales ni del acceso DNS. Requiere supervisión, sincronización válida, pruebas de fallo y reglas de firewall que permitan el transporte de HA.

Opción	Funcionamiento	Comprobación
Enable	Activa HA de Kea DHCPv6.	Ambos peers en estado consistente.
Primary	Sirve concesiones en operación normal.	Un solo nodo primario activo.
Standby	Supervisa al primario y puede asumir el servicio.	Concesiones sincronizadas y respuesta ante fallo.
XMLRPC	Puede replicar los parámetros generales de HA.	Verificar perspectiva local/remota invertida.

43.17. Server Settings → Local Name, Remote Name y Node Role

Local Name y Remote Name son nombres lógicos de los peers Kea; deben ser distintos y coherentes, con formato semejante a un nombre de host. Su finalidad es identificar nodos en el intercambio de alta disponibilidad, no publicar nombres DNS a clientes ni sustituir un certificado TLS.

Al sincronizar configuración mediante XMLRPC, pfSense puede intercambiar valores locales y remotos en la copia destinada al secundario. Revisar el resultado desde cada nodo antes de dar por válida la HA.

43.18. Server Settings → Local Address, Remote Address y Port

Local Address indica la dirección donde Kea recibe la comunicación de HA en ese nodo; Remote Address indica la del peer. Su puerto asociado controla la comunicación entre instancias. Habitualmente se usan interfaces dedicadas de sincronización, pero no deben divulgarse en documentación pública.

Según Netgate, el transporte HA puede usar direcciones IPv4 o IPv6 con independencia de la versión de DHCP que se está prestando. Es importante no confundir el direccionamiento de sincronización con el prefijo asignado a clientes.

43.19. Server Settings → Display Advanced: temporizadores de HA

Control avanzado	Valor de referencia Netgate	Consecuencia de un ajuste inadecuado
Heartbeat Delay	10 000 ms	Mensajes demasiado frecuentes o lentos.
Max Response Delay	60 000 ms	Detección tardía o excesivamente sensible; debe superar heartbeat.
Max Ack Delay	60 000 ms	Clasificación prematura o tardía de clientes sin respuesta.
Max Unacked Clients	0	Un umbral alto puede retrasar la toma de control.
Max Rejected Updates	10	Un exceso de discrepancias puede detener el proceso HA.

Estos valores son referencias de la documentación, no recomendaciones universales. Modificarlos solamente cuando haya mediciones y una causa real documentada; el último depende de conflictos en actualizaciones de concesiones entre peers.

43.20. Server Settings → TLS Transport y certificados

Enable TLS transport cifra el tráfico de heartbeat y sincronización de concesiones. En la configuración avanzada de TLS se documentan Server Certificate, Mutual TLS y Client Certificate. Con Mutual TLS cada extremo puede comprobar la identidad del otro mediante certificados apropiados.

TLS Transport no se sincroniza automáticamente por XMLRPC: se configura de forma manual en cada nodo. Garantizar cadena de confianza, certificados vigentes y parámetros compatibles. Si las opciones TLS difieren, la HA puede quedar inoperativa.

SEGURIDAD — SINCRONIZACIÓN KEA Proteger el transporte de alta disponibilidad y restringir el acceso a los peers autorizados. No incluir en documentación nombres operativos de host, IP de sincronización, certificados reales ni claves privadas.

43.21. Server Settings → Custom Configuration y JSON Dhcp6

JSON Configuration permite ampliar la configuración generada de Kea. El contenido debe ser un objeto JSON bien formado; se fusiona en la sección Dhcp6 y no debe incluir por segunda vez la clave superior "Dhcp6". Puede añadir opciones admitidas por Kea que aún no estén presentes en la GUI.

Los fragmentos JSON pueden alterar o sobrescribir ajustes establecidos visualmente. Usarlos únicamente bajo control de cambios, con validación previa y prueba de retorno; pfSense prueba la configuración y, si detecta un error, genera un aviso y puede intentar arrancar Kea sin el fragmento personalizado.

43.22. LAN → condiciones para habilitar DHCPv6

La pestaña LAN está disponible si existe un prefijo IPv6 estático o un prefijo obtenido mediante Track Interface desde una delegación WAN. DHCP Backend presenta el motor activo (Kea o ISC) en modo solo lectura; Enable DHCPv6 server on LAN interface habilita la prestación del servicio en ese segmento.

Si no hay prefijo o la delegación no ha llegado, no se debe inventar un ámbito. Antes de habilitar el servidor, verificar que la dirección y el prefijo de LAN son válidos y que Services → Router Advertisement tiene un modo compatible con el comportamiento requerido.

43.23. LAN → Deny Unknown Clients

Política	Respuesta esperada	Limitación
Allow All Clients	Se atienden las solicitudes del pool.	No impone control de identidad.
Allow known clients from any interface	Acepta clientes con mapeos conocidos en cualquier interfaz.	Necesita un inventario mantenido.
Allow known clients from only this interface	Solo clientes definidos en esta interfaz.	Puede excluir clientes legítimos no inventariados.

La política es por pool. Los mapeos DHCPv6 utilizan DUID, no exclusivamente MAC. No se debe considerar esta selección un control de acceso seguro frente a usuarios que configuren direcciones estáticas, falsifiquen identificadores o se conecten a puertos de switch sin restricción.

43.24. LAN → DNS Registration y Early DNS Registration

Cada política ofrece Track Server (heredar la elección global), Enable (forzar activación local) y Disable (forzar desactivación). DNS Registration afecta a nombres recibidos mediante leases, mientras que Early DNS Registration actúa anticipadamente sobre mapeos estáticos.

En redes que utilizan DNS autoritativo externo, evaluar si el DNS Resolver de pfSense debe almacenar esos registros o si conviene resolverlos mediante otra infraestructura. Las opciones no configuran por sí solas reenvío de consultas de clientes al DNS deseado.

43.25. LAN → Primary Address Pool: Prefix y Prefix Range

Prefix informa del prefijo IPv6 disponible en la interfaz y, cuando procede de delegación, identifica el seguimiento de la interfaz WAN y el Prefix ID. Prefix Range muestra el intervalo cubierto por el prefijo. Son campos informativos: no se asignan direcciones hasta definir un Address Pool Range válido y habilitar el servidor.

Una delegación dinámica puede cambiar si lo hace el prefijo proporcionado por el operador. El diseño debe considerar la renumeración y las implicaciones para rutas, reservas y resolución DNS.

43.26. LAN → Address Pool Range: From, To y Additional Pools

From y To definen los extremos incluidos del rango DHCPv6. Deben pertenecer al prefijo de LAN y From debe ser anterior a To. En interfaces con prefijo dinámico, Netgate permite omitir la porción de prefijo y configurar únicamente los bits de host, que se combinan con el prefijo delegado.

Add Address Pool permite separar intervalos no solapados del mismo segmento, aplicar políticas de asignación a determinadas clases de clientes o ampliar capacidad. Un pool adicional no crea por sí mismo una VLAN ni una nueva red independiente.

43.27. LAN → DHCPv6 Prefix Delegation: Delegated Prefix y Length

La delegación de prefijos DHCPv6 sirve a routers downstream que necesitan subredes completas para sus propias interfaces o VLAN. Delegated Prefix define el bloque enrutado que el servidor reparte, mientras que Delegated Length expresa la longitud de cada prefijo entregado al solicitante.

Por ejemplo, un bloque de documentación 2001:db8:1200::/48 puede dividirse en delegaciones /60, cada una con dieciséis subredes /64. Este ejemplo es puramente didáctico y no representa ninguna instalación. Comprobar que el bloque esté realmente enrutado hacia pfSense antes de publicar una delegación.

43.28. LAN → Server Options: DNS Servers

La sección Server Options permite entregar hasta cuatro servidores DNS IPv6 a clientes. Si se dejan en blanco y pfSense usa DNS Resolver o DNS Forwarder, puede anunciar su propia dirección como DNS; de otro modo, puede emplear servidores generales definidos en System → General Setup.

En un clúster de alta disponibilidad que presta DNS local se recomienda proporcionar la VIP CARP IPv6 correspondiente, evitando que los clientes dependan de la dirección exclusiva de un nodo. En redes con DNS interno autoritativo, anunciar los DNS de ese sistema.

43.29. LAN → Other DHCPv6 Options: dominio, búsqueda y leases

Campo documentado	Finalidad	Consejo
Domain Name	Sufijo de nombre enviado a los clientes.	Coherencia con zonas DNS internas.
Domain Search List	Sufijos para resolver nombres abreviados.	Verificar soporte según cliente.
Default Lease Time	Tiempo predeterminado de concesión (s).	Netgate documenta 7 200 s por defecto.
Maximum Lease Time	Duración máxima (s).	Netgate documenta 86 400 s por defecto.
NTP Servers	Opciones de servidores de tiempo.	Usar solo si los clientes las admiten.
Network Booting	Boot File URL y activación.	Revisar compatibilidad de arranque IPv6.

Las opciones detalladas de la pestaña LAN dependen del motor y de la versión. Las funciones exclusivas de ISC DHCP (como ciertos controles DDNS antiguos y opciones numéricas) no deben presentarse como campos de Kea si no están disponibles.

43.30. LAN → DHCPv6 Static Mappings y DUID

Una reserva DHCPv6 se identifica por DHCP Unique Identifier (DUID), no solo por MAC. Los campos documentados incluyen DHCP Unique Identifier, IPv6 Address opcional, Hostname y Description. La dirección de mapeo debe estar fuera de los pools dinámicos y su existencia no garantiza exclusividad frente a configuraciones manuales.

El DUID puede cambiar por reinstalación, clonación de sistema o acciones administrativas, lo que puede romper una reserva. Protegerlo como identificador operativo y no publicarlo junto con hostnames o direcciones en documentos técnicos.

43.31. Router Advertisements: dependencia indispensable

Modo RA	Comportamiento general	DHCPv6
Disabled	No se envían anuncios RA.	Los clientes no descubren router por RA.
Router Only	Anuncia router, sin DHCPv6/SLAAC dirigidos.	No se solicita DHCPv6 en este modo.
Unmanaged	SLAAC para direcciones de host.	Sin DHCPv6 de direccionamiento.
Managed	Direcciones obtenidas mediante DHCPv6.	Requiere servidor y cliente compatibles.
Assisted	SLAAC y DHCPv6 pueden coexistir.	Adecuado cuando hay clientes heterogéneos.
Stateless DHCP	SLAAC para dirección y DHCPv6 para opciones.	Información adicional, no dirección administrada.

Algunos sistemas móviles, incluidos dispositivos Android, no utilizan DHCPv6 para asignar direcciones y dependen de SLAAC. Por eso conviene revisar Managed frente a Assisted y las capacidades del parque de equipos. El anuncio de router proviene de RA, no de una opción gateway del servidor DHCPv6.



Figura 43.3. Relación conceptual entre alta disponibilidad Kea, concesiones y anuncios de router.

43.32. Procedimiento práctico: DHCPv6 Relay hacia un servidor remoto

01. Confirmar que existe conectividad IPv6 entre el firewall y el servidor central.
02. Desactivar DHCPv6 Server en todas las interfaces donde esté habilitado.
03. Abrir Services → DHCPv6 Relay; seleccionar Downstream Interfaces de clientes.
04. Añadir direcciones IPv6 de los servidores upstream autorizados.
05. Ajustar identificadores de agente si la política del servidor los necesita; elegir CARP si hay HA.
06. Activar el relay y guardar.
07. Revisar Router Advertisements y probar concesión, DNS y salida IPv6 desde un cliente compatible.

43.33. Procedimiento práctico: Kea DHCPv6 Server en LAN

01. Confirmar que existe un prefijo IPv6 válido en LAN, estático o seguido desde WAN.
02. Deshabilitar DHCPv6 Relay antes de activar el servidor.
03. Abrir Services → DHCPv6 Server → Settings y establecer la política DNS requerida.
04. En LAN, habilitar DHCPv6 Server, revisar el prefijo y definir un rango From–To sin solapes.
05. Ajustar DNS y dominio según servicios internos y guardar la configuración.
06. En Services → Router Advertisement → LAN, configurar Managed o Assisted según clientes.
07. Solicitar una concesión DHCPv6, verificar RA, DNS y conectividad de extremo a extremo.

43.34. Procedimiento práctico: reserva estable con DUID

01. Comprobar que el cliente recibe DHCPv6 y localizar su DUID desde la vista de concesiones o el sistema operativo.
02. Definir un mapeo estático con DUID correcto y dirección libre fuera del pool.
03. Asociar hostname y una descripción técnica genérica.
04. Guardar, renovar la concesión y comprobar que el cliente recibe la dirección esperada.
05. Verificar registro DNS si está habilitado y descartar conflictos con equipos configurados manualmente.

43.35. Procedimiento práctico: alta disponibilidad Kea para IPv6

01. Preparar los dos firewalls, la sincronización de configuración y los servicios CARP necesarios.
02. Configurar Settings con Primary y Standby, nombres diferenciados y direcciones de sincronización entre peers.
03. Comprobar temporizadores de HA y habilitar TLS con certificados válidos en los dos nodos.
04. En LAN, indicar como DNS la VIP CARP IPv6 cuando el DNS del propio firewall sea el servicio redundante.
05. Configurar los anuncios RA del router mediante una VIP link-local CARP adecuada.

06. Probar solicitudes durante operación normal y conmutación; revisar leases, rutas y registros.

43.36. Comprobación de funcionamiento: qué verificar

Prueba	Resultado esperado	Herramienta
Servicio activo	Kea o relay habilitado sin incompatibilidades.	Estado del servicio y avisos.
Prefijo LAN	IPv6 correcta y prefijo enrutado.	Interfaces; Status; rutas.
Concesión de cliente	IPv6 del ámbito esperado.	Status → DHCPv6 Leases; cliente.
Anuncio de router	Router predeterminado y modo RA adecuados.	Captura ICMPv6 / sistema cliente.
DNS	Servidores anunciados y resolución interna.	Consulta DNS desde cliente.
Relay	Solicitudes alcanzan servidor upstream.	Packet Capture UDP 546/547.
HA	Conmutación sin concesiones conflictivas.	Estado Kea y logs de HA.

43.37. Diagnóstico: incidencias frecuentes y resolución

Síntoma	Causa probable	Comprobación / solución
No aparece LAN	Interfaz sin IPv6 válida o prefijo no delegado.	Revisar Interfaces → LAN y Track Interface.
Relay no se activa	Servidor DHCPv6 activo en alguna interfaz.	Deshabilitar Server y volver a habilitar Relay.
Cliente tiene IPv6, sin internet	Falta RA, ruta o filtrado ICMPv6.	Inspeccionar RA, gateway y reglas.
Cliente no usa DHCPv6	SO sin soporte de asignación DHCPv6.	Usar SLAAC/Assisted cuando proceda.
Direcciones cambiantes	Prefijo WAN delegado renumerado.	Revisar delegación, DNS y seguimiento.
Fallan reservas	DUID cambia o está duplicado.	Consultar DUID actual y mapeos.
HA sin asumir servicio	TLS, sync o umbrales de failover.	Revisar certificados y contadores de HA.

43.38. Seguridad: controles imprescindibles para DHCPv6

DHCPv6 no autentica por sí solo a los equipos de forma resistente frente a usuarios maliciosos. Las políticas de clientes conocidos dificultan accesos accidentales, pero pueden eludirse mediante direccionamiento manual o suplantación de identificadores. Limitar el servicio a interfaces internas, segmentar las VLAN y restringir la llegada a servidores upstream no autorizados.

Para reducir ataques de RA malicioso o servidores DHCPv6 no autorizados, complementar pfSense con las protecciones del switching compatibles, como RA Guard y DHCPv6 Guard cuando estén disponibles. No bloquear mensajes ICMPv6 necesarios para Neighbor Discovery, Path MTU Discovery ni Router Advertisement.

43.39. Rendimiento y dimensionamiento

El tamaño de un prefijo IPv6 no obliga a ofrecer todas sus direcciones mediante DHCPv6: un pool pequeño y bien delimitado suele facilitar la auditoría. Estimar número de clientes, tiempos de concesión, dispositivos sin DHCPv6 y necesidades reales de Prefix Delegation.

En HA, los temporizadores deben ajustarse de acuerdo con latencia entre nodos y cantidad real de solicitudes; una respuesta prematura ante fallos breves o una espera excesiva pueden perjudicar la continuidad. En relay, validar la disponibilidad de los servidores externos y la pérdida de paquetes.

43.40. Matriz de aceptación y plan de reversión

Control	Criterio de aceptación	Si falla
Arquitectura	Solo server o relay, sin conflicto.	Restaurar servicio previo documentado.
Prefijo y RA	Clientes obtienen router y prefijo correctos.	Revisar LAN y modo RA.
DNS interno	Nombres y dominios se resuelven.	Restaurar política DNS anterior.
Concesiones	Sin solapes ni duplicados.	Revisar pools y mapeos.
HA	Un único primario lógico y standby funcional.	Deshabilitar conmutación problemática.
Seguridad	Sin anuncios/relay desde interfaces no previstas.	Retirar interfaces o reglas de paso.

43.41. Buenas prácticas de administración profesional

- Mantener actualizado el inventario de prefijos, servidores DNS y dependencias de RA sin incluir credenciales en documentación pública.
- Supervisar cambios de prefijo delegado por el proveedor y su impacto en servicios internos.
- No confundir una dirección SLAAC con una concesión ni asumir que todos los dispositivos admiten DHCPv6.
- Usar Kea para nuevas configuraciones salvo requisitos explícitos y documentados del backend heredado.
- Conservar copias previas al cambio y registrar resultados de validaciones desde más de un sistema operativo.

43.42. Glosario esencial

Término	Definición operativa
DHCPv6	Protocolo de configuración dinámica para redes IPv6.
Relay	Agente que traslada solicitudes DHCPv6 a servidores en otra red.
RA	Router Advertisement: anuncia router y parámetros de autoconfiguración.
SLAAC	Configuración autónoma de direcciones por el cliente con prefijos RA.
IA_NA	Identidad DHCPv6 para direcciones no temporales.
DUID	Identificador de cliente empleado por DHCPv6 y reservas.
PD	Prefix Delegation: entrega de bloques IPv6 a routers downstream.
Hot Standby	HA donde un nodo presta servicio y el otro conserva estado listo para asumir.
CARP	Protocolo utilizado por pfSense para direcciones virtuales redundantes.

43.43. Documentación oficial y referencias

- Netgate — DHCPv4 & DHCPv6 Relay
- Netgate — DHCPv6 Server
- Netgate — Kea Settings Tab
- Netgate — IPv6 Router Advertisements
- Netgate — High Availability Configuration Example
- Netgate — Troubleshooting High Availability DHCP Failover
- Netgate — DHCP Server Backend

44 Services → DNS Forwarder

dnsmasq · consulta y caché · Host Overrides · Domain Overrides

Ruta de administración: Services → DNS Forwarder. Esta sección documenta las opciones generales de reenvío DNS y las dos tablas de sobrescrituras, con el propósito de administrar los nombres de manera previsible, segura y verificable.

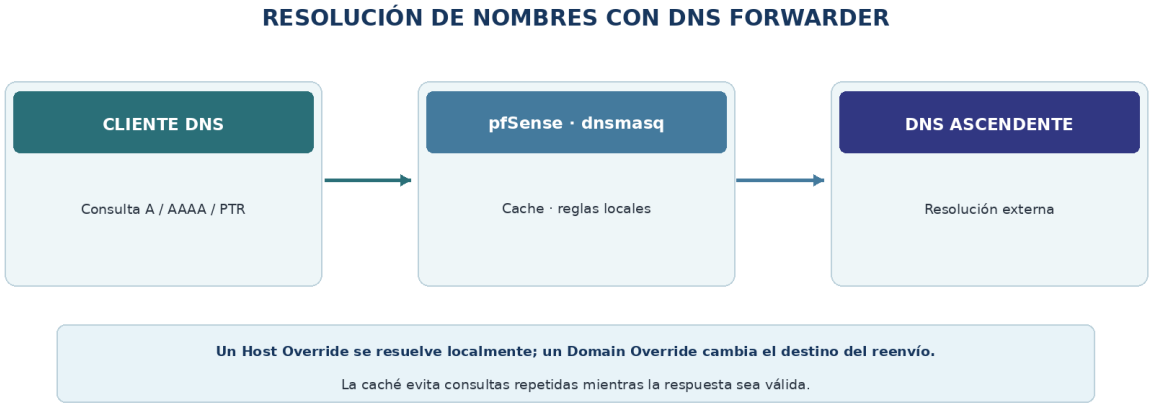


Figura 44.1. Esquema conceptual del cliente, la caché dnsmasq y la consulta a servidores DNS ascendentes.

44.1. Objetivo, ámbito y requisitos

DNS Forwarder ofrece un servicio de reenvío y caché DNS mediante dnsmasq. Escucha consultas de clientes autorizados, resuelve nombres locales definidos por overrides y remite a servidores ascendentes las peticiones que no puede responder localmente. El reenvío reduce el número de consultas repetidas y permite centralizar la elección de servidores DNS externos o corporativos.

A diferencia de DNS Resolver (unbound), dnsmasq no realiza por sí mismo resolución recursiva completa: necesita servidores upstream. La configuración habitual de pfSense Plus utiliza DNS Resolver; DNS Forwarder se habilita cuando lo requiere la arquitectura o se conserva una instalación ya adaptada a él.

44.2. Ventajas, aplicaciones y criterio de elección

Necesidad	Aplicación	Consideración
Resolver nombres internos	Host Overrides	Registro local explícito, una IP por entrada.
Reenviar dominio corporativo	Domain Overrides	Servidor específico y ruta accesible.
Controlar consultas DNS de clientes	Interfaces y reglas PF	La selección de interfaces no sustituye la política del firewall.
Usar caché de DNS externos	Reenvío a upstream	La validez está limitada por TTL de respuestas.
Recursión/DNSSEC/DoT integrados	Evaluar DNS Resolver	El reenviador no reemplaza las funciones de unbound.
DECISIÓN DE SERVICIO DNS Forwarder y DNS Resolver no pueden utilizar simultáneamente el mismo puerto e IP de escucha (habitualmente TCP/UDP 53). Planificar el cambio antes de deshabilitar el DNS que ya utilizan los clientes.		

44.3. Ruta, controles visibles y distribución de la pantalla

El menú Services → DNS Forwarder contiene General DNS Forwarder Options, Host Overrides y Domain Overrides. En la configuración general figuran Enable, Ignore System DNS, opciones de DNS Query Forwarding, Listen Port, Interfaces, Strict binding y Custom options. Las dos tablas inferiores gestionan entradas específicas de host y de dominio.

La presencia de una tabla vacía no permite deducir que el servicio carezca de registros por otros medios. El listado de overrides se usa para administrar las entradas definidas en esta sección. Las columnas y controles concretos del formulario adicional pueden variar según la versión instalada.

44.4. Modelo de funcionamiento: de la consulta a la respuesta

01. Un cliente remite una consulta DNS a una de las direcciones de escucha del firewall y al puerto configurado.
02. dnsmasq comprueba los registros locales y la disponibilidad de una respuesta válida en caché.
03. Si la consulta corresponde a una zona Domain Override, utiliza el destino configurado para dicha zona.
04. En caso contrario reenvía a los servidores DNS generales del sistema, salvo que Ignore System DNS lo impida.
05. El cliente recibe la respuesta, cuya permanencia en caché depende de los valores TTL y del comportamiento del servicio.

44.5. Enable: activar o desactivar DNS Forwarder

Enable DNS forwarder inicia el servicio dnsmasq como punto de consulta. Al desmarcarlo deja de atender consultas dirigidas a ese servicio, por lo que los clientes que dependan del firewall como DNS pueden perder resolución de nombres aunque conserven acceso IP. Es imprescindible verificar el servicio alternativo antes de detenerlo.

Si DNS Resolver está escuchando en la misma IP y puerto, no debe intentarse poner en marcha ambos sin redefinir de forma coherente sus puntos de escucha. La coordinación se realiza en Services → DNS Resolver, Services → DNS Forwarder y en las reglas de acceso.

44.6. Ignore System DNS: exclusión de los servidores globales

Do not use system DNS servers indica a dnsmasq que ignore los DNS configurados en System → General Setup y los que el firewall obtenga por sus interfaces dinámicas. En esta modalidad deben definirse explícitamente servidores ascendentes mediante directivas compatibles como server= dentro de Custom options, cuando se requiera resolver nombres no locales.

Resulta útil si el administrador desea separar los servidores usados por el sistema de los que emplean los clientes a través de dnsmasq. No convierte al reenviador en recursivo; una configuración sin upstream válidos puede impedir que se resuelvan dominios externos.

ADVERTENCIA — FALLO DE RESOLUCIÓN Antes de marcar Ignore System DNS, confirmar que existe una fuente DNS alternativa en Custom options, que es alcanzable por el firewall y que la política de enrutamiento permite enviarle consultas.

44.7. DNS Query Forwarding: estrategia de envío

Este bloque decide cómo se seleccionan los servidores de reenvío y qué peticiones no deben enviarse fuera de la red. Incluye tres opciones independientes: Query DNS servers sequentially, Require domain y Do not forward private reverse lookups. Ninguna de estas casillas sustituye un Host Override, un Domain Override o una regla de firewall.



Figura 44.2. Reenvío simultáneo frente al reenvío secuencial de consultas a DNS upstream.

44.8. Query DNS servers sequentially: paralelo o secuencial

Desmarcado: dnsmasq consulta en paralelo los servidores DNS generales y usa la primera respuesta recibida. Marcado: consulta secuencialmente los servidores en el orden definido en System → General Setup, recurriendo al siguiente cuando el primero no responde según los tiempos de espera del servicio.

La opción secuencial favorece la predictibilidad cuando los servidores ofrecen respuestas distintas, por ejemplo un DNS corporativo frente a uno público, pero puede introducir demoras si el primero no responde. El reenvío paralelo puede favorecer la latencia, pero también devolver una respuesta no deseada si gana el servidor público.

Modo	Ventaja	Riesgo o límite
Paralelo	Menor espera habitual ante varios upstream.	Respuestas inconsistentes si los servidores no son equivalentes.
Secuencial	Orden de precedencia explícito.	Demoras si un servidor prioritario está caído.
Domain Override	Servidor obligatorio para nombres concretos.	Depende de que la ruta y el servidor de ese dominio funcionen.

44.9. Require domain: nombres sin parte de dominio

Require domain impide reenviar peticiones de tipo A o AAAA relativas a nombres simples sin punto, como equipo1, cuando no existe una respuesta local obtenida de hosts o DHCP. En tal caso dnsmasq responde negativamente al cliente en lugar de enviar una consulta al DNS upstream.

Se recomienda cuando los nombres cortos deben resolverse únicamente en la red local y no deben difundirse a resolutores externos. No impide las consultas de nombres completos; para ellas se aplican overrides o upstream general, según corresponda.

44.10. Do not forward private reverse lookups

La opción evita remitir a servidores ascendentes generales consultas PTR de direcciones privadas RFC 1918 cuando el firewall no dispone de una correspondencia local. Puede reducir el ruido de consultas y evitar filtraciones innecesarias de identificadores de la red interna.

Los Host Overrides, las entradas DHCP disponibles y los Domain Overrides explícitos de zonas inversas mantienen su utilidad. Por ejemplo, una zona de tipo in-addr.arpa asociada expresamente a un DNS corporativo puede seguir reenviándose al servidor indicado, aunque esté marcada la opción global.

44.11. Listen Port: puerto DNS de escucha

Listen Port vacío utiliza el puerto DNS convencional 53, tanto UDP como TCP. Puede especificarse un puerto alternativo cuando la arquitectura obliga a mantener otro servicio DNS en el puerto estándar. Los clientes ordinarios no suelen admitir indicar un puerto DNS alternativo mediante DHCP, por lo que esta decisión debe ir acompañada de una solución de encaminamiento de consultas o de una configuración explícita en el cliente.

Comprobar el servicio que tiene vinculado el puerto, las reglas del firewall y el comportamiento de los clientes antes de cambiarlo. El DNS por TCP no es opcional: determinadas respuestas, transferencias operativas o condiciones de tamaño pueden requerirlo.

44.12. Interfaces: direcciones en las que se responde

El selector Interfaces permite responder por All, WAN, LAN, interfaces adicionales disponibles, variantes link-local IPv6 cuando correspondan y Localhost. Por defecto se utilizan las direcciones IPv4 e IPv6 disponibles; al seleccionar interfaces concretas se aceptan consultas dirigidas a sus direcciones y se descartan las dirigidas al resto.

En una red empresarial, limitar el servicio a interfaces internas que realmente necesitan DNS. Seleccionar WAN indiscriminadamente podría exponerlo a consultas desde redes no confiables si existen reglas permisivas. La elección de LAN no autoriza automáticamente el tráfico: deben existir reglas compatibles en el firewall.

Selección conceptual	Uso típico	Precaución
LAN interna	Dar DNS a clientes locales.	Comprobar TCP/UDP 53 y DHCP.
Localhost	Consultas del propio firewall.	Verificar el modo de resolución del sistema.
WAN	Solo diseños expresamente justificados.	Evitar exponer un resolutor abierto.
Direcciones IPv6	Servicios para clientes IPv6.	No habilitar Strict binding si requiere IPv6.
All	Laboratorios o redes controladas.	Superficie de exposición mayor.

44.13. Strict binding: vinculación estricta a interfaces

Strict interface binding obliga a dnsmasq a asociarse únicamente con las interfaces que contienen las direcciones seleccionadas, en lugar de vincularse ampliamente y descartar consultas a direcciones no elegidas. Puede ayudar a convivir con otros servicios DNS cuando se distribuyen IP y puertos de manera deliberada.

Advertencia técnica de Netgate: Strict binding no funciona con IPv6. Si se activa, dnsmasq no escucha en direcciones IPv6. Para instalaciones dual stack es preferible estudiar otras formas de segregación antes de usar esta opción.

COMPATIBILIDAD IPv6 Marcar Strict binding en un entorno que utiliza DNS por IPv6 puede cortar la resolución de los clientes IPv6, aunque IPv4 continúe respondiendo. Verificar ambas familias tras aplicar el cambio.

44.14. Custom options: directivas de dnsmasq

Custom options admite parámetros adicionales de dnsmasq separados por espacios o saltos de línea. Deben corresponder a directivas admitidas por la versión incorporada en pfSense Plus. Un error de sintaxis, una directiva incompatible o una configuración contradictoria puede impedir el inicio del servicio.

Ejemplo ilustrativo	Efecto esperado	Precaución
server=198.51.100.53	Define un DNS upstream de ejemplo reservado para documentación.	Solo usar una IP de servidor real en la configuración operativa.
max-ttl=30	Establece un límite de TTL en segundos para ciertas respuestas.	Un TTL demasiado corto incrementa consultas.
address=/lab.example.com/ 192.0.2.25	Respuesta local de ejemplo para subdominio indicado.	No usar como control de acceso o filtrado único.

Las líneas precedentes son muestras de sintaxis didáctica con direcciones y dominios reservados para documentación; no son instrucciones para pegar sin adaptación en un sistema de producción. Guardar cambios controlados, comprobar la sintaxis y disponer de una reversión preparada.

44.15. Relación con System → General Setup

El DNS Forwarder toma sus resolutores generales de System → General Setup y, dependiendo de la política configurada, también puede recibir servidores dinámicos de conexiones WAN. La opción DNS

Server Override de los ajustes del sistema decide si pueden incorporarse servidores enviados por proveedores externos. Ignore System DNS, por el contrario, pertenece al propio reenviador y altera las fuentes ascendentes que utiliza dnsmasq.

Es esencial distinguir DNS usado por el propio pfSense de DNS ofrecido a clientes a través del firewall. DNS Resolution Behavior determina cómo resuelve nombres el propio sistema y no equivale automáticamente a los servidores que escucha dnsmasq ni a los anunciados por DHCP.

44.16. Host Overrides: finalidad y límites

Host Overrides crea respuestas DNS locales que prevalecen para los nombres definidos. Permite publicar un servidor interno con un nombre conocido sin que la solicitud tenga que resolverse en Internet. Resulta especialmente útil para split DNS, nombres internos simples y servicios que necesitan distinguir una dirección interna de su dirección pública.

Según la documentación de Netgate, cada entrada Host Override del DNS Forwarder admite una única dirección IP. No debe trasladarse de manera literal el comportamiento del DNS Resolver cuando se requieren varios registros A/AAAA para un mismo nombre.

44.17. Host Overrides: campos del formulario Add/Edit

Campo	Función	Buenas prácticas
Host	Etiqueta del host, sin el dominio. Puede quedar vacía para la raíz de la zona.	Utilizar nombres estables.
Domain	Dominio asociado al host.	Preferir dominio administrado o home.arpa para uso interno.
IP Address	Dirección IPv4 o IPv6 que se devolverá al consultar el nombre.	Una dirección por entrada en dnsmasq.
Description	Texto administrativo de identificación.	Explicar servicio y motivo, sin secretos.
Additional Names for This Host	Nombres adicionales que comparten la dirección, si están disponibles.	Evitar alias ambiguos o duplicados.

Los campos del formulario de alta se documentan desde la referencia oficial de Netgate; no forman parte del listado vacío mostrado en la pantalla principal. Su disponibilidad exacta puede variar según la versión y la configuración del servicio.

44.18. Host Overrides: ejemplo didáctico de resolución local

Ejemplo neutro: el nombre portal.lab.example.com puede resolverse a 192.0.2.25 únicamente desde los clientes que consulten al DNS Forwarder. Es una dirección reservada para documentación, no una IP asignable a la infraestructura real. Un servicio publicado mediante otra dirección en Internet puede presentar una respuesta diferente, realizando split DNS.

01. Abrir Services → DNS Forwarder y localizar Host Overrides.
02. Elegir Add y completar Host y Domain con un nombre no utilizado por otra política.
03. Especificar una dirección IP autorizada, guardar y aplicar los cambios si la interfaz lo solicita.
04. Desde un cliente que use el DNS del firewall, consultar el FQDN y comprobar la dirección devuelta.
05. Comprobar conectividad al servicio de aplicación, no solo resolución del nombre.

44.19. Host Overrides: restricciones y errores habituales

Un Host Override no autoriza por sí mismo el acceso al servidor ni crea una regla de firewall. La respuesta DNS puede ser correcta y el servicio estar bloqueado por routing, reglas o NAT. También pueden aparecer resultados antiguos mientras persistan en cachés de clientes o servidores intermedios.

Evitar duplicar nombres internos en múltiples sistemas sin una política clara. La ausencia de respuesta en un cliente remoto puede deberse a que emplea otro DNS, usa DoH/DoT del navegador o no está autorizado a consultar al firewall.

44.20. Domain Overrides: finalidad y arquitectura

Domain Overrides dirige las consultas de un dominio concreto hacia servidores DNS distintos de los generales. Por ejemplo, cuando una sede tiene un DNS corporativo que conoce nombres internos, se puede reenviar solo esa zona y seguir usando otro DNS upstream para las demás consultas. El tráfico DNS hacia ese servidor puede requerir una VPN, rutas o reglas de paso específicas.

Es una selección por nombre de dominio; no equivale a añadir un registro A. Una zona delegada a un servidor remoto puede devolver múltiples tipos de registros conforme a la configuración de ese servidor.

44.21. Domain Overrides: campos del formulario Add/Edit

Campo	Comportamiento	Observación
Domain	Nombre de dominio cuyas consultas se derivan.	Definir el sufijo más específico necesario.
IP Address	Servidor DNS destino o marcadores especiales # y !.	Los marcadores alteran el reenvío, no representan IP.
Source IP	Dirección origen opcional para enviar la consulta.	Útil para un DNS remoto accesible por VPN.
Description	Referencia administrativa del override.	Describir dependencia y destino sin identificadores sensibles.

La documentación de Netgate identifica los comportamientos especiales del campo IP Address y la selección de Source IP. No debe interpretarse que un Domain Override cambia el gateway del firewall o concede permiso automático para alcanzar ese servidor.

44.22. Domain Overrides: significado de # y !

Valor de IP Address	Qué indica	Ejemplo de uso conceptual
Dirección IP	Enviar consultas del dominio al DNS señalado.	Zona interna mantenida por un DNS central.
#	Excepción que vuelve al reenvío DNS general en una subzona.	Una subzona que no debe seguir el override padre.
!	No reenviar consultas externas para la zona.	Responder solo con registros que se conozcan localmente.

Estos símbolos son directivas especiales documentadas para Domain Overrides del DNS Forwarder. No son un comodín de búsqueda en el nombre de dominio ni una ruta. La política resultante se debe validar expresamente con consultas de nombres existentes e inexistentes.

44.23. Domain Overrides: Source IP y servidores en VPN

Source IP puede fijar la dirección local desde la que el firewall consulta al servidor DNS remoto. Es relevante cuando el túnel VPN o el servidor remoto solo admite tráfico con determinadas direcciones de origen. Elegir una dirección que exista realmente en el firewall y cuya ruta de retorno esté definida; no utilizar arbitrariamente una IP que pertenezca a un cliente.

Verificar tanto el envío como la respuesta: una regla VPN permisiva en un extremo no soluciona una ruta de retorno ausente en el otro. Añadir rutas estáticas o políticas solo cuando la arquitectura las requiera.

44.24. Comparativa entre Host Overrides y Domain Overrides

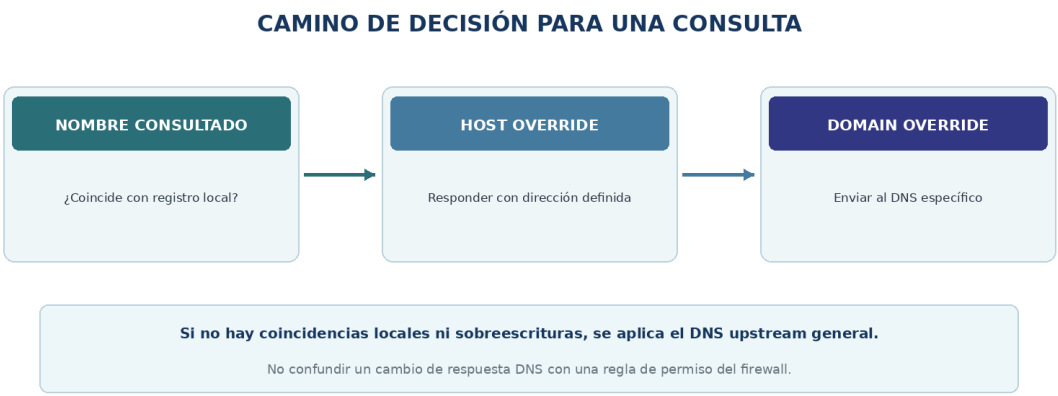


Figura 44.3. Criterio conceptual para resolver nombres locales y reenviar dominios concretos.

Característica	Host Override	Domain Override
Unidad de gestión	Nombre completo concreto	Zona o sufijo de dominio
Resultado	Dirección definida localmente	Respuesta del servidor DNS designado
Uso habitual	Portal interno, aplicación local	Directorio corporativo, DNS de otra sede
Depende de servidor DNS remoto	No para su registro local	Sí si requiere un destino upstream
Afecta a reglas de firewall	No las crea	No las crea

44.25. Vistas de las tablas y acciones administrativas

Las secciones Host Overrides y Domain Overrides agrupan las entradas existentes. Según el formato de la versión, las filas pueden mostrar nombre, dominio, destino, descripción y acciones de edición o borrado, y botones Add en cada sección. La operación de guardar puede requerir Apply Changes para cargar la nueva configuración en dnsmasq.

Antes de eliminar una entrada, comprobar si otras aplicaciones, equipos, VPN o reglas dependen de ese nombre. Una eliminación puede no ser perceptible hasta que expiren las respuestas retenidas en caché.

44.26. Procedimiento de puesta en marcha inicial

01. Registrar la configuración DNS anterior y verificar que existe una copia restaurable del firewall.
02. Decidir si se conservará DNS Resolver, se migrará a Forwarder o se distribuirán en IP/puertos distintos.
03. Revisar los DNS generales y el modo de resolución del propio firewall en System → General Setup.
04. Activar DNS Forwarder únicamente después de resolver conflictos de escucha y configurar Interfaces de confianza.
05. Comprobar que la política del firewall permite DNS desde los segmentos autorizados y deniega consultas externas no previstas.
06. Guardar, aplicar y comprobar A, AAAA y PTR desde equipos de prueba de las redes necesarias.

44.27. Procedimiento de migración DNS Resolver → DNS Forwarder

01. Inventariar Host Overrides, Domain Overrides, ACL, DNSSEC, DoT y cualquier función avanzada del DNS Resolver en uso.
02. Confirmar si esas capacidades pueden sustituirse o si la migración no es adecuada.
03. Establecer upstream, interfaces y reglas del Forwarder, sin crear conflicto de puerto con unbound.
04. Programar el cambio, detener o trasladar el Resolver y habilitar dnsmasq con un punto de retorno documentado.

05. Desde clientes IPv4 e IPv6, verificar resolución pública, interna y por VPN.
06. Ante fallos, recuperar el servicio anterior y su puerto de escucha.

CAMBIO CRÍTICO DE SERVICIO No deshabilitar unbound simplemente para activar dnsmasq sin verificar qué clientes utilizan el firewall como DNS, qué reglas dependen de nombres internos y qué servicios requieren DNSSEC o DNS over TLS.

44.28. Procedimiento de reenvío selectivo a DNS corporativo

01. Verificar que existe una ruta funcional desde el firewall hasta el servidor DNS corporativo.
02. Crear un Domain Override para el dominio interno correspondiente.
03. Configurar Source IP solo si el túnel, la ruta o el servidor lo requieren.
04. Aplicar cambios y consultar un nombre conocido de esa zona a través del DNS Forwarder.
05. Consultar un dominio público diferente para confirmar que el upstream general sigue operando.
06. Validar PTR de redes privadas si la arquitectura requiere zonas inversas corporativas.

44.29. Procedimiento de DNS local para servicios internos

01. Definir el nombre completo de un servicio y verificar que no exista duplicado en un DNS autoritativo.
02. Crear Host Override con una única dirección IP de destino.
03. Guardar, aplicar, y realizar la resolución desde un cliente con DNS apuntando al firewall.
04. Comprobar que el servidor de aplicación es accesible y que su certificado corresponde al nombre si se usa HTTPS.
05. Registrar el propietario operativo y la dependencia del registro en el inventario de servicios.

44.30. Procedimiento para cambiar el puerto de escucha

El uso de un Listen Port alternativo puede facilitar pruebas o convivencia con otros motores, pero los clientes DNS que solo conocen el puerto estándar necesitan un intermediario adicional o una configuración específica. El cambio de puerto no equivale a abrir el servicio a Internet y debe respetar el direccionamiento IP de escucha.

01. Identificar el servicio y el puerto ocupados actualmente.
02. Seleccionar puerto alternativo para DNS Forwarder cuando el diseño lo justifique.
03. Guardar y aplicar cambios sin desconectar el único mecanismo DNS operativo.
04. Probar con una herramienta capaz de especificar puerto, como dig -p, desde un origen autorizado.
05. Actualizar o revertir las reglas de redirección o el consumidor que debía utilizar ese puerto.

44.31. IPv6 y funcionamiento dual stack

El DNS Forwarder puede responder consultas de tipos A y AAAA, y escuchar en direcciones IPv4 e IPv6 según las interfaces seleccionadas. Una consulta AAAA no exige por sí misma transporte IPv6, pero un cliente que solo tiene acceso IPv6 a su servidor DNS necesita que el demonio escuche por IPv6 y que las reglas lo permitan.

Evitar Strict binding si se necesita DNS por IPv6. Comprobar accesibilidad IPv6 del servidor DNS y distinguirla de la obtención de direcciones IPv6 mediante RA y DHCPv6. El envío de un DNS a clientes puede depender de DHCPv6, RA (RDNSS) o configuración manual.

44.32. Relación con DHCP y registro de nombres

Según la versión y el backend de DHCP, existen diferencias en cómo se registran dinámicamente los nombres de los clientes. La documentación general de DNS Forwarder describe opciones DHCP Registration, Static DHCP y Prefer DHCP, pero estas no figuran en la lista de controles que se está documentando aquí y pueden no estar disponibles o no comportarse igual con Kea.

No dar por supuesto que un nombre DHCP aparecerá en dnsmasq por el mero hecho de habilitar DNS Registration dentro de Kea. En las implementaciones actuales, las funciones de registro de Kea se orientan a DNS Resolver; la interoperabilidad concreta debe validarse para la versión instalada.

44.33. Seguridad: evitar un servicio DNS abierto

Exponer un DNS recursivo o reenviador a redes no confiables puede facilitar abuso, reconocimiento o amplificación de tráfico. Limitar Interfaces a zonas internas, mantener reglas de acceso por origen, inspeccionar conexiones inesperadas y evitar abrir indiscriminadamente UDP/TCP 53 en WAN.

Las funciones de DNS Query Forwarding y los overrides controlan respuestas y destinos DNS, no autentican clientes ni bloquean todas las vías de resolución externa. Navegadores y sistemas pueden emplear DNS over HTTPS o TLS hacia otros destinos, por lo que las políticas corporativas requieren controles complementarios.

44.34. Seguridad: privacidad, integridad y registros

Al consultar DNS upstream, nombres de aplicaciones, servidores y dominios pueden salir a un tercero. Elegir destinos de confianza y documentar políticas de privacidad. Si la integridad criptográfica de las respuestas o el cifrado del transporte son requisitos, evaluar DNS Resolver y sus capacidades DNSSEC/DNS over TLS en lugar de atribuirlas automáticamente a dnsmasq.

Registrar solo lo necesario para el diagnóstico, con retención limitada y acceso restringido. No copiar volúmenes completos de consultas, nombres internos o direcciones de clientes a documentación pública.

44.35. Rendimiento: caché, TTL y latencia

La caché disminuye el tráfico repetitivo, pero durante un cambio DNS puede mantener respuestas anteriores hasta que expire el TTL. Consultar siempre la ruta de prueba concreta: equipo cliente, DNS Forwarder y servidor ascendente. El reenvío paralelo suele reducir espera; el secuencial favorece una precedencia más estable a costa de posibles timeouts.

Usar opciones personalizadas para TTL o tamaño de caché solo con mediciones y necesidades justificadas. Un TTL demasiado bajo aumenta las solicitudes; uno demasiado alto puede retrasar cambios de servicio o la recuperación tras failover.

44.36. Pruebas desde clientes: A, AAAA y PTR

Prueba	Comando o acción	Qué se verifica
Nombre IPv4	nslookup portal.lab.example.com <DNS-de-prueba>	Host Override: respuesta A prevista.
Nombre IPv6	dig @<DNS-de-prueba> AAAA example.com	Respuesta AAAA con la política correspondiente.
Inversa	dig @<DNS-de-prueba> -x <IP-de-prueba>	PTR local o encaminado correctamente.
Puerto alternativo	dig @<DNS-de-prueba> -p 5353 example.com	Servicio responde en puerto establecido.
Dominio corporativo	dig @<DNS-de-prueba> host.lab.example.com	Domain Override y ruta del servidor remoto.

Las expresiones entre signos angulares de la tabla son marcadores didácticos, no comandos para ejecutar literalmente. Las comprobaciones deben realizarse desde clientes y servidores de prueba autorizados. No se incluyen direcciones ni nombres reales de instalaciones.

44.37. Verificación desde pfSense Plus

01. Abrir Diagnostics → DNS Lookup y comprobar que el firewall puede consultar el dominio requerido.
02. Revisar Status → Services y confirmar que dnsmasq está iniciado y sin reinicios continuos.
03. Comprobar la configuración de System → General Setup para detectar DNS upstream ausentes o modificados por una WAN.
04. Usar Diagnostics → Packet Capture en una interfaz apropiada si se sospecha de ausencia de peticiones o respuestas.
05. Consultar reglas y estados para verificar el acceso UDP/TCP 53 entre clientes y firewall, y entre firewall y servidores externos.

La herramienta Diagnostics → DNS Lookup puede reflejar la política de resolución propia del sistema, que no siempre coincide con la de los clientes dirigidos explícitamente al Forwarder. Por ello es imprescindible comprobar también desde clientes reales de pruebas.

44.38. Limpiar cachés y distinguir errores persistentes

Netgate indica que reiniciar dnsmasq en Status → Services limpia la caché del DNS Forwarder. Las cachés del sistema operativo, aplicaciones y navegadores de los clientes pueden persistir, por lo que un resultado antiguo no demuestra por sí mismo que pfSense no haya aplicado un cambio.

Para diagnosticar, comparar respuestas contra el DNS Forwarder, contra el DNS ascendente y contra la caché local del cliente. Evitar reinicios innecesarios en producción si el problema puede aislarse primero con una consulta nueva.

44.39. Diagnóstico: incidencias frecuentes

Síntoma	Causa probable	Comprobación / corrección
dnsmasq no inicia	Puerto 53 ocupado o directiva incompatible.	Revisar servicios y Custom options.
Falla DNS externo	Ignore System DNS sin upstream válido.	Verificar server=, rutas y servidor.
Un host local no resuelve	FQDN mal definido u otro DNS en cliente.	Consultar con DNS explícito y revisar Host Overrides.
No responde IPv6	Strict binding activo.	Desactivar o rediseñar la escucha por IPv6.
Nombres remotos fallan	Domain Override o VPN sin rutas.	Verificar Source IP, reglas y retorno.
Respuestas inesperadas	Upstream paralelos incoherentes.	Establecer override o revisar modo secuencial.
Persisten IP antiguas	Cachés y TTL.	Comparar origen de consulta y renovar cachés.

44.40. Riesgos de cambios y estrategia de reversión

Los cambios de DNS pueden producir interrupciones de aplicaciones aunque las conexiones IP sigan operativas. Antes de modificar Enable, Listen Port, Interfaces, Strict binding, servidores upstream u overrides, registrar dependencias, obtener backup y acordar una ventana adecuada cuando el DNS presta servicio a múltiples redes.

01. Guardar una copia de la configuración anterior y anotar cuál era el DNS activo y dónde escuchaba.
02. Introducir una modificación por vez, priorizando un conjunto pequeño de clientes de validación.
03. Realizar pruebas internas, externas, IPv4, IPv6 y por VPN según el diseño.
04. Ante fallos, revertir el último cambio y restaurar el puerto e interfaces anteriores.
05. Confirmar el restablecimiento de resolución de nombres y actualizar el registro de cambio.

44.41. Matriz de aceptación para operación

Control de calidad	Resultado esperado	Si no se cumple
Servicio y puerto	Un servicio DNS escucha en IP/puerto previstos.	Corregir conflicto DNS Resolver / Forwarder.
Clientes autorizados	Responden únicamente redes y equipos previstos.	Limitar Interfaces y reglas PF.
Nombres locales	Host Overrides resuelven nombre correcto.	Revisar FQDN y cachés.
Zonas remotas	Domain Overrides responden por la ruta deseada.	Revisar DNS upstream, VPN y Source IP.
Nombres externos	Consulta pública responde con latencia aceptable.	Revisar upstream y Ignore System DNS.

Control de calidad	Resultado esperado	Si no se cumple
Dual stack	IPv4 e IPv6 funcionan cuando se requieren.	Revisar Strict binding e interfaces.
Plan de retorno	Restauración de servicio validada.	Ensayar antes de cambio crítico.

44.42. Buenas prácticas para administradores

- Utilizar DNS Resolver cuando se requieran funciones avanzadas de validación y cifrado no proporcionadas directamente por dnsmasq.
- No utilizar resolutores DNS públicos e internos intercambiables si sus zonas y respuestas difieren.
- Separar cambios de registros locales de cambios estructurales de puerto, interfaz o servidor upstream.
- Documentar cada Host Override y Domain Override con una finalidad operativa; eliminar dependencias obsoletas.
- Verificar siempre desde IPv4 e IPv6 cuando la organización utiliza ambas familias de direcciones.
- Conservar un procedimiento de recuperación accesible aun cuando el propio servicio DNS esté interrumpido.

44.43. Glosario operativo

Término	Definición
DNS Forwarder	Servicio que reenvía consultas y almacena respuestas DNS en caché.
dnsmasq	Demonio utilizado por el reenviador de pfSense Plus.
Upstream DNS	Servidor al que el reenviador envía consultas no resueltas localmente.
Host Override	Registro local de nombre a dirección.
Domain Override	Regla de reenvío para nombres de una zona.
PTR	Registro DNS que relaciona dirección IP con nombre en resolución inversa.
TTL	Tiempo de validez de una respuesta DNS en caché.
Split DNS	Respuestas diferentes para un mismo nombre según el punto de consulta.
FQDN	Nombre completo de host y dominio.
Dual stack	Disponibilidad simultánea de IPv4 e IPv6.

44.44. Fuentes y referencias oficiales de Netgate

- Netgate — DNS Forwarder
- Netgate — DNS Forwarder Configuration
- Netgate — Host Overrides / Domain Overrides
- Netgate — DNS Resolver
- Netgate — System General Setup: DNS
- Netgate — Troubleshooting DNS Resolution
- Netgate — Troubleshooting the DNS Cache
- Netgate — Split DNS / NAT Reflection
- Netgate — Wildcard Records DNS Forwarder/Resolver

45 Services → DNS Resolver

Unbound · General Settings · Advanced Settings · Access Lists

Ruta de administración: Services → DNS Resolver. Estudio técnico de las opciones generales, ajustes avanzados, políticas de acceso y resolución local de nombres en pfSense Plus, con procedimientos reproducibles, verificación y recomendaciones de operación segura.

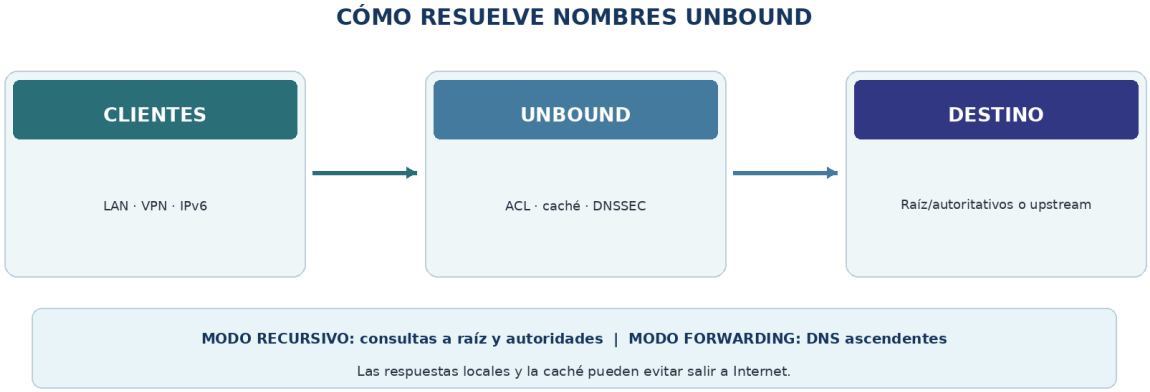


Figura 45.1. Esquema de clientes, Unbound y dos modalidades de resolución DNS.

45.1. Finalidad, alcance y arquitectura de DNS Resolver

DNS Resolver utiliza Unbound: resolutor recursivo y validador DNS con caché, soporte para DNSSEC, resolución local, reglas de acceso y posibilidad de reenviar consultas a servidores ascendentes. Es el servicio DNS predeterminado en las versiones actuales de pfSense. No debe confundirse con DNS Forwarder, basado en dnsmasq, ni con la configuración de DNS que utilizan los clientes por DHCP.

Este capítulo cubre las tres pestañas de la interfaz: General Settings, Advanced Settings y Access Lists. Asimismo se documentan Host Overrides y Domain Overrides integrados en General Settings, a partir de la referencia oficial de Netgate. Los valores disponibles pueden variar por revisión de pfSense Plus; se distingue en cada caso la función mostrada en el material y la información complementaria procedente de la documentación.

45.2. Cuándo conviene implantar Unbound

Necesidad	Configuración sugerida	Dependencia
Resolver consultas locales	Unbound habilitado en LAN/Localhost	ACL y reglas DNS de clientes
Validar respuestas externas	DNSSEC en modo recursivo	Hora NTP y conectividad DNS
Cifrar consultas ascendentes	Forwarding Mode + DoT saliente	Servidores upstream con 853/TCP y certificados válidos
Nombres internos / Split DNS	Host Overrides / Domain Overrides	Coherencia con el DNS corporativo
Redes VPN e IPv6	Interfaces de escucha y ACL específicas	Reglas y rutas apropiadas
Clientes IPv6-only	DNS64 combinado con NAT64	Traductor y prefijo apropiados

45.3. Recorrido de la pantalla y controles de navegación

Las pestañas de configuración son General Settings, Advanced Settings y Access Lists. General Settings administra escucha, recursión/reenvío, DNSSEC, DoT y sobrescrituras de nombres. Advanced Settings concentra privacidad, memoria, tiempos, protección y registros. Access Lists define la autorización de clientes por redes de origen. Los botones de aplicación y gestión del servicio pueden cambiar con la versión; Save almacena los cambios y la GUI puede exigir Apply Changes para activarlos.

45.4. Resolución recursiva frente a DNS Query Forwarding

En modo recursivo, Unbound recorre la jerarquía DNS desde servidores raíz hasta los autoritativos, y utiliza la caché para respuestas repetidas. No depende de la lista de DNS de System → General Setup. Con Enable Forwarding Mode, remite la consulta a resolutores configurados en System → General Setup o recibidos en interfaces dinámicas, de acuerdo con la política DNS del sistema.

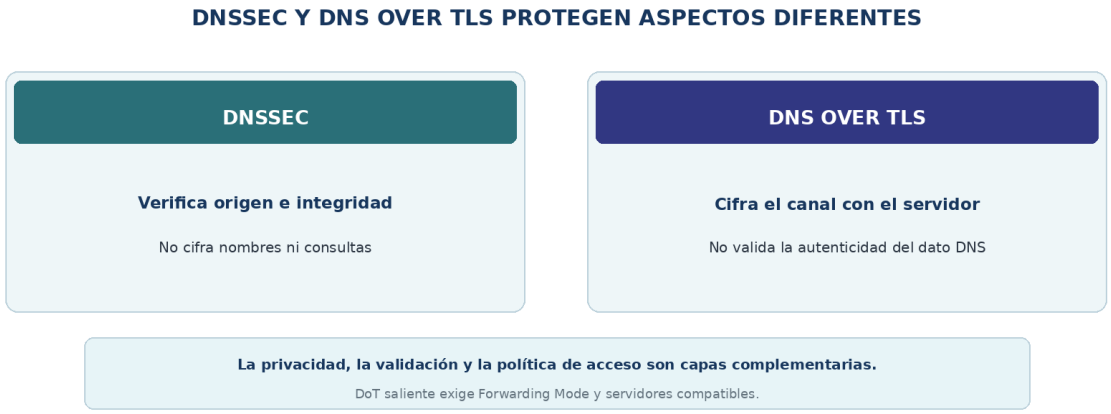


Figura 45.2. DNSSEC verifica respuestas; DNS over TLS protege la conexión con un servidor.

MULTI-WAN La recursión utiliza el encaminamiento del firewall y depende de la ruta de salida disponible; en modo forwarding pueden asociarse pasarelas a DNS ascendentes. No suponer que elegir varias interfaces de salida equivale a una conmutación automática de DNS.

45.5. Enable: activación del servicio

Enable DNS resolver inicia o detiene Unbound. Desactivarlo puede dejar sin DNS a los clientes que consultan la dirección del firewall, y afectar a servicios que resuelven nombres en el propio equipo. Antes de deshabilitarlo, inventariar clientes, DHCP y dependencias de certificados, VPN y actualizaciones.

No se pueden ejecutar DNS Resolver y DNS Forwarder escuchando simultáneamente en la misma dirección y puerto, normalmente TCP/UDP 53. Una convivencia requiere IP/puertos diferenciados y política expresa.

45.6. Listen Port y Enable SSL/TLS Service

Campo	Qué hace	Criterio profesional
Listen Port	Puerto de escucha DNS convencional TCP/UDP; vacío emplea el 53.	No cambiar salvo necesidad documentada; clientes DNS estándar esperan 53.
Enable SSL/TLS Service	Atiende consultas entrantes de clientes compatibles con DNS over TLS.	Exigir certificado y acceso limitado a clientes autorizados.
SSL/TLS Listen Port	Puerto para DoT entrante; vacío utiliza normalmente 853.	Comprobar transporte TCP 853, reglas y ausencia de conflictos.
SSL/TLS Certificate	Certificado de servidor para validar identidad en sesiones DoT.	Nombre, vigencia, CA de confianza y cadena correctos.

Activar DoT entrante modifica el comportamiento automático de encaminamiento de respuestas por interfaz, por lo que Netgate recomienda seleccionar de forma expresa las interfaces de escucha. DNSSEC y DoT no son equivalentes: DNSSEC protege autenticidad e integridad del dato, y TLS cifra la comunicación con el siguiente servidor.

45.7. Network Interfaces y Outgoing Network Interfaces

Network Interfaces especifica las direcciones en que Unbound atiende consultas. All usa las interfaces IPv4 e IPv6 disponibles; limitar a LAN y Localhost reduce superficie de exposición. Si se elige una interfaz con ambas familias, Unbound puede escuchar en ambas. Las consultas a otras direcciones no seleccionadas se descartan.

Outgoing Network Interfaces acota las interfaces desde las que Unbound origina consultas hacia servidores externos. No modifica las reglas del firewall ni sustituye el encaminamiento. La lista puede incluir enlaces WAN, direcciones link-local o localhost cuando la GUI lo ofrece; deben seleccionarse solo orígenes coherentes con el camino de red deseado.

Caso	Network Interfaces	Outgoing Interfaces
Clientes internos y una WAN	LAN + Localhost	All o WAN según enrutamiento
Dos WAN y modo forwarding	LAN + Localhost	Selección coherente con pasarelas DNS
Servicio aislado solo local	Localhost	Conectividad externa necesaria si resuelve Internet
Recursión desde Internet	No recomendado	No habilitar ACL abierta

45.8. Strict Outgoing Network Interface Binding

Con esta casilla activada, Unbound rechaza la resolución recursiva cuando ninguna de las interfaces de salida seleccionadas se encuentra disponible. Desactivada, el servicio puede utilizar otras interfaces disponibles si desaparecen las elegidas. Es una decisión entre política estricta de salida y continuidad del servicio: en redes con respaldo conviene ensayar explícitamente la pérdida de una WAN.

RIESGO DE CONTINUIDAD Una selección demasiado restrictiva puede producir fallos DNS aunque haya salida a Internet por otra WAN. Verificar disponibilidad, ruta, DNS upstream y respuesta desde cliente y firewall.

45.9. System Domain Local Zone Type: significado completo

Define cómo responde Unbound a consultas del dominio del sistema sin coincidencia en datos locales. En todos los tipos, las coincidencias locales se contestan conforme al registro disponible; la diferencia se encuentra en lo que ocurre con nombres o tipos no presentes.

Modo	Comportamiento si no hay respuesta local
Deny	Descarta sin responder.
Refuse	Devuelve código REFUSED.
Static	Devuelve NODATA o NXDOMAIN según consulta.
Transparent	Consulta normalmente si no existe el nombre local; por nombre local con otro tipo, NOERROR/NODATA.
Type Transparent	Permite reconsultar externamente también si coincide el nombre, pero no el tipo.
Redirect	Redirige respuestas de subdominios bajo la zona local según sus datos.
Inform	Resuelve normalmente y registra la consulta.
Inform Deny	Deniega y registra.
No Default	Elimina contenido predeterminado de la zona sin modificar de forma automática el comportamiento general.

Transparent es la opción predeterminada documentada. No elegir Static, Deny o Redirect sin inventariar subdominios, registros dinámicos y posibles nombres externos que compartan el sufijo.

45.10. DNSSEC: validación de respuestas

Enable DNSSEC Support activa validación criptográfica de datos firmados con DNSSEC. Permite identificar respuestas alteradas o inconsistentes con la cadena de confianza; no oculta nombres ni cifra peticiones. Su uso requiere fecha/hora correcta, tránsito DNS adecuado y ausencia de manipulación por equipos intermedios.

En Forwarding Mode la interacción con DNSSEC depende de la capacidad y el comportamiento del resolutor upstream. La documentación de Netgate recomienda especial cautela y, para determinadas configuraciones Multi-WAN con DNS forwarding, desactivarlo conforme a su procedimiento. No deshabilitar la validación globalmente como remedio permanente sin identificar el problema.

45.11. Python Module y controles adicionales del script

Enable Python Module incorpora un módulo Python de Unbound capaz de inspeccionar o alterar el tratamiento de consultas y respuestas. La documentación describe opciones condicionales Python Module Order (Pre Validator / Post Validator, con efecto cuando DNSSEC está habilitado) y Python Module Script, cuyo archivo debe residir en /var/unbound/ y terminar en .py.

Solo se justifica para políticas personalizadas mantenidas y auditadas. Un script defectuoso puede degradar o interrumpir el DNS. En el escenario descrito solo se observa el selector de activación: orden y ruta de script proceden de la documentación complementaria, no de una captura del formulario desplegado.

45.12. DNS Query Forwarding y DoT saliente

Enable Forwarding Mode sustituye la resolución recursiva directa por consultas a DNS ascendentes. Use SSL/TLS for outgoing DNS Queries to Forwarding Servers cifra esas consultas sobre el puerto 853 y exige Forwarding Mode activado. Todos los resolutores upstream empleados deben aceptar DoT, estar alcanzables y presentar certificados válidos para el nombre configurado cuando corresponda.

01. Definir resolutores con dirección y nombre de validación en System → General Setup.
02. Configurar sus pasarelas de salida cuando hay varias WAN y el diseño lo requiere.
03. Activar Enable Forwarding Mode y, si procede, DoT saliente.
04. Guardar, aplicar y verificar TCP 853 a los ascendentes.
05. Consultar un nombre externo, uno interno y una respuesta DNSSEC válida e inválida con un cliente de prueba.

ADVERTENCIA DE CIFRADO No marcar DoT saliente si alguno de los servidores configurados no soporta TLS en 853: la resolución puede quedar interrumpida. No confundir habilitar un servidor DoT local con cifrar las consultas hacia Internet.

45.13. OpenVPN Clients y registro de nombres

Register connected OpenVPN clients in the DNS Resolver registra nombres comunes de determinados clientes conectados a servidores OpenVPN compatibles, normalmente en modo tun con autenticación configurada según la documentación. El nombre se combina con el dominio del sistema. No implica que todo túnel VPN registre automáticamente sus equipos ni sustituye la resolución de un dominio remoto corporativo.

Los registros DNS aprendidos por DHCP pueden estar condicionados por el backend, la versión y sus ajustes. Verificar las opciones de DNS Registration del servidor DHCP y evitar duplicados con Host Overrides.

45.14. Display Custom Options y directivas manuales de Unbound

Display Custom Options expone directivas avanzadas que no disponen de control en la GUI. Solo utilizar parámetros compatibles con la versión de Unbound incluida y mantenerlos documentados; una sintaxis inválida puede impedir iniciar el servicio. Netgate señala que ciertas directivas requieren un encabezado server: para su correcta interpretación.

No se reproducen aquí fragmentos procedentes del firewall real. Los cambios manuales deben validarse en entorno controlado, anotando propósito, valor anterior y procedimiento de reversión.

45.15. Host Overrides: resolución interna y Split DNS

Host Overrides define registros locales que prevalecen frente al proceso ordinario de resolución. El formulario oficial incorpora Host, Domain, IP Address, Description y Additional Names for This Host. A diferencia del reenviador dnsmasq, el Resolver puede admitir varias direcciones para un mismo nombre, permitiendo respuestas A y AAAA.

01. Crear una entrada para un nombre de laboratorio bajo lab.example.com.
02. Asignar una dirección de documentación, por ejemplo 192.0.2.20, únicamente como ejemplo conceptual.
03. Guardar y aplicar cambios.

04. Consultar el FQDN desde un cliente cuyo DNS sea el firewall.
05. Comprobar además que la ruta y el servicio de destino funcionan: el override no crea reglas de acceso.

45.16. Domain Overrides: delegación a otro servidor DNS

Domain Overrides envía consultas de una zona específica al servidor indicado en IP Address. El formulario documentado incluye Domain, IP Address, TLS Queries, TLS Hostname y Description. Puede usarse un puerto no estándar con la notación IP@puerto. Si hay varios resolutores de una misma zona, se crean entradas independientes para el mismo dominio. Deben existir rutas y reglas compatibles, especialmente si el destino es accesible a través de VPN.

Un Domain Override no convierte a Unbound en autoritativo de esa zona. Se limita a dirigir la consulta al DNS que posee los registros deseados; tampoco representa por sí solo una política de filtrado robusta.

45.17. Advanced Privacy: Hide Identity y Hide Version

Opción	Activada	Desactivada
Hide Identity	Rechaza las consultas id.server y hostname.bind.	Puede responder con información identificativa del servidor.
Hide Version	Rechaza version.server y version.bind.	Puede revelar la versión del resolutor.

Se aconseja evitar revelar información innecesaria. Estas medidas complementan la limitación de redes de consulta y el mantenimiento del sistema, pero no reemplazan controles de acceso.

45.18. Query Name Minimization y Strict Query Name Minimization

Query Name Minimization reduce la cantidad de etiquetas de nombre enviadas a los servidores ascendentes y, cuando es posible, consulta inicialmente el tipo A. En modalidad normal es una técnica de mejor esfuerzo que conserva compatibilidad con autoridades que no siguen el comportamiento esperado. Strict Query Name Minimization prohíbe el retroceso al nombre completo y puede provocar fallos de resolución en numerosos dominios.

La documentación de Netgate describe QNAME Minimization como desactivado de forma predeterminada. Comprobar el valor efectivo del sistema: puede proceder de una configuración anterior o de cambios de versión. Strict solo tiene efecto cuando la minimización básica está habilitada.

RIESGO DE COMPATIBILIDAD No habilitar Strict Query Name Minimization indiscriminadamente: puede causar fallos con servidores autoritativos incompatibles. Aplicar tras pruebas DNS representativas.

45.19. Prefetch Support y Prefetch DNS Key Support

Opción	Beneficio	Coste o precaución
Prefetch Support	Anticipa el refresco de respuestas frecuentemente solicitadas antes de caducar.	Aumenta las consultas y la carga, aproximadamente 10 % en escenarios indicados por Netgate.
Prefetch DNS Key Support	Adelanta DNSKEY al detectar DS, reduciendo latencia de validación.	Consume recursos adicionales; requiere caché apropiada.

45.20. Harden DNSSEC Data, Serve Expired y Aggressive NSEC

Control	Activado	Precaución
Harden DNSSEC Data	Exige datos DNSSEC para zonas con ancla de confianza.	Evita rebajar validación por ausencia de firmas; no desactivar sin causa.
Serve Expired	Permite servir datos expirados bajo la política de actualización en segundo plano.	Equilibra disponibilidad y riesgo de información obsoleta.
Aggressive NSEC	Utiliza negaciones DNSSEC validadas para sintetizar respuestas negativas.	Comprobar DNSSEC y comportamiento de nombres inexistentes.

45.21. Drop Old UDP Queries y defensa ante saturación

Drop Old UDP Queries define el tiempo, en segundos, que una consulta UDP puede permanecer en la cola del socket antes de descartarse. El valor 0 desactiva la función de descarte por este criterio; Netgate describe 3 segundos como punto de partida seguro en muchos casos. Su utilidad crece ante saturaciones, pero descartes excesivos pueden percibirse como intermitencia DNS.

45.22. Message Cache Size y caché RRSet

Message Cache Size almacena códigos de respuesta y estados de validación. La GUI del material ofrece 4, 10, 20, 50, 100, 250 y 512 MB, y la referencia indica 4 MB por defecto. La caché de RRSet conserva los registros DNS y se ajusta automáticamente al doble del tamaño elegido para mensajes. Dimensionar memoria con métricas reales: un valor mayor no soluciona una ruta defectuosa, una ACL errónea o un DNS upstream caído.

45.23. Incoming TCP Buffers y Outgoing TCP Buffers

Incoming TCP Buffers controla las conexiones/búferes TCP de entrada por hilo; Outgoing TCP Buffers los destinados a consultar autoridades. Los valores enumerados incluyen 0, 10, 20, 30 y 50, con valor predeterminado 10. En 0, Unbound no acepta consultas TCP entrantes o no emite consultas TCP salientes, respectivamente. Esto puede romper respuestas voluminosas, uso de DNSSEC y recuperación por truncamiento UDP; no se aconseja deshabilitar TCP.

45.24. EDNS Buffer Size: MTU, fragmentación y TCP fallback

EDNS Buffer Size anuncia el tamaño del búfer UDP EDNS. Automatic calcula un valor a partir de las MTU de interfaces activas; también se muestran 512, 1220, 1232, 1432, 1480 y 4096 bytes. Valores reducidos disminuyen riesgo de fragmentación, aunque pueden incrementar cambios a TCP; valores altos elevan el riesgo de respuestas UDP fragmentadas y timeouts en redes que no las gestionan bien.

Configuración	Contexto habitual	Riesgo / verificación
Automatic	Punto de partida con MTU coherente.	Revisar si existen túneles de MTU reducida.
1232	Valor conservador habitual en caminos dual-stack.	Puede necesitar más consultas TCP.
1432	Alternativa recogida por Netgate ante algunos fallos de fragmentación.	No es solución universal para toda MTU.
4096	Máximo clásico de EDNS en Unbound.	Mayor posibilidad de fragmentación en redes reales.

45.25. Number of Queries per Thread y Jostle Timeout

Number of Queries per Thread limita las consultas simultáneas por hilo (512, 1024 o 2048 según la versión instalada). Superado el límite, Unbound puede descartar solicitudes cuando no puede desalojar consultas antiguas. Jostle Timeout controla cuándo sustituir consultas de larga duración en un servidor saturado; 100, 200, 500 y 1000 ms, con 200 ms como valor predeterminado documentado. Ajustar según carga y latencia real antes de incrementar capacidad.

45.26. Maximum TTL y Minimum TTL para RRsets y Messages

Maximum TTL limita durante cuánto tiempo se mantiene un dato en caché aunque el origen anuncie una vida útil mayor; el valor predeterminado documentado es 86400 s. Minimum TTL eleva la permanencia mínima, con valor 0 por defecto, respetando así las duraciones declaradas por el propietario del dominio. Fijar un mínimo elevado puede conservar datos antiguos tras cambios de IP y dificultar migraciones o recuperación ante fallo.

45.27. Keep Probing, TTL for Host Cache Entries y Number of Hosts to Cache

Keep Probing permite seguir comprobando servidores considerados caídos; sin esta opción, su revaluación puede retrasarse hasta el vencimiento del caché de infraestructura. TTL for Host Cache Entries conserva la información de latencia, estado y soporte EDNS de servidores ascendentes, con opciones de 1, 2, 5, 10 y

15 minutos (15 min por defecto). Number of Hosts to Cache limita la cantidad de servidores anotados; el valor por defecto es 10.000 y hay alternativas desde 1.000 hasta 200.000.

45.28. Unwanted Reply Threshold: protección ante respuestas sospechosas

El umbral registra respuestas inesperadas por hilo y, cuando alcanza el límite, limpia cachés RRSet y de mensajes e informa en el log. La lista incluye Disabled y cifras de varios millones; Netgate recomienda 10 millones como inicio si se activa. La limpieza puede aumentar súbitamente la carga de consultas y no sustituye actualizaciones ni mitigación de ataques.

45.29. Log Level: niveles 0 a 5

Nivel	Salida de log	Uso recomendado
0	Sin trazas ordinarias; errores relevantes.	Entorno estable, mínimo volumen.
1	Información operativa básica.	Operación habitual; nivel por defecto.
2	Información operativa detallada.	Diagnóstico inicial.
3	Detalle por consulta.	Investigación puntual, gran volumen.
4	Detalles algorítmicos internos.	Análisis especializado y temporal.
5	Identificación de clientes en fallos de caché.	Máxima cautela por privacidad y volumen.

A mayor nivel aumenta la posibilidad de almacenar nombres consultados e información relativa a clientes. Limitar retención, accesos y duración del diagnóstico. Preferir niveles bajos en producción.

45.30. Disable Auto-added Access Control: efecto sobre clientes

De forma predeterminada Unbound permite consultas de las redes de interfaces internas del firewall y determinadas redes de VPN. Disable Auto-added Access Control suprime esas autorizaciones automáticas: los orígenes permitidos deben definirse expresamente en Access Lists. Un cambio sin ACL preparadas puede cortar DNS a toda una LAN aunque las reglas del firewall permitan el puerto 53.

ADVERTENCIA DE ACCESO Antes de desactivar las ACL automáticas, crear y verificar las ACL manuales que cubren todas las redes cliente, los equipos de administración y VPN necesarias. Conservar una vía de administración alternativa.

45.31. Disable Auto-added Host Entries

Elimina los registros generados automáticamente para las direcciones IPv4 e IPv6 principales del firewall dentro del dominio configurado en System → General Setup. Puede impedir que clientes resuelvan el nombre del propio firewall si no existe otro registro adecuado. No modifica direcciones reales ni elimina reglas de firewall.

45.32. Experimental Bit 0x20 Support

Utiliza variaciones de mayúsculas y minúsculas en las consultas DNS para añadir entropía frente a intentos de suplantación. Es una función experimental y no reemplaza DNSSEC. Algunos servidores no respetan el patrón de mayúsculas esperado; solo activar si se ha validado compatibilidad y comportamiento del resolver.

45.33. DNS64 Support y DNS64 for Localhost

DNS64 sintetiza respuestas AAAA para ciertos nombres que solo tienen A, de manera que los clientes IPv6-only puedan comunicarse con servicios IPv4 a través de NAT64. Activar DNS64 sin un traductor NAT64 y un prefijo de síntesis coherentes no crea conectividad por sí solo. DNS64 for Localhost controla una excepción específica que evita sintetizar respuestas DNS64 para consultas desde localhost; modificarla únicamente si se conoce el motivo técnico.

45.34. Access Lists: finalidad, interfaz y controles

La pestaña Access Lists muestra una tabla con Access List Name, Action, Description y Actions. El botón Add crea una ACL; las filas existentes permiten administrarlas con los iconos que ofrezca la versión. Una

lista vacía solo significa ausencia de ACL manuales visibles: no prueba que no existan ACL automáticas internas. Las ACL de Unbound filtran consultas por origen, mientras las reglas PF deciden si el tráfico puede llegar al servicio.

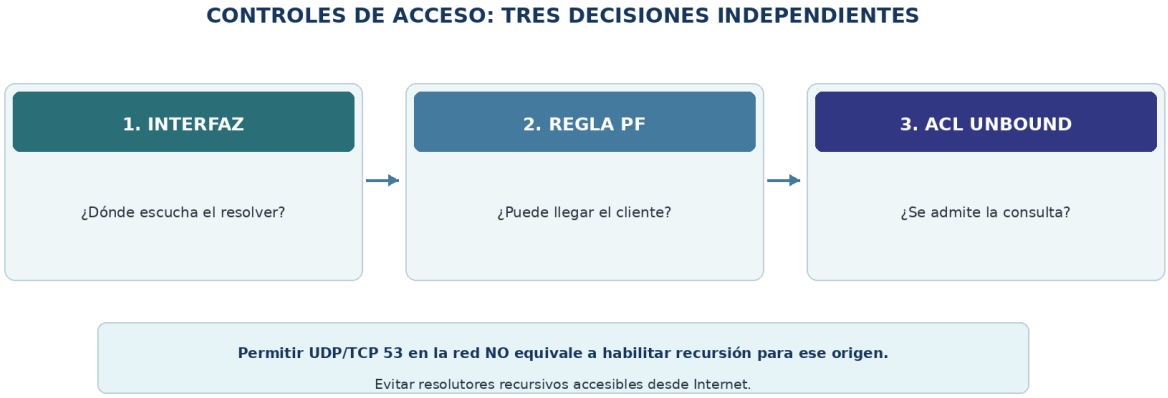


Figura 45.3. Punto de escucha, reglas PF y ACL de Unbound son controles complementarios.

45.35. Formulario de Access List: campos documentados

Campo	Qué especifica	Recomendación
Access List Name	Nombre de la ACL y comentario de configuración.	Identificador técnico breve, sin nombres de clientes reales.
Action	Tratamiento de consultas de las redes listadas.	Preferir mínimo privilegio.
Description	Texto administrativo de referencia.	Indicar propósito y responsable funcional, no credenciales.
Networks	Una o varias redes de origen IPv4/IPv6 con su prefijo.	Usar prefijos exactos: /32 o /128 para un único host.

45.36. Las seis acciones ACL de Unbound

Acción	Qué ocurre con la consulta	Cuándo emplearla
Allow	Permite recursión y consultas locales del origen.	LAN o VPN de confianza.
Deny	Descarta sin emitir respuesta.	Bloqueo silencioso deliberado.
Refuse	Devuelve código REFUSED al cliente.	Bloqueo explícito y fácil de diagnosticar.
Allow Snoop	Autoriza consultas recursivas y no recursivas que pueden inspeccionar caché.	Solo equipos de diagnóstico muy confiables.
Deny Nonlocal	Permite datos locales autoritativos y descarta recursión externa.	Clientes que solo precisan registros internos.
Refuse Nonlocal	Permite datos locales y rechaza consultas no locales con REFUSED.	Política de datos internos con respuesta explícita.

45.37. Procedimiento: crear una ACL segura para una red

01. Identificar una subred de laboratorio expresamente autorizada, sin tomar valores de una instalación existente.
02. Entrar en Services → DNS Resolver → Access Lists y seleccionar Add.
03. Rellenar Access List Name, Action = Allow, Description y Networks (prefijo de origen).
04. Guardar, aplicar cambios y comprobar el estado del servicio.
05. Verificar consultas A, AAAA y PTR desde un cliente autorizado.
06. Repetir consulta desde un origen no autorizado y confirmar que no dispone de recursión.

45.38. Escenario: delegar solo un dominio por VPN

Para resolver una zona corporativa remota se configura Domain Override hacia su DNS autoritativo/central accesible por VPN. Primero se comprueban ruta y reglas que permiten alcanzar el servidor; después el cliente interno debe tener acceso al DNS Resolver local mediante su interfaz, reglas y ACL. La delegación de dominio no significa abrir un resolver recursivo al extremo remoto.

45.39. Escenario: DNS cifrado y validado para clientes internos

Un diseño razonable puede admitir consultas DNS locales TCP/UDP 53 y restringir las comunicaciones de salida a resolutores DoT previamente seleccionados, con Forwarding Mode. Si además se requiere DNSSEC, se debe evaluar si la validación es posible y coherente con el comportamiento de esos upstream. Las consultas DoT entrantes exigen certificado confiable y dirección de servicio estable; habilitarlo no fuerza automáticamente a los clientes a usarlo.

45.40. Escenario: DNS en Multi-WAN y conmutación

Con enlaces redundantes, examinar la elección de servidores DNS en System → General Setup, pasarelas asociadas a cada resolutor, rutas reales y políticas de failover. Los servidores obtenidos por DHCP pueden quedar asociados a su interfaz dinámica. Si se usa Strict Outgoing Interface Binding hay que prever qué sucederá al caer la interfaz elegida.

01. Registrar los resolutores upstream y pasarelas previstas para cada salida.
02. Verificar resolución con ambas WAN disponibles.
03. Simular pérdida controlada del enlace principal dentro de una ventana de mantenimiento.
04. Comprobar consultas nuevas, latencia, rutas y logs.
05. Reponer el enlace, probar failback y revisar la política de salida de cada resolutor.

45.41. Procedimiento: puesta en marcha inicial de DNS Resolver

01. Asegurar acceso de administración, copia de configuración y estado de DNS Forwarder.
02. Activar DNS Resolver y mantener Listen Port en 53 salvo arquitectura que exija otro valor.
03. Seleccionar Network Interfaces: LAN y Localhost según necesidades, sin exponer WAN indiscriminadamente.
04. Decidir Resolver Mode o Forwarding Mode y, en este último caso, definir upstream válidos.
05. Configurar DNSSEC y, si procede, DoT con sus dependencias.
06. Comprobar ACL automáticas o añadir redes manuales específicas.
07. Guardar y aplicar; probar resolución y registros antes de desplegar a más clientes.

45.42. Comprobaciones funcionales desde clientes y firewall

Realizar pruebas de consulta con dig, nslookup o Diagnostics → DNS Lookup según herramientas disponibles. Los siguientes valores son únicamente de documentación: 192.0.2.1 representa el DNS del firewall de prueba y example.com es un dominio de prueba. No pegarlos como parámetros de producción.

Prueba de ejemplo	Qué demuestra	Interpretación
dig @192.0.2.1 example.com A	Resolución IPv4 y alcanzabilidad del puerto DNS.	La respuesta por sí sola no demuestra DNSSEC.
dig @192.0.2.1 example.com AAAA	Tratamiento de registros IPv6.	No presupone conectividad IPv6 extremo a extremo.
dig @192.0.2.1 example.com +tcp	Aceptación de DNS por TCP.	Útil si UDP falla o hay respuestas grandes.
dig @192.0.2.1 example.com +dnssec	Consulta con datos DNSSEC solicitados.	Validación efectiva requiere revisión del resultado y flags.
nslookup portal.lab.example.com 192.0.2.1	Funcionamiento de un Host Override.	La dirección debe ser la configurada en el laboratorio.

45.43. Averías frecuentes: síntomas, hipótesis y solución

Síntoma	Causas probables	Comprobación / corrección
DNS no responde en LAN	Unbound inactivo, ACL, interfaz o regla PF.	Estado del servicio; verificar escucha, TCP/UDP 53 y ACL.
Solo falla DNSSEC	Reloj, interceptación o respuesta rota en upstream.	NTP, consultas de prueba y logs; no desactivar validación permanentemente.
DoT saliente no funciona	Forwarding desactivado, 853 bloqueado, upstream sin TLS.	Validar configuración de todos los resolutores y ruta TCP 853.
DNS IPv6 falla	Interfaz IPv6 no escuchada, cliente fuera de ACL.	Revisar ACL IPv6, RA/DHCPv6 y firewall.
Falla tras activar Strict QNAME	Autoridad incompatibles.	Desactivar solo Strict, probar de nuevo.
Respuestas antiguas	TTL, caché local/remota o Serve Expired.	Revisar TTL y actualizar con procedimiento controlado.
Sin DNS tras perder una WAN	Binding estricto, ruta o servidor upstream inaccesible.	Verificar otra salida y resolver alternativo.

45.44. Controles de seguridad y endurecimiento

- Limitar Network Interfaces a redes de confianza y Localhost; no exponer recursión públicamente.
- Combinar ACLs de Unbound con reglas de Firewall para TCP/UDP 53 y, si se usa, DoT TCP 853.
- Mantener DNSSEC y NTP operativos; distinguir fallos de validación de errores de red.
- Evitar Allow Snoop salvo necesidad puntual de diagnóstico y acceso restringido.
- No incrementar Log Level sin evaluar privacidad, espacio disponible y retención.
- Documentar cada Domain Override y sus dependencias de VPN, routing, TLS y resolución de certificados.

45.45. Rendimiento, capacidad y métricas útiles

El ajuste de cachés, buffers y límites de consultas debe responder a evidencia: tasa de consultas, aciertos de caché, latencia, saturación de CPU, memoria y fallos de red. Incrementar Message Cache Size puede mejorar cargas repetidas, pero también aumenta el uso de RAM de RRSet. Prefetch reduce expiraciones de nombres frecuentes a costa de tráfico adicional. Dejar EDNS en Automatic como punto de partida y cambiarlo solo ante síntomas comprobados de fragmentación.

45.46. Plan de cambio y recuperación: evitar cortes de DNS

01. Exportar la configuración actual y anotar versión, estado de Unbound y DNS Forwarder, interfaces y ACL.
02. Elegir una ventana de bajo impacto y verificar una ruta de administración independiente del DNS.
03. Aplicar un único grupo coherente de cambios por intervención.
04. Medir consultas desde clientes IPv4/IPv6, un nombre local y un dominio externo.
05. Si aparece una avería, revertir el último cambio mediante la GUI o restauración de configuración, sin comprometer acceso de administración.
06. Verificar servicios dependientes: VPN, actualizaciones, DHCP, agentes de monitorización y servicios empresariales.

REGLA DE CAMBIO La resolución DNS es transversal: una modificación aparentemente local puede interrumpir autenticación, correo, VPN, software de negocio y navegación. Conservar una ruta administrativa accesible por dirección IP y respaldo probado.

45.47. Matriz de aceptación de la configuración

Control	Resultado esperado	Evidencia
Servicio y puertos	Unbound activo; TCP/UDP 53 o puertos definidos sin conflictos.	Status → Services y consulta de prueba.
Interfaces / ACL	Solo clientes autorizados resuelven consultas.	Pruebas desde dos orígenes y revisión de PF.
Nombres locales	Host Overrides y Domain Overrides responden correctamente.	Consulta A/AAAA/PTR de nombres de laboratorio.
DNSSEC	Validación estable y reloj correcto.	Pruebas con dominios firmados y logs.
TLS	DoT entrante/saliente según diseño; certificado verificado.	Prueba de sesión y tráfico 853.
Redundancia	DNS sigue el comportamiento esperado al fallar una salida.	Prueba de pérdida de WAN y recuperación.
Registro y privacidad	Nivel de log proporcional a la necesidad.	Revisión de logs y retención.

45.48. Glosario esencial

Término	Definición
Unbound	Servicio de recursión, reenvío, validación y caché de DNS.
ACL	Lista de control de acceso que autoriza o restringe consultas por origen.
DNSSEC	Extensiones DNS para validar autenticidad e integridad del dato.
DoT	DNS over TLS: cifrado de consultas entre dos extremos compatibles.
QNAME Minimization	Reducción de etiquetas del nombre divulgado en consultas intermedias.
RRSet	Conjunto de registros DNS del mismo propietario, tipo y clase.
EDNS	Extensiones del protocolo DNS para tamaños y funciones adicionales.
DNS64	Síntesis de AAAA para acceso IPv6 a destinos IPv4 mediante NAT64.
NXDOMAIN	Respuesta DNS que indica que el nombre solicitado no existe.
REFUSED	Código de respuesta que señala rechazo explícito de una consulta.
TTL	Tiempo de conservación de una respuesta DNS en caché.

45.49. Referencias oficiales de Netgate y estándares

- Netgate — DNS Resolver (Unbound)
- Netgate — DNS Resolver Configuration
- Netgate — DNS Resolver Advanced Options
- Netgate — DNS Resolver Access Lists
- Netgate — Host Overrides
- Netgate — Domain Overrides
- Netgate — DNS Resolver Mode
- Netgate — General Setup / DNS Servers
- Netgate — Multi-WAN and DNS

- Netgate — DNS Troubleshooting
- IETF — RFC 9156: DNS Query Name Minimisation
- IETF — RFC 7858: DNS over TLS
- IETF — RFC 6147: DNS64

46 Services → Dynamic DNS

Dynamic DNS Clients · RFC 2136 Clients · Check IP Services

Ruta de administración: Services → Dynamic DNS. Estudio de las tres pestañas de configuración, sus formularios asociados, la actualización de registros DNS ante cambios de dirección y la integración con enlaces WAN dinámicos, IPv6 y escenarios Multi-WAN.

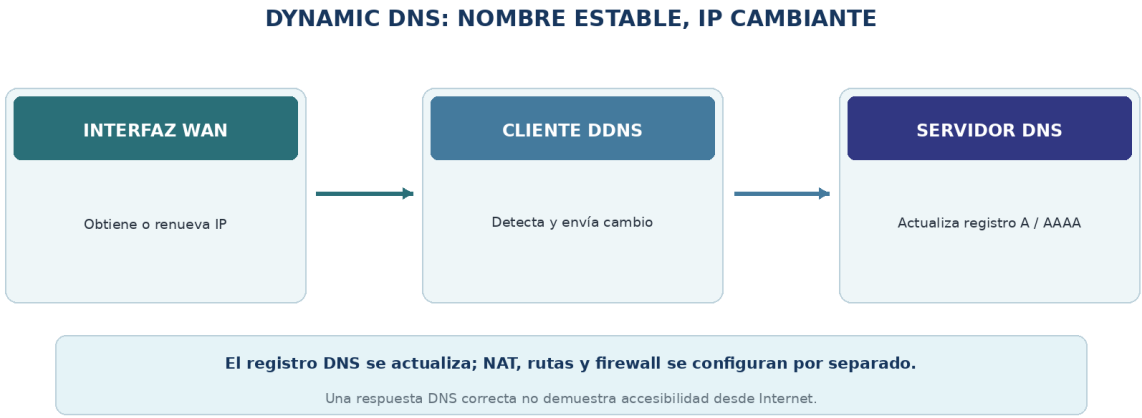


Figura 46.1. Arquitectura general de actualización de un nombre DNS cuando cambia una dirección WAN.

46.1. Finalidad y alcance del servicio Dynamic DNS

Dynamic DNS (DDNS) mantiene asociado un nombre DNS a una dirección IPv4 o IPv6 que puede variar. El firewall comprueba la dirección relevante y envía una actualización al proveedor o al servidor DNS autorizado. Su utilidad principal es conservar un nombre estable para acceso remoto, pasarelas VPN, monitorización y servicios publicados cuando la dirección exterior no es fija.

El menú contiene Dynamic DNS Clients, RFC 2136 Clients y Check IP Services. Cada pestaña reúne un mecanismo diferente de actualización o comprobación de direcciones. Los formularios y proveedores disponibles pueden variar por versión de pfSense Plus.

46.2. Qué resuelve DDNS y qué no resuelve

Sí permite	No garantiza por sí solo
Actualizar el registro A/AAAA asociado a una IP variable.	Conectividad, apertura de puertos o disponibilidad del servicio.
Mantener un nombre de conexión para clientes VPN.	Superar CGNAT o restricciones de puertos del operador.
Asociar registros a interfaces o determinadas configuraciones Multi-WAN.	Que sesiones existentes sobrevivan a una caída de WAN.
Enviar actualizaciones mediante proveedor o RFC 2136.	Que todos los resolutores externos invaliden de inmediato su caché.
DISTINCIÓN IMPORTANTE Dynamic DNS administra la publicación de una dirección en DNS. La exposición de servicios exige, cuando corresponda, direccionamiento alcanzable, NAT, reglas de firewall, certificados, rutas, gateways y seguridad del servicio.	

46.3. Recorrido del menú y tipos de cliente

Pestaña	Función	Caso de uso
Dynamic DNS Clients	Actualización mediante proveedores compatibles y APIs HTTP/HTTPS.	WAN doméstica o empresarial de IP dinámica.
RFC 2136 Clients	Actualización DNS dinámica estándar contra servidor que admita RFC 2136.	Zona DNS bajo control propio o corporativo.
Check IP Services	Define páginas de comprobación de la dirección pública observada desde Internet.	WAN detrás de NAT de otro equipo.

46.4. Pantalla Dynamic DNS Clients: estructura y columnas

El listado mostrado contiene las columnas Status, Interface, Service, Hostname, Cached IP, Description y Actions, junto a Add. Cuando no hay entradas, la tabla aparece vacía. Los indicadores verdes de estado y Cached IP señalan que, según el seguimiento del cliente DDNS, el valor está actualizado respecto al proveedor; la comprobación externa sigue siendo necesaria.

Columna	Interpretación y comprobación
Status	Indicador de estado de la entrada. Revisar alertas, fallos y última ejecución antes de asumir funcionamiento.
Interface	Interfaz o selección de salida monitorizada; relevante para una o varias WAN.
Service	Proveedor o modo de actualización configurado.
Hostname	Nombre DNS administrado por la entrada.
Cached IP	Última dirección recordada por el cliente; no sustituye una consulta externa al DNS autoritativo.
Description	Nota operativa de la entrada para identificación y auditoría.
Actions	Acceso a las operaciones disponibles para la entrada, como editar o eliminar; según revisión pueden variar los iconos.

46.5. Acciones de la tabla: Add, edición, desactivación y actualización

Add abre el formulario de alta de un cliente. Tras crear una entrada aparecen las acciones compatibles con la versión, normalmente editar, deshabilitar o eliminar. El formulario de edición también puede disponer de Save and Force Update para enviar una actualización de prueba de manera expresa. Eliminar una entrada suprime su automatización, pero no necesariamente elimina el registro que permanezca en el proveedor DNS.

01. Seleccionar la pestaña Dynamic DNS Clients.
02. Abrir Add y elegir Service Type.
03. Seleccionar la interfaz o gateway group, si está disponible y es adecuado al diseño.
04. Introducir nombre DNS y las credenciales exigidas por el proveedor.
05. Guardar y comprobar estado, Cached IP, logs y resolución desde una red ajena.

46.6. Formulario: Disable, Service Type e Interface to Monitor

Campo	Qué hace	Criterio profesional
Disable	Desactiva la actualización de esa entrada sin necesariamente borrarla.	Útil en mantenimiento o migración de proveedor.
Service Type	Selecciona proveedor o configuración Custom.	Las opciones exactas dependen de la versión y la API del proveedor.
Interface to Monitor	Toma la dirección supervisada de una WAN u otra interfaz seleccionada.	Elegir la salida que deba figurar en DNS; validar la familia IPv4/IPv6.
Gateway group	Cuando está admitido, permite seguir cambios entre WAN conforme a la política del grupo.	Comprobar coherencia con NAT, políticas de entrada y failover real.

Una interfaz con dirección privada puede exigir comprobar la dirección pública externa. Un gateway group no convierte automáticamente dos operadores con CGNAT en una solución de acceso entrante.

46.7. Hostname, Domain Name, MX y Wildcards

Campo	Significado
Hostname	Normalmente FQDN completo; algunos proveedores exigen únicamente el nombre de host.
Domain Name	Campo condicional para proveedores como Namecheap, que separan host y dominio.

Campo	Significado
MX	Servidor de correo asociado, solo si el proveedor admite esta actualización.
Wildcards	Si el proveedor lo soporta, permite resolver subdominios bajo el nombre DDNS hacia la misma IP.

Para los procedimientos se utiliza el dominio reservado de documentación example.com. No conviene utilizar comodines para publicar servicios indiscriminadamente: un wildcard DNS no habilita por sí solo servicios o permisos de firewall.

46.8. Username, Password, tokens y claves API

Las credenciales son específicas del proveedor: pueden ser usuario/contraseña, token, clave API, identificador de acceso y secreto. Algunos proveedores requieren que Username quede en blanco o contienen credenciales en un campo distinto al que su nombre sugiere. Netgate documenta, por ejemplo, variantes para Namecheap, FreeDNS, Route 53 y otras integraciones; verificar siempre la guía vigente del proveedor.

- Utilizar credenciales con el alcance mínimo necesario para modificar exclusivamente los registros previstos.
- No escribir tokens en Description, exportaciones compartidas, capturas ni anotaciones de diagnóstico.
- Guardar la configuración cifrada de forma segura y limitar la lectura de backups.
- Rotar los secretos y efectuar Save and Force Update tras una modificación, comprobando resultado y resolución.

SECRETO DE PUBLICACIÓN Una clave que permite alterar el registro DNS puede desviar clientes a otro destino. Protegerla como credencial administrativa y revisar permisos de la cuenta del proveedor.

46.9. Verbose Logging, Verify SSL Peer y Description

Campo	Efecto	Recomendación
Verbose Logging	Incrementa detalles de actualización y diagnóstico.	Activar temporalmente ante fallos y reducirlo después.
Verify SSL Peer	Valida la identidad del servidor HTTPS mediante su certificado.	Mantener validación en servicios públicos fiables; no deshabilitarla por conveniencia.
Description	Anotación para inventariar finalidad y responsable funcional.	Usar un identificador neutro del servicio sin secretos.

En algunos textos de ayuda de Netgate, la referencia a certificados autofirmados puede resultar ambigua. Lo importante es comprobar en la versión instalada si la opción activa o relaja la validación. Evitar desactivar comprobaciones de certificado, ya que un atacante podría interceptar la actualización.

46.10. Proveedores con parámetros propios: aspectos más frecuentes

Proveedor o modo	Campos o peculiaridades documentadas
Namecheap	Hostname separado de Domain Name; token en Password; Username vacío.
Route 53	Identificador de acceso, clave secreta, Zone ID y TTL cuando proceda.
Custom	Interface to send update from, Force IPv4 Resolving, Update URL y Result Match.
HE.net Tunnelbroker	Puede utilizar identificador de túnel como Hostname para actualizar el extremo IPv6.
Otros proveedores	El formulario puede exponer opciones diferentes según API; no extrapolar campos de uno a otro.

46.11. Custom Dynamic DNS: URL y comprobación de respuesta

El modo Custom permite trabajar con un servicio que no figure en Service Type. Update URL corresponde al endpoint autorizado; el marcador %IP% puede sustituirse por la dirección conocida cuando el proveedor lo requiera. Result Match compara la respuesta con un texto esperado para confirmar éxito. Una

coincidencia errónea puede mostrar fallo aunque el registro cambie, o presentar éxito aparente si la API responde ambiguamente.

01. Consultar la API pública del proveedor y crear una credencial limitada.
02. Definir Update URL en HTTPS con el formato indicado por su documentación.
03. Usar %IP% únicamente donde la API espere la dirección publicada.
04. Establecer Result Match con la respuesta exacta de éxito cuando esté disponible.
05. Guardar, forzar una actualización de prueba y confirmar con consulta DNS independiente.

46.12. IPv4, IPv6 y registros A/AAAA

El registro A almacena una dirección IPv4; el AAAA, una dirección IPv6. No debe suponerse que todos los proveedores o tipos de entrada actualizan ambas familias ni que un nombre con A y AAAA ofrece idéntica conectividad por ambas. En acceso dual-stack, comprobar las dos resoluciones y las reglas IPv6 por separado. Si la WAN utiliza prefijos IPv6 dinámicos, analizar también las direcciones publicadas y la estabilidad del servicio de destino.

46.13. Multi-WAN: supervisión, conmutación y dirección publicada

Netgate permite seleccionar, cuando procede, un gateway group para que el cliente DDNS refleje el cambio entre salidas. Este mecanismo solo actualiza la referencia DNS y está sujeto a los eventos de monitorización, TTL y políticas del proveedor. La infraestructura debe contemplar qué WAN recibe conexiones y qué VIP/NAT/puertos se mantienen durante la conmutación.

01. Crear y probar los gateways y el grupo correspondiente.
02. Definir la entrada DDNS sobre la selección apropiada y guardar.
03. Verificar que la IP publicada coincide con la salida que realmente permite recibir tráfico.
04. Simular fallo de la WAN principal en una ventana controlada y observar el cambio DNS.
05. Comprobar el acceso externo por el servicio de aplicación o VPN, no solo el ping del firewall.
06. Reponer la WAN y verificar el retorno de registros y sesiones nuevas.

MULTI-WAN Un servicio ejecutado en el propio firewall puede utilizar la ruta predeterminada y no balancear conexiones como lo hace una regla de política para clientes. La verificación de DDNS debe incluir salida efectiva y ruta del proceso.

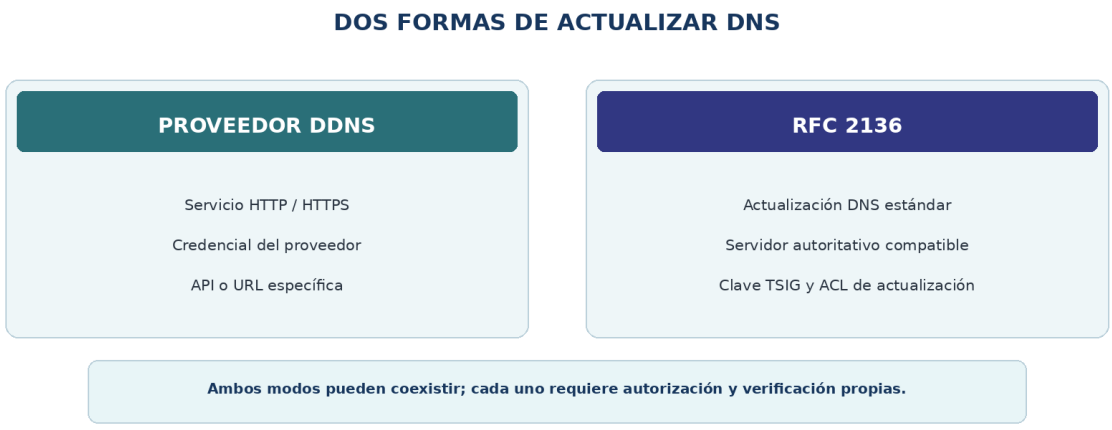


Figura 46.2. Actualización mediante proveedor DDNS y mediante DNS estándar RFC 2136.

46.14. RFC 2136 Clients: concepto y casos de uso

RFC 2136 define el protocolo de actualización dinámica de DNS. pfSense Plus puede remitir actualizaciones a servidores que lo admitan, como BIND o determinadas configuraciones de Windows Server DNS. Es independiente de la pestaña de proveedores HTTP/HTTPS y puede coexistir con ella; requiere permisos expresos del servidor autoritativo.

46.15. RFC 2136: campos Enable, Interface, Hostname y Zone

Campo	Función y recomendación
Enable	Habilita la entrada de actualización. Desactivado, no envía cambios para ese registro.
Interface	Dirección que el cliente enviará para actualizar los registros seleccionados.
Hostname	FQDN del registro a actualizar; ejemplo documental host.dynamic.example.com.
Zone	Zona DNS de la operación, si se exige; normalmente opcional según servidor.

46.16. RFC 2136: TTL, Key Name, Key Algorithm y Key

TTL (segundos) controla durante cuánto tiempo los resolutores pueden conservar una respuesta antigua; Netgate sugiere habitualmente valores bajos, en torno a 30-180 segundos cuando la IP cambia con frecuencia. El valor real se fija conforme al diseño y la carga DNS. Key Name identifica la clave autorizada en el servidor; Key Algorithm define el algoritmo criptográfico, y Key contiene el secreto TSIG, que no debe aparecer en documentación, trazas ni anotaciones.

La autenticación TSIG protege la autorización de la actualización entre cliente y servidor. Debe restringirse el secreto a un ámbito concreto y configurar permisos en el lado autoritativo. Un nombre o algoritmo que no coincide produce errores de actualización aunque el DNS siga respondiendo consultas ordinarias.

46.17. RFC 2136: Server, Protocol, Use Public IP y Update Source

Campo	Efecto
Server	Servidor DNS autorizado que recibe la actualización; debe ser alcanzable desde pfSense.
Protocol	Según el formulario documentado, sin marcar usa UDP; marcado, TCP.
Use Public IP	Si se detecta IP privada en interfaz seleccionada, puede consultar la IP pública exterior.
Update Source	Interfaz o dirección origen empleada para transmitir el mensaje de actualización.
Update Source Family	IPv4 o IPv6 del origen desde el que se envía la actualización.
Record Type	A, AAAA o Both, según direcciones y registros que se pretenda mantener.
Description	Texto administrativo sin secretos.

46.18. RFC 2136: procedimiento sobre servidor DNS autoritativo

01. Crear una zona de laboratorio bajo example.com y habilitar actualizaciones para el nombre concreto previsto.
02. Generar una clave TSIG en el servidor DNS y limitar sus permisos; custodiar el secreto externamente.
03. En pfSense, abrir Services → Dynamic DNS → RFC 2136 Clients → Add.
04. Configurar Enable, Interface, Hostname, Zone si procede, TTL, Key Name, Key Algorithm y Key.
05. Indicar Server, Protocol, Record Type y Update Source conforme a rutas y red disponibles.
06. Guardar y ejecutar Save and Force Update si la versión proporciona la acción.
07. Consultar directamente el servidor autoritativo y después un resolutor independiente.
08. Revisar logs del servidor DNS y del firewall si la actualización no aparece.

Netgate indica que las actualizaciones RFC 2136 se desencadenan por cambio de IP o periódicamente, aproximadamente cada 25 días; no equivale a una transmisión de todas las entradas con cada consulta DNS.

46.19. RFC 2136: errores de autenticación, permisos y zona

Síntoma	Causa probable	Comprobación
REFUSED / denegado	Actualizaciones no permitidas o política de zona.	Permisos del servidor DNS y nombre afectado.
BADKEY / BADSIG	TSIG incorrecta, algoritmo o secreto no coincidente.	Key Name, algoritmo, clave y registros del autoritativo.
Sin respuesta	Ruta, firewall, puerto, UDP/TCP o servidor fuera de línea.	Ping, captura de paquetes y conectividad 53/UDP-TCP.
Actualiza A pero no AAAA	Record Type o dirección IPv6 ausente.	Estado IPv6 de interfaz y tipo de registro.
Se mantiene IP anterior	TTL, caché, nombre incorrecto o actualización rechazada.	Consulta directa a autoritativo y después a cachés externas.

46.20. Check IP Services: cuándo es necesario

Cuando la WAN recibe una dirección privada de un router intermedio, el firewall puede necesitar averiguar qué IP pública ven los servicios externos. Check IP Services define una página web que responde con dicha IP; después una entrada DDNS compatible puede utilizar este resultado para publicar la dirección observada. El servicio debe devolver la dirección de manera estable y comprensible por el cliente.

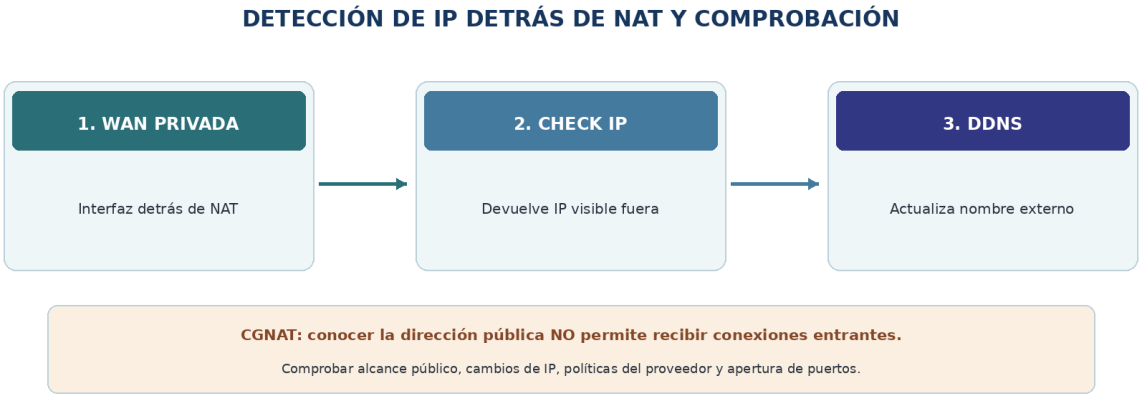


Figura 46.3. Comprobación pública tras un NAT; diferencia entre resolver DDNS y poder aceptar conexiones entrantes.

46.21. Check IP Services: Enable, Name, URL y Description

Campo	Qué hace
Enable	Permite que los clientes DDNS utilicen este servicio de verificación.
Name	Nombre corto distintivo para localizarlo en los selectores.
URL	URL completa de la página que informa de la dirección observada.
Description	Explicación administrativa de propósito, fiabilidad y origen del servicio.

La página de comprobación debe devolver la IP del solicitante, no una cadena de caracteres arbitraria. La documentación oficial muestra formatos con el texto Current IP Address seguido de una dirección; también se admiten formatos conforme a la versión y al cliente.

46.22. Check IP Services: Username/Password y Verify SSL Peer

Username/Password añade autenticación opcional a la URL cuando el verificador es privado. Verificar que el cliente accede a través de TLS válido y que las credenciales no quedan incrustadas en una URL compartida. El significado exacto del control Verify SSL Peer debe comprobarse sobre la versión instalada porque los textos de ayuda publicados por Netgate contienen una redacción confusa con certificados autofirmados. La práctica segura es verificar identidad del servidor y no desactivar validación para solventar errores.

46.23. Cómo implantar un servicio Check IP confiable

01. Seleccionar un servicio de comprobación HTTPS fiable o alojar una página controlada que devuelva únicamente la IP pública observada.
02. Comprobar manualmente desde cada salida WAN que la respuesta coincide con la dirección que se quiere publicar.
03. Crear la entrada en Check IP Services con nombre, URL y opciones de validación apropiadas.
04. Asociarla al cliente DDNS que soporte esa modalidad de detección.
05. Simular cambios de ruta/NAT y comparar Cached IP, servidor autoritativo y consulta externa.

Un endpoint alojado por terceros recibe peticiones del firewall; considerar privacidad y disponibilidad. Un verificador comprometido podría provocar que el cliente DDNS publique una dirección incorrecta.

46.24. CGNAT y doble NAT: limitaciones de accesibilidad

Las direcciones privadas RFC 1918 o las direcciones compartidas del espacio 100.64.0.0/10 pueden señalar que el enlace no tiene una IPv4 pública directamente enrutable. Check IP descubrirá la dirección pública usada al salir, pero una red del operador con CGNAT puede impedir conexiones entrantes y redirecciones de puerto hacia el firewall. La solución suele pasar por disponer de IPv4 pública accesible, IPv6 global con reglas, VPN saliente hacia punto público o servicios de intermediación, según política de seguridad.

NO CONFUNDIR Que dynamic.example.com resuelva a una IP pública no demuestra que una sesión TCP entrante llegue al firewall. Verificar desde otra conexión y consultar la política del proveedor si existe CGNAT.

46.25. Consulta del estado, Cached IP y validación externa

01. Consultar Status y Cached IP del cliente en la GUI.
02. Verificar en el proveedor o autoritativo el valor actual del registro A y/o AAAA.
03. Desde otra red, consultar DNS con nslookup o dig y comparar valor y TTL.
04. Comprobar el servicio real por el puerto previsto, tras revisar NAT/firewall cuando corresponda.
05. Registrar fecha y motivo de cambio, tiempos de actualización y resultado de prueba.

La caché DNS puede mantener una IP antigua durante su TTL. Forzar una actualización DDNS no invalida por sí mismo las respuestas ya conservadas en los resolutores de terceros.

46.26. Procedimiento de alta: proveedor DDNS habitual

01. Crear el hostname en el proveedor de confianza y revisar su mecanismo de autenticación.
02. En Dynamic DNS Clients, pulsar Add y escoger Service Type.
03. Seleccionar Interface to Monitor y especificar el hostname documental de laboratorio.
04. Introducir las credenciales o token bajo el formato propio del proveedor.
05. Habilitar validación TLS y logging temporal de diagnóstico si se precisa.
06. Guardar, enviar actualización de prueba y consultar el registro con DNS externo.

46.27. Caso empresarial 1: acceso VPN mediante hostname dinámico

Una instalación necesita que sus clientes VPN utilicen un nombre en lugar de una dirección IP mutable. DDNS actualiza vpn.dynamic.example.com cuando cambia la WAN. El servicio VPN debe escuchar en la interfaz apropiada, disponer del certificado correspondiente y estar permitido por las reglas de entrada; los clientes deberán volver a resolver el nombre cuando su conexión necesite restablecerse. En conexiones ya establecidas, el cambio de IP puede exigir reconexión.

46.28. Caso empresarial 2: DNS corporativo con actualizaciones RFC 2136

La organización administra su zona en BIND o Windows DNS y permite que un único registro sea actualizado por pfSense mediante TSIG. Se crea una clave de alcance limitado, se autoriza únicamente la

zona/subzona necesaria y se registran las acciones. Las consultas de terceros pueden permanecer en caché y los registros AAAA requieren pruebas equivalentes a los A.

46.29. Caso empresarial 3: WAN detrás de router de operador

El equipo exterior hace NAT y entrega una dirección privada al firewall. Check IP determina la dirección pública exterior y el cliente DDNS la publica. Si el NAT de borde permite reenvío, este debe configurarse en todos los dispositivos relevantes y someterse a pruebas externas. Si hay CGNAT del proveedor, no debe presuponerse que el reenvío sea posible.

46.30. Caso empresarial 4: failover y publicación de acceso remoto

Dos enlaces WAN permiten continuidad de salida, pero el acceso entrante requiere que la WAN de respaldo proporcione una dirección alcanzable. Se define un grupo de gateways compatible, la entrada DDNS asociada y los accesos permitidos en cada camino. Se comprueban cambios de IP, tiempos de propagación, reconexión y comportamiento de los servicios expuestos. El diseño puede requerir alternativas cuando una de las WAN usa CGNAT.

46.31. Seguridad de las actualizaciones y protección de credenciales

- Aplicar mínimo privilegio sobre tokens de proveedor, credenciales TSIG y zonas actualizables.
- Preferir HTTPS con certificado validado y algoritmos TSIG actualizados y admitidos por el servidor.
- Restringir conectividad a los endpoints necesarios y supervisar errores de actualización.
- Evitar publicar interfaces o accesos administrativos por DDNS sin VPN y control de acceso adecuados.
- Mantener copia segura de configuración, rotación de secretos y evidencia de cambios.

46.32. Rendimiento, frecuencia de cambios y TTL DNS

Los registros dinámicos deben equilibrar rapidez de propagación y número de consultas. Un TTL muy elevado puede retrasar la convergencia tras la pérdida de WAN; demasiado bajo puede incrementar peticiones y no garantiza que todos los clientes resuelvan inmediatamente. En RFC 2136 se citan 30–180 segundos como intervalo razonable para muchos casos. Evitar programar actualizaciones repetitivas innecesarias cuando no cambia la IP: pueden existir límites de API y políticas antiabuso del proveedor.

46.33. Diagnóstico: el registro no se actualiza

Comprobación	Prueba / causa
Interfaz monitorizada	¿La IP observada es la esperada y hay ruta para llegar al servicio de actualización?
Autenticación	¿Token, usuario, contraseña, zona, clave TSIG y permisos continúan válidos?
Conectividad / SSL	¿Resuelve el endpoint, funciona HTTPS/TLS y se acepta su certificado?
Respuesta del proveedor	¿Existe fallo HTTP, cuota, límite de frecuencia o resultado de API inesperado?
Registro / caché	¿La consulta se hace al autoritativo o a una caché que conserva el valor previo?
WAN secundaria	¿La IP pública observada y la ruta coinciden con el enlace deseado?

46.34. Diagnóstico: DNS correcto, servicio inaccesible

Revisar si existe IP pública realmente alcanzable, cambios de port-forwarding, reglas de entrada, reglas IPv6, disponibilidad de VPN/aplicación, gateway y rutas de respuesta, certificados y firewall externo. También comprobar CGNAT, filtrado del operador y diferencias entre WAN principal y respaldo. Un test satisfactorio de DNS no reemplaza pruebas TCP/UDP del servicio.

46.35. Plan de cambio, rollback y continuidad

01. Exportar configuración antes de editar entradas, sin publicar los secretos almacenados.

02. Anotar proveedor, tipo, interfaz de monitorización, FQDN y TTL sin credenciales.
03. Realizar cambio en ventana controlada y disponer de acceso administrativo independiente del hostname DDNS.
04. Validar consulta directa al autoritativo, consulta pública y conexión real al servicio.
05. Si aparece incidencia, revertir la entrada o activar la configuración anterior y volver a medir resolución y conectividad.

46.36. Matriz de aceptación de la configuración

Control	Resultado esperado	Evidencia
Cliente activo	Entrada habilitada y sin errores de actualización.	Status y logs DDNS.
Registro DNS	El A/AAAA coincide con la dirección prevista.	Consulta al servidor autoritativo.
Check IP	El servicio informa de la salida pública correcta.	Comparación de respuesta por interfaz.
Multi-WAN	La publicación cambia cuando corresponde.	Prueba planificada de failover.
Acceso real	La aplicación/VPN acepta conexiones desde fuera.	Prueba desde red independiente.
Seguridad	Credenciales limitadas y protegidas.	Revisión de permisos, TLS y secretos.
Recuperación	Plan de reversión reproducible.	Registro de prueba y respaldo.

46.37. Glosario

Término	Significado
DDNS	DNS dinámico: actualización automática de registros cuando cambia una IP.
A / AAAA	Tipos de registro para IPv4 e IPv6 respectivamente.
FQDN	Nombre DNS totalmente cualificado.
TTL	Tiempo recomendado para conservar en caché un registro DNS.
RFC 2136	Protocolo de actualizaciones dinámicas de DNS.
TSIG	Autenticación mediante clave compartida de mensajes DNS, incluida actualización.
Cached IP	Dirección registrada por el cliente DDNS como última conocida.
Check IP	Servicio que muestra la dirección pública observada de un cliente.
CGNAT	NAT de operador compartido, con limitaciones habituales para conexiones entrantes.
Gateway group	Agrupación de pasarelas para políticas de conmutación o balanceo.

46.38. Pruebas DNS externas: consulta, caché y conectividad

La comprobación debe hacerse desde una red independiente del firewall, preferiblemente con otro proveedor. Para verificar la actualización de una zona, preguntar al servidor autoritativo y, en paralelo, a uno o más resolutores recursivos. Si la respuesta autoritativa ya es nueva pero el cliente ve la IP antigua, estudiar el TTL y la caché antes de cambiar de nuevo las credenciales.

Prueba	Método reproducible	Qué permite descartar
Consulta normal	nslookup vpn.dynamic.example.com	Error de sintaxis de nombre y ausencia de respuesta DNS.
Registro IPv4	dig vpn.dynamic.example.com A +short	Desajuste de dirección A respecto a WAN publicada.

Prueba	Método reproducible	Qué permite descartar
Registro IPv6	dig vpn.dynamic.example.com AAAA +short	Omisión o error de AAAA en servicios dual-stack.
Consulta autoritativa	dig @servidor-autoritativo vpn.dynamic.example.com A	Problemas de actualización frente a retención en caché.
Prueba de servicio	Conexión a VPN o servicio de prueba desde otra red	Errores NAT, firewall, rutas, CGNAT o servicio caído.

Los nombres anteriores son ejemplos reservados. Sustituirlos por nombres de laboratorio propios al ejecutar pruebas, sin registrar credenciales ni valores internos en el libro.

46.39. Ficha de revisión y auditoría de DDNS

Cada entrada dinámica debe contar con responsable funcional, servicio dependiente, proveedor, hostname, selección de interfaz, registros A/AAAA, TTL, credencial custodiada, método de verificación y procedimiento de reversión. Revisar periódicamente si el hostname continúa en uso y retirar tokens de entradas retiradas.

Momento	Control mínimo	Acción si no cumple
Alta	Credencial limitada y FQDN autorizado; IP externa validada.	No publicar hasta completar las comprobaciones.
Cambio WAN	Gateway correcto; IP publicada y conectividad externa comprobadas.	Revisar política de salida y propagación DNS.
Rotación de claves	Actualizar credencial y ensayar actualización forzada.	Restablecer secreto controlado y revisar logs.
Baja de servicio	Eliminar automatización y registros obsoletos cuando proceda.	Revocar token y comprobar ausencia de exposición.

46.40. Referencias oficiales de Netgate y estándares

- Netgate — Dynamic DNS: visión general
- Netgate — Configuring a Dynamic DNS Client
- Netgate — Configuring RFC 2136 Dynamic DNS updates
- Netgate — Configuring IP Address Check Services
- Netgate — Configuring BIND as an RFC 2136 Server
- Netgate — Changing Credentials and Keys
- Netgate — Troubleshooting Multi-WAN
- Netgate — DNS Lookup
- IETF — RFC 2136: Dynamic Updates in DNS
- IETF — RFC 2845: Secret Key Transaction Authentication
- IETF — RFC 6598: Shared Address Space (CGNAT)

47 Services → IGMP Proxy

Multicast IPv4 · Upstream / Downstream · Reglas y diagnóstico

Ruta de administración: Services → IGMP Proxy. Estudio de la pantalla principal, los controles Enable y Verbose Logging, la tabla de instancias y el formulario Add. Se incorporan procedimientos, escenarios empresariales, verificación y pautas de administración seguras.

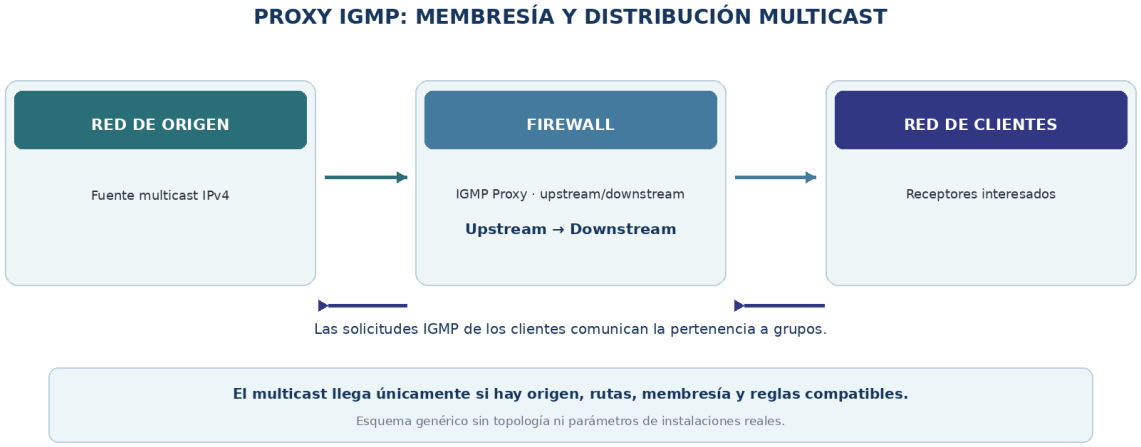


Figura 47.1. Arquitectura conceptual de un proxy IGMP entre la fuente y las redes de recepción.

47.1. Finalidad, alcance y utilidad de IGMP Proxy

IGMP Proxy permite transportar tráfico multicast IPv4 desde una red de origen hacia segmentos donde existen receptores suscritos a determinados grupos. Su función no consiste en repetir indiscriminadamente todo el tráfico: utiliza la información de membresía de IGMP para aproximar las necesidades de los clientes y solicitar el flujo correspondiente hacia la red de origen.

Resulta útil en entornos IPTV, distribución de vídeo o audio multicast, sistemas de información que transmiten a varios receptores y determinadas aplicaciones empresariales que atraviesan subredes. La prestación depende igualmente de la fuente, del equipo de acceso, de las VLAN y de los switches intermedios.

47.2. Multicast frente a unicast y broadcast

Modalidad	Destino y comportamiento	Uso habitual
Unicast	Un emisor entrega tráfico a un receptor; cada destino puede requerir flujo propio.	Navegación, acceso a servidores, sesiones TCP.
Broadcast	Emisión a todos los equipos de un dominio de difusión compatible.	ARP en IPv4 y determinados mecanismos locales.
Multicast	Un emisor transmite a un grupo lógico cuyos receptores expresan interés.	IPTV, distribución multimedia y telemetría de grupo.

Las direcciones de grupo multicast IPv4 pertenecen a 224.0.0.0/4. IGMP participa en la gestión de la membresía; el contenido de las aplicaciones suele circular mediante UDP, aunque IGMP por sí mismo no usa números de puerto.

47.3. Conceptos fundamentales: grupo, IGMP, upstream y downstream

Concepto	Interpretación operativa
Grupo multicast	Identificador lógico IPv4 al que un receptor solicita pertenecer; no identifica un servidor único.
Join / membresía	Comunicación de interés por un grupo, conforme a las versiones de IGMP compatibles.

Concepto	Interpretación operativa
Leave	Notificación de abandono cuando corresponde al mecanismo y versión usados.
Upstream	Segmento por el que se alcanza la fuente de los datos multicast.
Downstream	Segmento donde están los receptores y donde se atiende su membresía.
TTL	Límite de saltos IPv4 utilizado para acotar el alcance de paquetes multicast.

47.4. Ruta y estructura de la pantalla principal

La pantalla muestra Services / IGMP Proxy, una sección General IGMP Options, un botón Save y una segunda sección IGMP Proxy con un listado de instancias y el botón Add. Si aún no hay instancias definidas, la tabla se presenta vacía y Add permite comenzar la configuración.

47.5. General IGMP Options: Enable

Enable — Enable IGMP. Activa el servicio de proxy IGMP sobre las instancias definidas. Desactivado, no se utiliza el proxy para transmitir los grupos entre las redes indicadas, aunque cada segmento puede mantener el comportamiento multicast local propio de sus equipos. Habilitarlo sin una instancia upstream y una downstream correctamente definidas no constituye una configuración funcional.

ADVERTENCIA Antes de habilitar el servicio, comprobar rutas, fuente multicast, grupos, reglas y compatibilidad del equipamiento. Un error puede interrumpir televisión IP o distribución multicast empresarial sin afectar necesariamente al tráfico unicast.

47.6. General IGMP Options: Verbose Logging

Verbose Logging — Enable verbose logging. Amplía el detalle de los mensajes emitidos por el servicio para investigaciones temporales: inicio, problemas de interfaz o incidencias relativas a grupos. Para observar mensajes informativos debe ajustarse asimismo el nivel de registro en Status → System Logs → Settings, según indica el propio texto de ayuda.

Mantener el registro detallado únicamente el tiempo indispensable; genera más eventos, puede ocupar espacio local y dificultar la revisión. Los mensajes de igmpproxy pueden consultarse entre los registros de Routing en pfSense, conforme a la documentación de Netgate.

47.7. Botón Save y aplicación de cambios

Save registra las opciones globales de la pantalla. Después de habilitar o modificar el proxy conviene comprobar el estado del proceso y el efecto real sobre el tráfico, porque guardar parámetros no demuestra por sí mismo que exista una fuente multicast válida ni receptores activos. Distinguir la configuración de opciones generales del guardado de cada instancia individual creada mediante Add.

47.8. Listado IGMP Proxy: columnas y lectura operativa

Columna	Qué representa
Name	Identificador o interfaz de la instancia del proxy.
Type	Función de la instancia: Upstream o Downstream.
Values	Valores y condiciones asociados, tales como redes y parámetros que corresponda mostrar.
Description	Texto administrativo para distinguir la finalidad de una entrada.
Actions	Controles para administrar entradas existentes: edición o eliminación según versión.
Add	Abre el formulario para añadir una instancia al servicio.

47.9. Add: formulario de creación de una instancia

Netgate documenta los campos Interface, Description, Type, Threshold y Networks, además del control Add Network. Estos campos se presentan en el formulario de creación al utilizar Add, no en la tabla de resumen de instancias. Los nombres pueden variar ligeramente según la versión de pfSense Plus instalada.

47.10. Formulario Add: Interface

Interface permite elegir la interfaz lógica por la que se comunicará el proxy para la instancia. La selección debe corresponder a la zona real de origen o de receptores. En entornos con VLAN, el puerto físico y la VLAN lógica no son equivalentes: revisar el etiquetado y las reglas existentes antes de asociarlos al proxy.

47.11. Formulario Add: Type — Upstream

Upstream indica el lado que comunica con las fuentes multicast disponibles. El servicio solamente admite una instancia upstream. No elegir automáticamente la WAN por su nombre: la fuente puede encontrarse en otra interfaz interior o en una red especializada. La elección es lógica y depende del recorrido que sigue el tráfico.

47.12. Formulario Add: Type — Downstream

Downstream designa una o varias interfaces donde hay clientes que solicitan recibir grupos. Se necesita al menos una entrada downstream. Cuando existen varias redes receptoras, es posible definir las instancias apropiadas, siempre que el modelo de distribución sea compatible y se controle el alcance del tráfico permitido.

REQUISITO DOCUMENTADO Para una configuración funcional debe existir una única interfaz Upstream y como mínimo una Downstream. Si la arquitectura exige varias fuentes ascendentes complejas o enrutamiento multicast avanzado, evaluar soluciones específicas antes de forzar el uso del proxy.

47.13. Formulario Add: Description

Description es una anotación de propósito administrativo. Utilizar una etiqueta genérica y funcional, sin nombres reales, IP internas ni datos operativos. Una descripción eficaz indica la dirección de flujo o la función técnica, por ejemplo «Origen multicast» o «Receptores de laboratorio».

47.14. Formulario Add: Threshold — criterio TTL

Threshold establece el umbral TTL de los datos reenviados a través de la interfaz. La documentación de Netgate indica que los paquetes con TTL inferior al umbral se ignoran y que, si el campo se deja en blanco, el valor predeterminado es 1. No confundir este umbral con una reserva de ancho de banda ni con una prioridad de QoS.

El TTL disminuye al atravesar saltos de enrutamiento. Si el emisor impone un TTL reducido, el flujo puede no cruzar el firewall aunque la membresía y las reglas sean correctas. Un umbral excesivo puede impedir tráfico legítimo: documentar el valor elegido y probar con capturas del paquete real.

47.15. Formulario Add: Networks y Add Network

Networks admite una lista de entradas de red en formato CIDR que delimita las subredes cuyo tráfico multicast se permite gestionar en la instancia. Add Network incorpora filas adicionales. Los valores deben corresponder al diseño real; no hay que confundir una dirección de grupo multicast con una subred IPv4 origen o con una máscara de dirección de interfaz.

En ejemplos y esquemas se emplean direcciones de prueba de RFC 5737; no representan ni sugieren la red utilizada por ningún organismo. En un entorno operativo se comprueba qué redes identifica la fuente y cuáles son los prefijos esperados por el proxy y el equipo de acceso.

47.16. Guardar, editar o eliminar una instancia

01. Abrir Services → IGMP Proxy y examinar si existen instancias en el listado.
02. Pulsar Add y elegir Interface, Type, Description, Threshold y Networks conforme al diseño.
03. Guardar la instancia y comprobar que se muestra con el tipo esperado.

04. Completar la pareja Upstream/Downstream antes de habilitar el servicio global.
05. Activar Enable, guardar y verificar el estado del servicio y los flujos.
06. Para modificar una red o interfaz, editar la entrada, guardar y repetir la comprobación funcional.
07. Para retirar una instancia, confirmar primero que no depende de ella un servicio en funcionamiento y disponer de reversión.

47.17. Esquema de señalización IGMP y transporte de datos



Figura 47.2. IGMP controla la membresía; el caudal de aplicación multicast circula por separado.

Los paquetes IGMP utilizan el número de protocolo IP 2; no tienen un puerto TCP o UDP para abrir. La transmisión audiovisual que utilizan aplicaciones multicast suele ser UDP hacia direcciones de grupo. Es habitual que los dos tipos de paquete necesiten permisos y comprobaciones diferentes.

47.18. Reglas de firewall imprescindibles en el downstream

Netgate exige una regla en la interfaz downstream que permita el tráfico IGMP. En Advanced Options de dicha regla debe activarse Allow packets with IP Options, ya que los paquetes de control multicast pueden contener opciones IP que el filtrado descartaría de otra forma. La regla debe limitarse a las fuentes y destinos pertinentes; no conviene sustituirla por un permiso general sin justificación.

01. Identificar la interfaz downstream donde se reciben las solicitudes IGMP de los clientes.
02. Abrir Firewall → Rules en dicha interfaz y crear o revisar una regla Pass adecuada para IGMP.
03. Revisar Address Family = IPv4 y seleccionar el protocolo IGMP cuando esté disponible.
04. En las opciones avanzadas de la regla, activar Allow packets with IP Options.
05. Verificar orden, interfaces, fuentes y destinos; aplicar los cambios.
06. Repetir la captura de solicitudes de membresía y revisar el registro del firewall.

47.19. Tráfico UDP multicast y reglas adicionales

Permitir IGMP no autoriza automáticamente el contenido multimedia. Si las reglas impiden la llegada del flujo UDP multicast, deben establecerse permisos ajustados al origen esperado, grupo multicast, protocolo y, cuando proceda, puertos de aplicación. Los paquetes de datos también pueden verse afectados por políticas de enrutamiento, origen, interfaces WAN o filtros del conmutador. La entrada y salida de multicast deben evaluarse de forma independiente.

SEGURIDAD No permitir sin criterio todo 224.0.0.0/4 ni todo el tráfico UDP entre interfaces. Documentar la fuente, el grupo, la necesidad operativa y quién puede suscribirse.

47.20. IGMP Proxy, IGMP Snooping y enrutamiento multicast

Tecnología	Dónde actúa	Qué resuelve
IGMP Proxy	Interconexión de redes IP por un equipo que conoce upstream y downstream.	Aproxima la membresía de clientes entre segmentos en un diseño sencillo.

Tecnología	Dónde actúa	Qué resuelve
IGMP Snooping	Switch Ethernet, normalmente en capa 2.	Evita inundar indiscriminadamente puertos sin receptores interesados.
PIM / daemon de routing multicast	Routers con topologías y árboles multicast más complejos.	Enrutamiento multicast avanzado para redes de mayor escala.
Bridge	Mismo dominio de capa 2.	Comparte difusión sin resolver necesariamente el problema entre subredes.

La documentación oficial de Netgate identifica el paquete PIMD como alternativa que asume funciones de enrutamiento multicast cuando las necesidades exceden al IGMP Proxy integrado. IGMP Snooping no sustituye al proxy y una mala configuración del conmutador puede impedir el flujo aunque pfSense esté configurado correctamente.

47.21. Relación con IPv4 e IPv6: IGMP frente a MLD

IGMP se utiliza para membresía multicast IPv4. En IPv6 se emplea Multicast Listener Discovery (MLD) y su tratamiento no es equivalente a activar IGMP Proxy. No se debe presentar este servicio como una solución genérica para distribuir multicast IPv6. Diseñar el manejo de IPv6 de manera específica si el proyecto lo exige.

47.22. Limitaciones: multidifusión local y servicios de descubrimiento

Los mecanismos de descubrimiento mDNS y SSDP utilizan direcciones multicast particulares, pero su propagación entre redes puede estar restringida por el ámbito, el TTL, la aplicación y las reglas. No debe suponerse que IGMP Proxy resolverá por sí solo Bonjour, impresión automática, DLNA o descubrimiento de dispositivos. Netgate documenta herramientas distintas, como UDP Broadcast Relay, para determinados casos de descubrimiento entre subredes.

47.23. Aplicación práctica: distribución de vídeo multicast

Un equipo de laboratorio envía un flujo a un grupo IPv4 administrativamente delimitado. El firewall comunica el segmento de fuente upstream con una LAN de receptores downstream. El objetivo es que el tráfico se distribuya cuando un cliente solicite el grupo, conservando el aislamiento de otros servicios y una política de firewall restrictiva.

01. Inventariar origen multicast, grupo utilizado, TTL del emisor y red donde están los receptores.
02. Comprobar que la fuente emite tráfico hacia el grupo y que el enlace upstream lo transporta.
03. Definir la instancia upstream y su lista de redes autorizadas.
04. Añadir una instancia downstream para la red de receptores.
05. Configurar las reglas necesarias para IGMP, IP Options y datos multicast.
06. Habilitar IGMP Proxy y comprobar inicio del proceso.
07. Solicitar el grupo desde un cliente de prueba, medir la recepción y retirar la suscripción.

47.24. Aplicación práctica: clientes en varias VLAN

En una arquitectura con receptores distribuidos entre varias VLAN, cada segmento receptor requiere una evaluación independiente: dirección IP, filtrado, rutas, aislamiento, características del switch y permisos de los equipos. El uso de múltiples entradas downstream no transforma automáticamente el proxy en un sistema de enrutamiento multicast complejo.

47.25. Aplicación práctica: IPTV suministrada por un operador

La entrega IPTV puede depender de VLAN específicas, controles del operador, asignación de direcciones, membresía IGMP, multicast de datos y restricciones de routers o switches. El proxy debe conectarse al segmento de origen correcto, pero no sustituye a los requisitos de la línea contratada. Comprobar el modelo de recepción, el terminal y las características de la red de acceso sin copiar parámetros particulares de ningún proveedor.

47.26. Verificación funcional: pruebas mínimas de aceptación

Componente	Prueba	Resultado esperado
Servicio	IGMP Proxy habilitado y proceso en ejecución.	No se observan errores de arranque.
Origen	Capturar flujo IPv4 multicast en upstream.	El emisor transmite el grupo esperado.
Membresía	Capturar IGMP en downstream al unirse un cliente.	Se ve la solicitud de pertenencia.
Firewall	Verificar Pass/IGMP e IP Options.	No existen bloqueos inesperados.
Datos	Capturar datos multicast en downstream.	El cliente recibe la carga de la aplicación.
Retirada	Dejar de solicitar el grupo.	Se reduce o cesa el envío según el comportamiento del sistema.

47.27. Diagnóstico de paquetes mediante la interfaz web

Diagnostics → Packet Capture ofrece capturas sobre la interfaz de entrada y la de salida. Es útil capturar IGMP en el lado downstream y, en paralelo o de forma sucesiva, los datagramas multicast en upstream y downstream. El paquete puede verse al llegar a una interfaz incluso cuando una regla posterior impide su tránsito; correlacionar siempre captura y firewall log.

01. En la GUI, abrir Diagnostics → Packet Capture y elegir la interfaz downstream.
02. Usar un filtro de protocolo IGMP cuando esté disponible; si el selector no lo ofrece, revisar las opciones de filtro personalizadas.
03. Generar la solicitud desde un cliente y comprobar aparición de mensajes IGMP.
04. Cambiar a la interfaz upstream y filtrar por el grupo multicast de la prueba.
05. Repetir en downstream para confirmar la salida del flujo de datos.
06. Comparar TTL, grupo, tráfico presente y posibles bloqueos en los registros.

47.28. Diagnóstico avanzado con tcpdump

Cuando se dispone de consola administrativa autorizada, tcpdump facilita filtros precisos. En ejemplos genéricos, «interfaz_de_prueba» es un marcador conceptual, no un nombre real de interfaz; debe sustituirse por el identificador local después de comprobar Interfaces → Assignments. Ejecutar capturas de duración limitada para no consumir recursos.

Filtro orientativo	Objetivo
tcpdump -ni interfaz_de_prueba igmp	Observar informes, consultas y señalización IGMP.
tcpdump -ni interfaz_de_prueba multicast	Observar tráfico enviado a direcciones multicast.
tcpdump -ni interfaz_de_prueba host 239.20.30.40	Filtrar un grupo IPv4 de ejemplo; confirmar sintaxis en el entorno de pruebas.
tcpdump -ni interfaz_de_prueba udp	Analizar la carga habitual cuando la aplicación emplea UDP.

47.29. Registros, estado del servicio y supervisión

Revisar los registros del subsistema Routing en Status → System Logs, donde Netgate incluye igmpproxy. Si se necesita más contexto activar temporalmente Verbose Logging y adecuar el nivel global de eventos. Complementar con el registro de firewall, gráficos de interfaces, contadores y medidas del switch. Una ausencia de mensajes no demuestra que el servicio funcione, del mismo modo que una captura de IGMP no confirma entrega de vídeo.

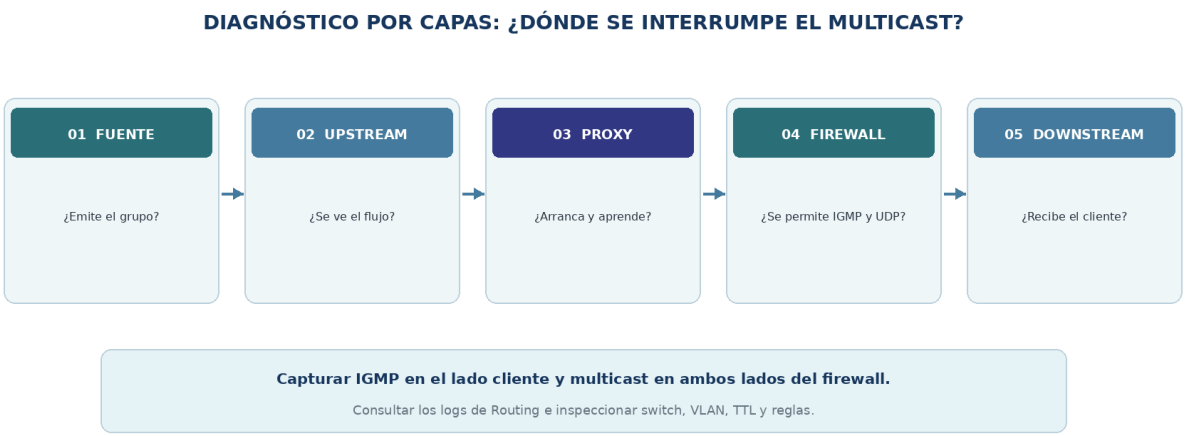


Figura 47.3. Secuencia de diagnóstico entre emisor, upstream, proxy, reglas y receptor.

47.30. Problemas frecuentes: matriz de causas y soluciones

Síntoma	Causa posible	Comprobación recomendada
No arranca	Falta upstream/downstream o entrada inválida.	Revisar instancias, interfaces y log Routing.
No hay IGMP en LAN	Cliente no se suscribe o switch filtra.	Capturar tráfico en puerto/VLAN de receptor.
IGMP visible, sin datos	Sin fuente, reglas, TTL o ruta incorrecta.	Captura upstream/downstream y firewall log.
Vídeo entrecortado	Pérdidas, congestión, multicast flooding o equipo limitado.	Revisar caudal, drops y snooping.
Funciona en una VLAN y no otra	Política o VLAN incoherente.	Ver reglas y conectividad por cada segmento.
Sólo falla tras un cambio	Regla, interfaz, switch o ruta alterados.	Comparar respaldo y revertir por fases.

47.31. TTL, filtros de switches y bucles de red

El TTL bajo puede impedir que el flujo alcance un destino después de cruzar un router. A su vez, los filtros multicast, el snooping mal configurado y la ausencia de querier cuando el diseño lo necesita pueden causar interrupciones que no se solucionan modificando pfSense. Evitar bucles de capa 2 y comprobar STP/switching por separado; IGMP Proxy no es un mecanismo de prevención de bucles.

47.32. Multicast, consumo de ancho de banda y rendimiento

A diferencia del unicast repetido por cliente, el multicast optimiza la transmisión de una fuente a un grupo, pero una suscripción excesiva, una tabla de snooping incorrecta o un switch que inunda puertos pueden elevar el tráfico agregado. Vigilar interfaces, memoria, CPU y errores de enlace, así como la capacidad real del proveedor. No asignar QoS genérica sin conocer la aplicación, su tasa y sus tolerancias.

47.33. Política de seguridad y segmentación

- Permitir únicamente los grupos, orígenes y redes de receptores exigidos por la operación.
- Evitar el reenvío indiscriminado hacia interfaces externas o segmentos sensibles.
- Registrar la justificación de cada permiso IGMP y UDP multicast, junto con el responsable.
- Realizar pruebas en un receptor controlado antes de abrir nuevas VLAN.
- Mantener los cambios reversibles y utilizar backups de configuración apropiados.
- Comprobar los efectos colaterales sobre servicios que también utilizan multicast local.

47.34. Plan de cambio y reversión segura

01. Registrar el estado previo de Enable, Verbose Logging, instancias y reglas afectadas; hacer respaldo.
02. Identificar una ventana de mantenimiento y un equipo de prueba representativo.

03. Introducir una instancia cada vez, empezando por la fuente upstream y los receptores downstream.
04. Aplicar reglas específicas, activar el servicio y comprobar recepción.
05. En caso de degradación, desactivar temporalmente el servicio o revertir instancias y reglas según el plan.
06. Confirmar que el comportamiento previo y los servicios empresariales no relacionados se han recuperado.

47.35. Matriz final de validación profesional

Control	Criterio de aceptación	Evidencia
Arquitectura	Un upstream y al menos un downstream correctos.	Listado y revisión del diseño.
Membresía	Solicitud IGMP observada en red de receptores.	Captura limitada y documentada.
Datos	Tráfico multicast permitido y visible en el destino.	Captura en ambas interfaces.
Seguridad	Reglas específicas, IP Options y alcance revisado.	Revisión de reglas y logs.
Rendimiento	Caudal y pérdidas dentro del objetivo del servicio.	Medidas de switch y firewall.
Reversión	Respaldo y pasos de retorno ensayados.	Registro de cambio.

47.36. Glosario técnico

Término	Significado
IGMP	Internet Group Management Protocol: control de membresía multicast IPv4.
IGMP Proxy	Servicio que aproxima membresía y distribución multicast entre redes.
Upstream	Interfaz del lado de las fuentes de tráfico multicast.
Downstream	Interfaz del lado de clientes interesados en grupos.
TTL	Time to Live: límite IPv4 que se reduce con los saltos de red.
Snooping	Inspección de mensajes IGMP por switches para optimizar puertos de entrega.
Querier	Equipo que formula consultas de membresía IGMP en un segmento.
MLD	Control de membresía multicast en redes IPv6.
PIM	Familia de protocolos de enrutamiento multicast avanzado.
IP Options	Opciones de cabecera IPv4 que requieren tratamiento específico en ciertas reglas.

47.37. Plantilla de revisión de una incidencia multicast

Para que una incidencia pueda investigarse y repetirse, registrar la hora, la versión de pfSense Plus, el síntoma del receptor, el grupo multicast de prueba y los puntos donde hay evidencia del flujo. En el informe operativo interno pueden conservarse los valores autorizados, pero no se deben transferir a documentos destinados a publicación.

Fase	Pregunta clave	Acción ante fallo
Recepción del origen	¿Existe UDP multicast en el segmento upstream?	Confirmar emisión y puertos de acceso antes de cambiar reglas.
Señalización	¿Aparecen joins IGMP desde los receptores?	Revisar cliente, snooping, querier y VLAN downstream.
Proxy	¿El proceso está activo y tiene instancias válidas?	Inspeccionar configuración y log Routing.

Fase	Pregunta clave	Acción ante fallo
Filtrado	¿La regla IGMP permite IP Options?	Corregir permisos de forma restringida.
Transporte	¿El mismo grupo aparece al salir por downstream?	Comprobar TTL, reglas, switch y multicast de datos.
Experiencia	¿La aplicación recibe sin pausas ni pérdidas?	Medir caudal, latencia, errores y congestión.

47.38. Compatibilidad del formulario y variaciones de versión

La página principal separa las opciones globales Enable y Verbose Logging del inventario de instancias. El formulario Add incorpora Interface, Description, Type, Threshold y Networks, con Add Network para ampliar la lista. La disposición exacta, las acciones de las filas y los textos de ayuda pueden cambiar entre versiones de pfSense Plus; comprobarlos siempre antes de aplicar un procedimiento operativo.

47.39. Lista de control antes de producción

- Se ha comprobado que el origen emite el grupo esperado y que existe exactamente un upstream.
- Cada red receptora autorizada dispone de una instancia downstream y de reglas coherentes.
- IGMP se permite con IP Options cuando es necesario, sin abrir flujos ajenos.
- El multicast de datos atraviesa las interfaces previstas con TTL suficiente.
- Se han verificado las VLAN y el tratamiento de IGMP Snooping en los switches.
- El procedimiento de reversión conserva un acceso administrativo independiente del servicio.

47.40. Ficha de despliegue: elementos que deben quedar documentados

La ficha de operación de un servicio multicast debe permitir que otro administrador pueda comprobar su funcionamiento sin conocer detalles privados. Antes de implantar, documentar internamente las características de origen y destino y conservar aquí únicamente el esquema de comprobaciones:

Elemento	Verificación requerida
Fuente multicast	Aplicación de origen, dirección de grupo y tasa nominal del flujo.
Red upstream	Interfaz lógica correcta; conectividad con la fuente y políticas de acceso.
Red downstream	Segmentos receptores, reglas IGMP, permisos de datos y aislamiento.
Conmutación	Compatibilidad de IGMP Snooping, querier y VLAN entre equipos.
Calidad	Pérdida de paquetes, latencia, variación de retardo y estabilidad de vídeo.
Soporte	Procedimiento de captura y ubicación de registros de servicio.
Reversión	Acceso administrativo, respaldo previo y pasos de retorno comprobados.

47.41. Buenas prácticas de mantenimiento periódico

La monitorización no debe limitarse a verificar que el proceso está activo. Conviene solicitar periódicamente un flujo controlado, observar si el número de receptores cambia como se espera y revisar las interfaces con más tráfico multicast. Tras modificar reglas, puertos de switch, VLAN o firmware, repetir al menos una prueba upstream/downstream y comprobar que no se producen inundaciones de tráfico en otros segmentos.

47.42. Referencias oficiales de Netgate y estándares

- Netgate — IGMP Proxy: configuración del servicio
- Netgate — Configuring Firewall Rules: IP Options
- Netgate — Routing Logs: igmpproxy

- Netgate — Packet Capture GUI
- Netgate — Using tcpdump on the command line
- Netgate — PIMD in Package List
- Netgate — UDP Broadcast Relay
- IETF — RFC 2236: IGMPv2
- IETF — RFC 3376: IGMPv3
- IETF — RFC 2365: Administratively Scoped IP Multicast

48 Services → NTP

Settings · ACLs · Serial GPS · PPS · Seguridad y diagnóstico

La sincronización horaria mantiene coherentes los registros, los certificados, las autenticaciones y la correlación de eventos de red. Este capítulo describe las cuatro pestañas del servicio NTP de pfSense Plus, con criterios para configurar fuentes fiables, restringir el acceso, utilizar relojes de referencia y comprobar la calidad de la sincronización.

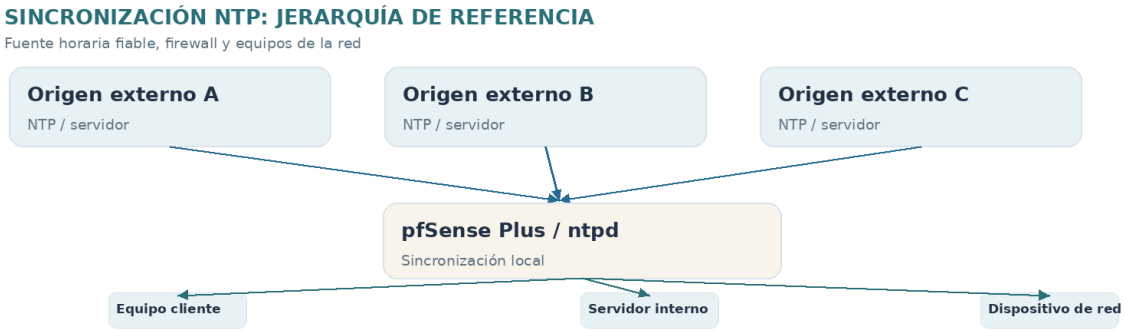


Figura 48.1. Modelo general de obtención, disciplina y distribución de tiempo.

48.1. Finalidad del servicio y aplicaciones empresariales

El servicio NTP (Network Time Protocol) permite que pfSense Plus sincronice su propio reloj con fuentes externas y, cuando está habilitado, atienda consultas de clientes de la red. Centralizar la hora facilita el análisis cronológico de registros de firewall, VPN, autenticación, servidores, sistemas de control y monitorización. Una hora incorrecta puede invalidar certificados, alterar la evaluación de eventos y dificultar investigaciones de incidencias.

48.2. Conceptos técnicos que conviene distinguir

Concepto	Significado operativo	Interpretación
UTC / zona horaria	NTP transmite referencias temporales; la presentación local depende de la zona horaria.	La zona horaria se configura por separado bajo System → General Setup.
Stratum	Posición en la jerarquía respecto de la fuente de referencia.	No sustituye a indicadores de precisión, latencia ni estabilidad.
Offset	Desviación estimada entre el reloj local y una fuente.	Buscar valores bajos y estables, no un único valor aislado.
Delay / Jitter	Retardo de ida y vuelta y variación de medidas.	Suelen aumentar con congestión o rutas inestables.
Reach	Registro octal de respuestas recientes del peer.	Permite detectar pérdidas y falta de disponibilidad.
PPS	Impulso por segundo para ajustar el instante temporal.	No aporta fecha ni hora por sí solo.

48.3. Ruta y estructura de la pantalla

Ruta principal: Services → NTP. El módulo presenta las pestañas Settings, ACLs, Serial GPS y PPS. Settings gestiona el servicio y sus fuentes horarias; ACLs controla las operaciones permitidas a los clientes; Serial GPS incorpora un receptor compatible como reloj de referencia; y PPS permite emplear una fuente física de pulsos. Las opciones concretas pueden variar ligeramente según versión, controlador o hardware disponible.

48.4. Settings: Enable NTP Server

Enable NTP Server activa el demonio ntpd y permite la sincronización horaria del sistema y la atención de solicitudes NTP según los enlaces configurados. Desactivar la opción detiene el servicio ntpd: deja de proporcionar hora a los clientes que dependan de él y puede cambiar el método de disciplina del reloj del firewall. No equivale a desactivar todos los mecanismos de puesta en hora durante el arranque del sistema.

ATENCIÓN Si el firewall es la referencia NTP de servidores, equipos de seguridad o redes aisladas, deshabilitar el servicio sin alternativa validada puede producir pérdida de sincronía y errores de autenticación o certificados.

48.5. Settings: Interface y direcciones de escucha

Interface limita las interfaces en las que ntpd acepta consultas. No aparecen las interfaces sin dirección IP. Según la descripción del formulario, sin ninguna seleccionada se escucha mediante comodín en todas; seleccionar todas las interfaces las vincula explícitamente. Netgate advierte de que la selección también puede afectar a las direcciones de origen utilizadas para consultar servidores remotos: no es solo un filtro de clientes. En una red empresarial conviene ofrecer NTP en las interfaces internas necesarias y controlar además UDP/123 con reglas y ACLs.

48.6. Settings: Time Servers y tipos Server, Pool y Peer

Time Servers permite introducir los orígenes temporales: nombres DNS o direcciones de servidores. Server define un servidor individual; Pool solicita varios candidatos de un conjunto; Peer expresa una asociación de pares con comportamiento NTP simétrico y debe reservarse a diseños que lo requieran. El botón Add incorpora otra entrada. Los servidores iniciales pueden proceder de System → General Setup; esta dependencia debe verificarse antes de realizar cambios.

Campo/Tipo	Qué modifica	Criterio profesional
Server	Un destino concreto de sincronización.	Adecuado para referencias internas controladas.
Pool	Una agrupación de candidatos resueltos dinámicamente.	Reduce dependencia de una sola IP; respetar límites de uso.
Peer	Asociación entre pares NTP.	Usar solo en diseños planificados para evitar bucles o fuentes indeseadas.
Add	Añade otra fila de fuente.	Revisar redundancia, independencia y DNS.
Authenticated	Marca fuentes sometidas a autenticación cuando el esquema de claves es compatible.	Configurar y verificar la clave, el identificador y el algoritmo según la versión disponible.

48.7. Settings: Prefer y No Select

Prefer indica una preferencia por una fuente frente a otras candidatas aceptables; no convierte una fuente inválida en válida. No Select impide emplear esa entrada para disciplinar el reloj, aunque conserva datos para análisis estadístico. Son opciones de uso especializado: No Select es particularmente útil para comparar una fuente antes de confiar en ella.

48.8. Settings: selección de fuentes y regla de mayoría

NTP compara distintas fuentes para detectar valores inconsistentes; una sola fuente utilizable no ofrece verificación independiente. El formulario recomienda normalmente tres a cinco fuentes fiables o un pool. Si solo existe una, puede ser aceptada; dos fuentes que discrepan pueden quedar sin selección. Seleccionar preferentemente fuentes independientes (red y administración) reduce fallos correlacionados, pero no conviene multiplicar de forma indiscriminada las consultas a pools públicos.

48.9. Settings: Max candidate pool peers

Max candidate pool peers fija el número máximo de candidatos obtenidos de pools. El valor mostrado como predeterminado es 5. Un límite muy bajo reduce la reserva disponible; uno demasiado alto incrementa

conexiones, mensajes y carga sobre servidores públicos, muchos mantenidos por voluntariado. Mantener el valor predeterminado suele resultar adecuado para instalaciones generales.

48.10. Settings: Orphan Mode

Orphan Mode permite seguir prestando servicio basado en el reloj local cuando se pierden todas las referencias utilizables. El número define el stratum anunciado durante ese estado; el valor documentado habitual es 12 para que los clientes prefieran otras referencias disponibles de mejor calidad. Es una medida de continuidad, no una garantía de exactitud: el reloj local puede derivar con el tiempo.

ATENCIÓN Orphan Mode no sustituye a Internet, un GPS válido o una referencia temporal real. Documentar el tiempo máximo tolerable sin fuentes externas antes de confiar en él.

48.11. Settings: Minimum y Maximum Poll Interval

Los intervalos regulan cuánto puede espaciar ntpd sus consultas. La lista del formulario emplea exponentes en base 2: 3 equivale a 8 s; 6, a 64 s; 10, a 1.024 s; y 17, a 131.072 s. Minimum Poll Interval nunca puede superar a Maximum Poll Interval. Default delega el criterio en los valores del servicio; Omit evita fijar el parámetro explícitamente. Intervalos demasiado breves elevan las solicitudes; demasiado largos pueden reducir la capacidad de seguir cambios de la fuente.

Exponente	Intervalo	Lectura
3	8 s	Sondeo muy corto; excepcional.
4	16 s	Sondeo corto.
5	32 s	Sondeo corto.
6	64 s	Poco más de un minuto.
7	128 s	2 min 8 s.
8	256 s	4 min 16 s.
9	512 s	8 min 32 s.
10	1.024 s	17 min 4 s.
11	2.048 s	34 min 8 s.
12	4.096 s	1 h 8 min 16 s.
13	8.192 s	2 h 16 min 32 s.
14	16.384 s	4 h 33 min 4 s.
15	32.768 s	9 h 6 min 8 s.
16	65.536 s	18 h 12 min 16 s.
17	131.072 s	1 día 12 h 24 min 32 s.

48.12. Settings: NTP Graphs

NTP Graphs habilita gráficos RRD de estadísticas como offset, jitter, dispersión y estabilidad del reloj. Su valor predeterminado aparece desactivado. Es útil durante el ajuste y la monitorización prolongada, aunque consume almacenamiento y recursos de escritura. Conviene definir si la organización necesita tendencias históricas o basta con la información en tiempo real de Status → NTP.

48.13. Settings: Logging — mensajes de peers y del sistema

Log peer messages registra variaciones en relaciones y estados de fuentes; Log system messages añade eventos operativos del demonio. Ambos aparecen normalmente desactivados y se consultan en Status → System Logs → NTP, siempre que el nivel de logging permita visualizar los mensajes. Activarlos de manera selectiva facilita el diagnóstico, pero no es recomendable convertir el registro detallado en una fuente de ruido permanente.

48.14. Settings: Statistics Logging

Statistics Logging abre opciones avanzadas para generar archivos diarios persistentes en /var/log/ntp. Los controles documentados permiten registrar estadísticas de la referencia (clockstats), disciplina del reloj (loopstats) y peers (peerstats). Son especialmente útiles al investigar pérdidas de sincronía, oscilaciones u offsets recurrentes, pero deben acompañarse de una política de retención y vigilancia de espacio libre.

Opción avanzada	Registra	Uso
Reference clock statistics	Mediciones del reloj de referencia.	Ajustes finos de GPS u otras fuentes locales.
Clock discipline statistics	Variación y correcciones aplicadas al reloj.	Investigación de deriva y estabilidad.
NTP Peer Statistics	Información temporal y de calidad por peer.	Comparación entre fuentes externas.

48.15. Settings: Leap Seconds y archivo de corrección

Leap Seconds permite definir un archivo de segundos intercalares para ntpd. La corrección se administra internacionalmente y puede anunciarse en junio o diciembre, pero no se produce automáticamente todos los años. La documentación de Netgate recomienda emplear un fichero fiable y vigente, especialmente si se opera con referencias de stratum 1 o aplicaciones sensibles al tiempo. Debe evitarse cargar información caducada o improvisada; el archivo publicado por IANA/IERS puede actualizarse y expirar periódicamente.

48.16. Settings: DNS Resolution

DNS Resolution ofrece Auto, IPv4 e IPv6 para orientar cómo se resuelven las fuentes NTP definidas por nombre. Auto permite la elección habitual; forzar IPv4/IPv6 puede ser útil ante incidencias de conectividad específicas, teniendo en cuenta que el texto del formulario advierte que esta restricción no afecta necesariamente del mismo modo a las entradas de tipo Pool. Antes de cambiar este ajuste conviene comprobar resolución DNS y rutas en la familia IP seleccionada.

48.17. Settings: Enable NTP Server Authentication

Enable NTP Server Authentication activa autenticación simétrica NTPv3 (RFC 1305) para escenarios con clientes compatibles. En la configuración adicional documentada aparecen la Authentication Key y el Digest Algorithm; estos datos deben coincidir con los de los clientes configurados para comprobar la identidad de la fuente. La edición concreta y los algoritmos ofrecidos dependen de la versión; no conviene inventar una selección que no aparezca en el equipo. Esta autenticación clásica no equivale a NTS (Network Time Security) ni ofrece cifrado general del tráfico horario.

RECOMENDACIÓN Guardar las claves en un gestor seguro, restringir permisos y ensayar compatibilidad antes de exigir autenticación a clientes críticos. No incluir secretos reales en documentación operativa ni en capturas.

48.18. ACLs: objetivo y relación con las reglas de firewall

ACLs aplica restricciones internas de ntpd a consultas o asociaciones procedentes de clientes y redes. Las reglas del firewall controlan si llega UDP/123; las ACLs deciden qué tipos de solicitudes se atienden una vez alcanzado el servicio. Para un control completo deben configurarse conjuntamente. Las restricciones por defecto se aplican a clientes que no tengan una política más específica.

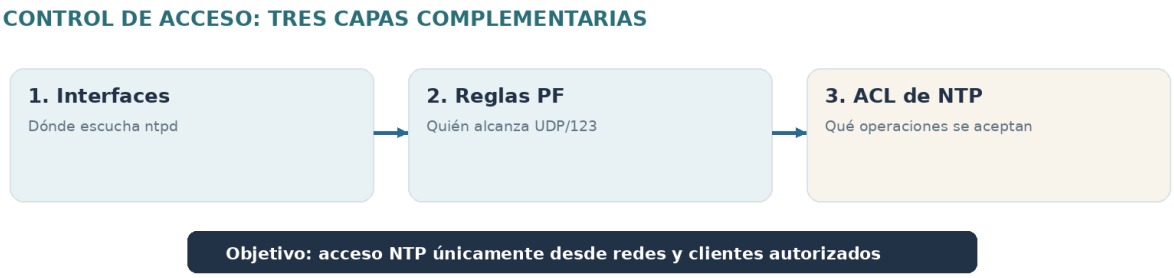


Figura 48.2. Interfaces, filtrado PF y restricciones propias del servicio NTP.

48.19. ACLs: Default Access Restrictions

Default Access Restrictions agrupa controles aplicables de modo general. Importante: las casillas de restricción no significan permitir, sino denegar la clase de operación especificada, con la excepción del comportamiento de respuesta Kiss-o'-Death. Una política restrictiva debe probarse primero desde la red de administración para evitar perder visibilidad sobre Status → NTP.

48.20. ACLs: seis controles documentados

Control	Resultado al activarlo	Precaución
Kiss-o'-Death	Emite respuestas de control KoD cuando se produce una infracción; su frecuencia está limitada.	Puede informar al cliente de que debe reducir el tráfico.
Modifications	Deniega operaciones de ntpq/ntpdc que intentan modificar configuración.	Suele ser adecuado bloquear cambios remotos.
Queries	Deniega las consultas de control ntpq/ntpdc.	Puede dejar sin funcionar Status → NTP al usar ntpq.
Service	Deniega paquetes salvo consultas de control ntpq/ntpdc.	Bloqueará sincronización ordinaria de clientes.
Peer Association	Deniega nuevas asociaciones de pares no autorizadas.	Útil contra relaciones de sincronización indeseadas.
Trap Service	Deniega el servicio de traps de control remoto.	No confundir con eventos syslog locales.

48.21. ACLs: Custom Access Restrictions, Network/Mask y Restrictions

Custom Access Restrictions permite aplicar políticas a redes concretas mediante Add. Network/Mask contiene la dirección de red y máscara correspondiente; Restrictions ofrece los mismos controles que Default Access Restrictions en formato abreviado. La tabla de restricciones debe tratarse como una política de acceso NTP, no como una lista de subredes con permiso automático. Para redes de terceros y VLAN sensibles, permitir solo la sincronización necesaria y bloquear controles administrativos.

48.22. ACLs: política recomendada para una red empresarial

El servicio debería estar disponible únicamente para clientes internos autorizados; los controles remotos de administración y nuevas asociaciones no solicitadas deben limitarse. En WAN, salvo necesidad justificada y protegida, resulta preferible no escuchar ni aceptar solicitudes externas. Si se abre UDP/123 al exterior, existe riesgo de abuso de recursos y uso del servidor en ataques de amplificación cuando la versión y configuración lo permiten.

48.23. Serial GPS: función y requisitos de hardware

Serial GPS admite un receptor GPS que entregue información horaria por puerto serie compatible. Si el dispositivo también dispone de una señal PPS utilizable, puede aportar una referencia de mayor precisión. Netgate indica que los receptores GPS USB pueden funcionar, pero desaconseja utilizarlos como fuente de tiempo de alta calidad por latencias y variabilidad propias de USB. Es recomendable mantener además varias referencias NTP externas independientes.

48.24. Serial GPS: GPS Type, Serial Port y Baud Rate

Campo	Función	Recomendación
GPS Type	Selecciona modelo; Default si se desconoce y Custom para dispositivos no incluidos.	Comprobar documentación del receptor.
Serial Port	Puerto local detectado. En FreeBSD suelen aparecer cuau… o cuaU… para USB.	Comprobar disponibilidad y permisos.
Baud Rate	Velocidad de transmisión del enlace serie.	Ajustarla al dispositivo; 4.800 es habitual en NMEA clásico.

48.25. Serial GPS: NMEA Sentences

NMEA Sentences indica qué frases de datos del receptor se procesan. El comportamiento habitual permite todas las compatibles; se puede limitar el conjunto cuando se conoce el formato válido del dispositivo o se están investigando incoherencias. No es correcto asumir que todas las sentencias contienen información temporal suficiente ni que cualquier GPS NMEA garantiza una referencia estable.

48.26. Serial GPS: Fudge Time 1, Fudge Time 2 y Stratum

Fudge Time 1 añade un ajuste de compensación al PPS del GPS; Fudge Time 2 ajusta el desfase atribuido a la información temporal recibida. Ambos son ajustes finos que deben sustentarse en mediciones, no en valores arbitrarios. Stratum expresa la preferencia asignada a la fuente de referencia en la configuración del driver. La pantalla documenta valor 0 para dar preferencia al GPS; no debe interpretarse como que el servicio ofrecerá automáticamente un stratum 0 válido a los clientes NTP.

48.27. Serial GPS: Flags de referencia y proceso PPS

Flag	Efecto	Cuándo utilizarlo
Prefer this clock	Favorece la fuente GPS si es aceptable.	Receptor estable y validado.
Do not use this clock	Solo recoge estadísticas, no sincroniza.	Fase de observación y ensayo.
PPS signal processing	Procesa PPS disponible en el driver GPS.	Solo con salida física PPS compatible.
Falling edge PPS	Emplea el flanco descendente en lugar del ascendente.	Cuando así lo especifica el diseño eléctrico.
Kernel PPS discipline	Permite al kernel utilizar PPS directamente.	Requiere soporte y pruebas de precisión.
Obscure location	Oculta la ubicación en datos mostrados.	Privacidad y reducción de exposición.
Log sub-second fraction	Registra fracciones de segundo para ajustes.	Diagnóstico temporal; evitar logs continuados.

48.28. Serial GPS: Clock ID, Initialization y NMEA Checksum Calculator

Clock ID representa un identificador corto de 1 a 4 caracteres; el habitual es GPS. GPS Initialization contiene comandos que deben enviarse al receptor al arrancar; con GPS Type Custom pueden ser indispensables. NMEA Checksum Calculator facilita verificar la suma de comprobación de una secuencia de inicialización NMEA. Una configuración de inicialización errónea puede dejar el receptor sin información utilizable, por lo que se recomienda conservar la cadena funcional anterior.

48.29. PPS: finalidad, límites y diferencias frente a GPS

PPS Source (Non-GPS) permite utilizar una fuente que emite un pulso periódico por segundo, por ejemplo una señal de radio o equipo especializado. PPS sirve para afinar el instante y la estabilidad, pero no

determina la fecha/hora absoluta. Debe combinarse con una fuente temporal que indique qué segundo se está contando. Esta distinción es decisiva al planificar servidores de tiempo aislados.

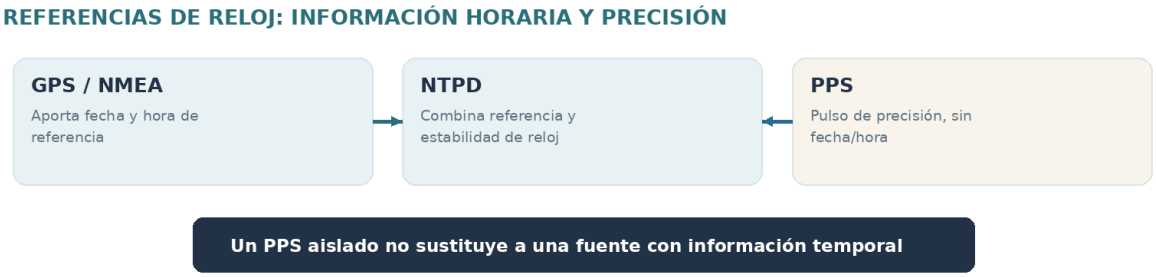


Figura 48.3. La información de hora y los pulsos de precisión cumplen funciones distintas.

48.30. PPS: Serial Port y Fudge Time 1

Serial Port selecciona el puerto físico disponible para los pulsos. Fudge Time 1 introduce un offset constante para compensar el retardo del receptor, cableado o procesamiento. Antes de aplicar un ajuste conviene medir el error medio frente a una fuente confiable y mantener un histórico de las mediciones.

48.31. PPS: Stratum, Flags y Clock ID

Campo u opción	Descripción	Advertencia
Stratum	Preferencia de fuente; predeterminado documentado: 0.	No implica sincronización horaria autónoma.
Falling edge PPS	Sincronización al flanco descendente.	Usar solo cuando la señal corresponde a ese flanco.
Kernel PPS clock discipline	Disciplina de reloj mediante el kernel.	Depende de soporte del sistema y hardware.
Record a timestamp	Registra una marca cada segundo; permite análisis de estabilidad.	Puede aumentar la cantidad de datos recogidos.
Clock ID	Código de 1 a 4 caracteres, típicamente PPS.	Identificador técnico de fuente.

48.32. Procedimiento: puesta en marcha de NTP corporativo

1. Comprobar fecha, zona horaria y resolución DNS bajo System → General Setup; verificar rutas hacia las fuentes.
2. Abrir Services → NTP → Settings, habilitar el servicio y seleccionar las interfaces internas necesarias.
3. Configurar tres a cinco fuentes razonablemente independientes, o un pool fiable sin exceder el máximo de candidatos.
4. Conservar Prefer y No Select sin alterar salvo justificación; revisar Orphan Mode y los intervalos de consulta.
5. Guardar y comprobar en Status → NTP la existencia de una fuente activa, offset, jitter, delay y reach.
6. Permitir UDP/123 solo desde las redes cliente autorizadas; revisar la configuración de ACLs.
7. Configurar clientes internos para consultar la dirección de servicio del firewall y documentar el punto de reversión.

48.33. Procedimiento: asegurar ACLs sin perder observabilidad

1. Identificar los segmentos que requieren servicio y la red de administración que realiza diagnósticos.
2. Verificar que la ruta de acceso administrativa y las reglas de firewall permiten las pruebas desde un equipo controlado.
3. En Services → NTP → ACLs, limitar Modifications, Peer Association y Trap Service según el diseño.

4. Evitar habilitar Queries indiscriminadamente si se necesita Status → NTP; registrar el cambio y probar visibilidad.
5. Crear restricciones por Network/Mask para segmentos concretos y comprobar que los clientes siguen sincronizando.
6. Revisar registros, capturas y estado; revertir el último ajuste si deja sin sincronización o diagnóstico.

48.34. Procedimiento: incorporación de GPS serie

1. Verificar el receptor y su puerto compatible, así como disponibilidad de señal satelital y salida NMEA.
2. Abrir Services → NTP → Serial GPS y seleccionar GPS Type, Serial Port y Baud Rate compatibles.
3. Conservar la selección amplia de NMEA inicialmente; restringir solo tras una prueba y con soporte del fabricante.
4. Mantener inicialmente Fudge Time 1 y 2 sin compensaciones especulativas y no activar flags PPS sin salida comprobada.
5. Guardar y examinar Status → NTP, comparando offset, reach y estabilidad frente a fuentes independientes.
6. Una vez validada la fuente, documentar las correcciones aplicadas y conservar referencias NTP externas de respaldo.

48.35. Procedimiento: referencia PPS externa

1. Confirmar que existe una fuente horaria completa que pueda complementarse con PPS.
2. Conectar la fuente al puerto serie soportado y comprobar señal eléctrica, flanco y compatibilidad de controladores.
3. En Services → NTP → PPS elegir puerto, configurar Clock ID y dejar Fudge Time 1 sin ajuste arbitrario.
4. Activar Kernel PPS o Falling edge únicamente si corresponde al dispositivo y al diseño.
5. Guardar y comprobar el comportamiento en Status → NTP y con estadísticas antes/después.
6. Si el servicio se degrada, desactivar PPS y volver a las referencias NTP previamente validadas.

48.36. Escenarios empresariales de aplicación

Escenario	Diseño general	Riesgo principal
Oficinas y servidores	Firewall sincronizado con pool externo y clientes internos apuntando a NTP local.	Dependencia de un único servidor local.
Red con salida restringida	Fuentes corporativas accesibles por rutas autorizadas; servicio interno controlado.	Bloquear UDP/123 hacia las referencias.
Alta disponibilidad	Dos referencias locales comprobadas con fuentes independientes.	Peering mal diseñado o reloj local en modo huérfano.
Sede sin salida estable	Varias fuentes externas cuando hay enlace y GPS validado si se justifica.	GPS/USB sin precisión y referencia absoluta ausente.
Sistema virtualizado	Revisión de reloj del hipervisor y del invitado; un responsable de disciplina bien definido.	Saltos de tiempo y fuentes en conflicto.

48.37. Verificación: Status → NTP y lectura de indicadores

Status → NTP muestra servidores, tipo de peer, estrato, reference ID, último contacto, intervalos, reach, delay, offset y jitter. No basta con que una fila sea visible: debe haber una fuente activa seleccionada y una tendencia estable. Un peer marcado como Unreach/Pending requiere revisar acceso y comunicaciones; False Ticker u Outlier indican fuentes rechazadas por algoritmos de selección. El estado puede tardar varias consultas en estabilizarse.

Indicador	Interpretación útil	Qué investigar si empeora
Active Peer / Candidate	Fuente empleada o viable como respaldo.	Desaparición de pares fiables.
Reach	Historial octal de recepciones.	Pérdidas, filtrado, rutas, DNS.
Offset (ms)	Desvío temporal estimado.	Saltos de hora, deriva o fuentes dispares.
Jitter (ms)	Variabilidad del offset.	Latencia variable, GPS/USB, carga o temporización.
Stratum	Proximidad lógica a la referencia.	Fuentes no sincronizadas o modo huérfano.

48.38. Diagnóstico: pruebas de red y servicio

Las pruebas deben comenzar por reloj del sistema, DNS y conectividad a las fuentes. Comprobar que UDP/123 está permitido en la ruta, que ntpd escucha en la interfaz prevista y que las ACLs no niegan el servicio. Si se utilizan opciones de autenticación, confirmar compatibilidad de clave y digest. En caso de problemas intermitentes, contrastar logs de NTP, Packet Capture y los contadores de pérdidas antes de modificar las preferencias o intervalos.

```
ntpq -p
ntpq -c rv
```

Los comandos anteriores son referencias de diagnóstico cuando el acceso a la consola y el soporte del demonio lo permitan. Conviene privilegiar Status → NTP y las herramientas gráficas de diagnóstico del firewall, ejecutando comandos con criterio y autorización.

48.39. Errores frecuentes y acciones correctivas

Síntoma	Causas probables	Medida de diagnóstico
No hay fuente válida	DNS, puerta de enlace, UDP/123 o reloj muy desfasado.	Resolver nombres, comprobar ruta, registros y estado.
Cliente sin hora	Interfaz no escuchando, ACL o regla PF.	Ver UDP/123 y restricciones de ntpd.
Status → NTP no muestra información	ACL Queries activa.	Revisar control, revertir con acceso seguro.
Fuentes incompatibles entre sí	Peering incorrecto, servidores defectuosos.	Comparar offsets y descartar fuente no confiable.
GPS sin datos	Puerto serie o baud erróneo, frases NMEA ausentes.	Comprobar receptor, puerto y formato.
PPS sin sincronización	PPS no contiene hora absoluta.	Añadir fuente temporal completa.
Reloj de VM cambia abruptamente	Sincronía host/invitado, migración o contador inestable.	Revisar políticas del hipervisor y eventos.
Logs crecen demasiado	Peer/System/Statistics habilitados continuamente.	Reducir detalle y revisar retención.

48.40. Reloj de virtualización y arranque de pfSense Plus

En una VM, el sistema puede recibir correcciones temporales del hipervisor o de servicios del invitado. Debe existir una política clara y coherente para evitar saltos y luchas entre mecanismos de sincronización. La documentación de Netgate también diferencia el arranque de ntpd del proceso inicial de puesta en hora del firewall: puede haber comprobaciones del reloj y una sincronización puntual antes de iniciar el servicio. La necesidad de habilitar o deshabilitar NTP en una VM se decide según el diseño probado y no de forma automática.

48.41. Seguridad, continuidad y minimización de exposición

La hora precisa afecta a TLS, PKI, VPN, registros y autenticación. Exponer un servidor NTP a redes no confiables sin control facilita consultas abusivas y puede afectar disponibilidad. Restringir interfaces, reglas y ACLs; mantener software actualizado; proteger claves; validar fuentes; y disponer de un plan de funcionamiento cuando no hay acceso a referencias externas. Registrar cualquier modificación de parámetros de reloj con fecha y motivo de cambio.

48.42. Rendimiento, capacidad y registro histórico

Con valores predeterminados adecuados, el consumo de NTP suele ser contenido. Los elementos que más pueden alterar la carga son pools demasiado extensos, intervalos de sondeo excesivamente cortos, generación de estadísticas diarias y registro detallado en exceso. Las mediciones deben comparar el estado en intervalos representativos, no durante unos pocos segundos de la puesta en marcha.

48.43. Matriz profesional de validación y aceptación

Prueba	Resultado esperado	Evidencia a registrar
Fuentes externas	Al menos una activa y alternativas viables.	Status → NTP, lista de peers.
Sincronización cliente	Consulta NTP responde en red autorizada.	Test desde equipo cliente.
Restricción indebida	Red no autorizada no accede al servicio.	Registro o captura controlada.
ACL administrativa	Las modificaciones y asociaciones no autorizadas se bloquean.	Política y prueba autorizada.
Pérdida de WAN	Comportamiento de reloj documentado según tiempo transcurrido.	Prueba planificada, Orphan Mode.
GPS / PPS (si existe)	Referencia estable con datos y señal correctos.	Comparación de offset/jitter.
Reinicio	Sincronía se restablece y evita desvíos prolongados.	Eventos de arranque y estado.

48.44. Procedimiento de reversión ante cambios problemáticos

1. Conservar copia de configuración y registrar valores previos de Settings y ACLs.
2. Si el servicio deja de sincronizar, restaurar fuentes conocidas y accesibilidad de sus interfaces.
3. Revertir cambios recientes de ACLs y firewall de forma controlada, sin abrir indiscriminadamente a WAN.
4. Desactivar temporalmente GPS/PPS o preferencias avanzadas si la fuente nueva es la causa probable.
5. Comprobar Status → NTP y la hora de un cliente de prueba antes de cerrar la incidencia.
6. Documentar causa, solución y evidencia, evitando copiar direcciones o claves en reportes compartidos.

48.45. Glosario técnico

Término	Definición breve
NTP / ntpd	Protocolo y demonio para sincronizar el tiempo.
Pool	Conjunto dinámico de fuentes NTP.
Stratum	Nivel jerárquico de referencia temporal.
Peer	Fuente o par configurado para una relación NTP.
KoD	Kiss-o'-Death: mensaje que informa de una restricción o limitación.

Término	Definición breve
NMEA	Formato frecuente de mensajes de receptores de navegación.
PPS	Pulse Per Second; pulso de precisión por segundo.
Offset / Jitter	Desfase estimado y variabilidad temporal.
ACL	Restricción de comportamiento de las consultas al demonio.

48.46. Auditoría temporal y evidencias para mantenimiento

Una auditoría de NTP no se limita a comprobar que ntpd está activo: debe demostrar la calidad de la fuente, la continuidad del servicio y la consistencia entre dispositivos. Conviene registrar en las ventanas de mantenimiento el origen horario seleccionado, el reach y los offsets de las fuentes, la zona horaria y los sistemas críticos que consumen NTP. La evidencia debe almacenarse con permisos adecuados y sin secretos ni identificadores que no sean imprescindibles.

Evidencia técnica	Frecuencia sugerida	Criterio de revisión
Estado y fuentes NTP	Tras cambios y revisión periódica.	Fuente activa válida; referencias alternativas disponibles.
Reach y pérdidas	Cuando aparecen alarmas o incidencias.	Desaparición de respuestas o pérdidas sostenidas.
Offset y jitter	Línea base y cambios de topología.	Desviaciones crecientes respecto de la normalidad.
ACL y reglas PF	Cambios de segmentos o seguridad.	Ninguna red ajena recibe servicio por error.
Zona horaria y registros	Auditorías y cambios de horario local.	Marcas temporales consistentes entre sistemas.
Prueba de pérdida de fuentes	Ejercicio planificado de continuidad.	Comportamiento de Orphan Mode conocido.

48.47. Validación desde clientes y límites de las pruebas

Desde clientes Windows puede utilizarse w32tm para observar la fuente y la respuesta de un servidor NTP. En Linux y otros sistemas conviene emplear la herramienta de monitorización correspondiente al servicio de tiempo instalado; ntpq solo es adecuado cuando el demonio y los permisos de consulta lo permiten. Una prueba que confirma el puerto UDP abierto no demuestra por sí sola que la hora distribuida sea correcta: también debe compararse la referencia, el offset y la estabilidad.

```
w32tm /stripchart /computer:<SERVIDOR_NTP> /samples:5 /dataonly
```

El marcador <SERVIDOR_NTP> representa una dirección o nombre aprobado para el entorno y no un dato de configuración. No se debe publicar ni modificar en el firewall una IP real para ilustrar la prueba. Si un cliente no se sincroniza, validar primero conectividad y DNS; después, las ACLs y el estado del servicio; finalmente, las políticas de hora específicas del cliente.

48.48. Autenticación de tiempo: alcance y límites de seguridad

La autenticación simétrica NTPv3 de la pantalla usa un secreto compartido y un algoritmo de resumen pactado con el cliente; permite comprobar mensajes compatibles, pero no cifra toda la comunicación y depende de la protección de la clave. NTS (Network Time Security) es otro mecanismo con negociación y seguridad modernas definido en una especificación diferente; no debe suponerse que la casilla NTPv3 Authentication añade NTS, ni presentar NTS como función disponible sin comprobar soporte específico en la versión instalada. Para las redes de alta criticidad, la seguridad horaria requiere una política conjunta de orígenes confiables, segmentación y alertas de deriva.

48.49. Referencias oficiales y material normativo

[R1] Netgate: NTPD — introducción — https://docs.netgate.com/pfsense/en/latest/services/ntpd/index.html

[R2] Netgate: NTP Server Configuration y ACLs — https://docs.netgate.com/pfsense/en/latest/services/ntpd/server.html

[R3] Netgate: Serial GPS — https://docs.netgate.com/pfsense/en/latest/services/ntpd/gps.html

[R4] Netgate: PPS Source (Non-GPS) — https://docs.netgate.com/pfsense/en/latest/services/ntpd/pps.html

[R5] Netgate: NTP Daemon Status — https://docs.netgate.com/pfsense/en/latest/monitoring/status/ntp.html

[R6] Netgate: Clock Bootstrap Behavior — https://docs.netgate.com/pfsense/en/latest/services/ntpd/bootstrap.html

[R7] Netgate: Troubleshooting Clock Issues — https://docs.netgate.com/pfsense/en/latest/troubleshooting/time-synchronization.html

[R8] Netgate: General Configuration / Time Zone — https://docs.netgate.com/pfsense/en/latest/config/general.html

[R9] RFC 5905 — Network Time Protocol Version 4 — https://www.rfc-editor.org/rfc/rfc5905

[R10] RFC 1305 — NTP Version 3 — https://www.rfc-editor.org/rfc/rfc1305

Los campos y opciones de las pestañas Settings se corresponden con la interfaz descrita; los parámetros de ACLs, Serial GPS y PPS se completan con la documentación oficial de Netgate. Según versión, plataforma y hardware, pueden variar las etiquetas o disponibilidad de determinados controles.

49 Services → PPPoE Server

Concentrador de acceso · usuarios · RADIUS · redes de clientes · diagnóstico

El servidor PPPoE permite exigir una sesión autenticada antes de proporcionar conectividad IP sobre un segmento Ethernet. Este capítulo desarrolla la pantalla de administración, todos los campos del formulario de alta documentados por Netgate, el diseño de direccionamiento y las comprobaciones de seguridad y funcionamiento. Los esquemas y escenarios son conceptuales, independientes de cualquier despliegue real.

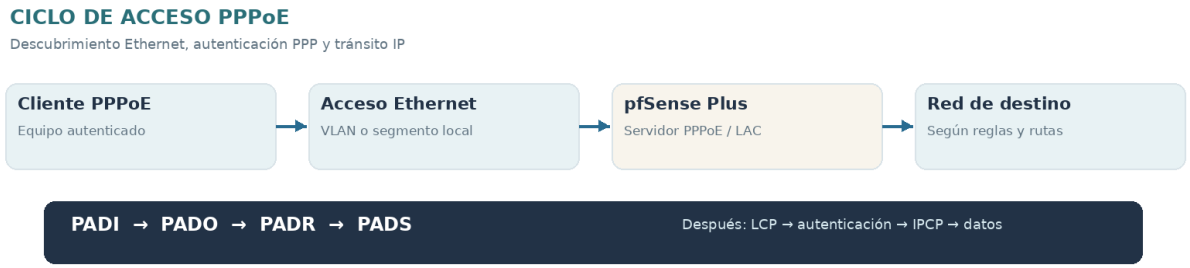


Figura 49.1. Fases de descubrimiento y establecimiento de una sesión de acceso PPPoE.

49.1. Propósito del servicio y utilidad empresarial

pfSense Plus puede comportarse como concentrador de acceso (LAC) para clientes que inician sesiones PPPoE desde una red local. El cliente descubre el servicio en Ethernet, presenta credenciales y, si se autoriza, obtiene parámetros IP de su sesión. Puede emplearse para redes de acceso controlado, laboratorios de autenticación, entornos de operadores pequeños o segmentos donde se requieren cuentas individualizadas. No debe confundirse con los parámetros PPPoE de una interfaz WAN que se conecta a un proveedor externo.

49.2. PPPoE frente a DHCP, portal cautivo y VPN

Mecanismo	Función principal	Diferencia esencial
PPPoE Server	Sesión PPP autenticada sobre Ethernet.	Requiere compatibilidad PPPoE en el extremo cliente.
DHCP Server	Entrega de configuración IP sin sesión PPP.	No autentica mediante el intercambio PPPoE.
Captive Portal	Control de acceso web a clientes IP.	Interacción normalmente en capa de aplicación.
Servidor VPN	Túnel sobre redes IP preexistentes.	PPPoE descubre al concentrador en la capa 2.

49.3. Ruta exacta y alcance de las pantallas documentadas

Ruta: Services → PPPoE Server. El listado permite consultar las instancias y Add abre su creación. Los apartados siguientes explican el alta, RADIUS y los usuarios. Un listado vacío indica que no hay instancias registradas; la distribución de los formularios puede variar entre versiones.

49.4. Lectura del listado principal: columnas

Columna	Significado	Comprobación
Interface	Interfaz sobre la que escucha el concentrador.	Que corresponda al segmento Ethernet previsto.
Local IP	Dirección local usada como referencia del servidor PPPoE.	Que no sea otra dirección ya configurada en el firewall.

Columna	Significado	Comprobación
Number of users	Cantidad de usuarios relacionada con la entrada; según datos mostrados por la interfaz.	No equipararlo automáticamente con sesiones simultáneas.
Description	Etiqueta administrativa para identificar el servicio.	Usar descripción funcional, sin credenciales.
Actions	Controles de mantenimiento de cada servidor.	Confirmar la entrada antes de editar o eliminar.

49.5. Botón Add y acciones de edición posteriores

Add abre un nuevo servidor PPPoE. Una vez creada una instancia, la tabla presenta acciones de administración que pueden variar según la versión y el estado; habitualmente incluyen edición y eliminación. Editar parámetros de escucha, direccionamiento o autenticación puede desconectar clientes o impedir nuevas conexiones. Antes de borrar una instancia, comprobar las cuentas, sesiones activas, dependencias de NAT y reglas de acceso, y conservar un respaldo reciente de la configuración.

49.6. Fundamentos del protocolo y su secuencia

PPPoE utiliza una fase de descubrimiento con mensajes PADI, PADO, PADR y PADS, que establece una sesión identificada antes de comenzar PPP. Después se negocian opciones de enlace mediante LCP, autenticación y parámetros IP mediante IPCP. Una sesión puede terminarse normalmente o mediante PADT. Discovery emplea EtherType 0x8863 y el tráfico de sesión EtherType 0x8864: no son puertos TCP o UDP. Esta secuencia, definida por RFC 2516, ayuda a distinguir un fallo Ethernet de un rechazo de credenciales o un fallo IP.

Mensaje	Emisor / finalidad	Significado de diagnóstico
PADI	Cliente: busca concentradores PPPoE.	Si no aparece, revisar cliente, NIC y VLAN.
PADO	Servidor: ofrece disponibilidad.	Si no aparece, revisar segmento y servicio.
PADR	Cliente: solicita una sesión al servidor.	Si no llega, revisar descubrimiento.
PADS	Servidor: confirma y asigna identificador.	Si existe, el problema puede estar después, en PPP.
PADT	Cualquiera: indica terminación.	Investigar motivos de cierre o reintentos.

49.7. Formulario Add: Enable y selección de interfaz

Enable activa o desactiva la instancia definida. Interface selecciona una única interfaz sobre la que atender sesiones PPPoE. Netgate admite varias instancias en interfaces separadas, pero no implica que una sola instancia pueda atender simultáneamente múltiples interfaces. Elegir la interfaz de acceso correcta: activar el servidor en un segmento compartido o no controlado puede exponer autenticación PPPoE donde no se pretendía. No seleccionar por error una WAN de producción.

49.8. Total User Count: límite global de usuarios simultáneos

Total User Count fija cuántos clientes puede aceptar esta instancia de PPPoE en total. Es un límite de capacidad del servicio, no el número de cuentas creadas. Debe dimensionarse según clientes previstos, rendimiento y direcciones disponibles; configurar más conexiones que direcciones asignables puede provocar fallos parciales tras la autenticación. Una reducción del máximo puede impactar nuevas sesiones y debe planificarse durante ventanas de mantenimiento.

49.9. User Max Logins: sesiones concurrentes por usuario

User Max Logins limita cuántas conexiones concurrentes puede mantener una misma identidad. Un valor restrictivo ayuda a evitar reutilización indebida de cuentas; permitir varias sesiones puede ser útil cuando

un mismo titular dispone de diversos equipos o circuitos. La política debe ser coherente con la capacidad del servidor y con RADIUS, si existe; no equivale al límite global Total User Count. Para investigar accesos duplicados, comparar usuario, sesión y hora en las herramientas disponibles.

49.10. Server Address: dirección local anunciada a los clientes

Server Address define la dirección que el firewall anuncia al cliente como extremo o puerta de enlace de su sesión PPPoE. La advertencia de Netgate es explícita: esta dirección NO puede ser una IP que ya esté en uso en otra interfaz o dirección del firewall. Es una condición distinta a la dirección LAN convencional. Elegir el valor junto con el plan de rangos remotos, rutas y seguridad; registrar su función en el inventario técnico, evitando solapamientos.

ADVERTENCIA CRÍTICA No copiar la IP actual de LAN en Server Address: la documentación oficial prohíbe utilizar una dirección ya asignada al firewall. Validar solapamientos antes de guardar.

49.11. Remote Address Range y Subnet Mask: direcciones de cliente

Remote Address Range determina el inicio del conjunto de direcciones de clientes; Subnet Mask delimita la red en la que se construirán dichas asignaciones. Deben evitarse solapamientos con interfaces locales, pools DHCP, VPN y bloques de sitios remotos. Un diseño correcto distingue la dirección del concentrador de las direcciones entregadas a los clientes y garantiza enrutamiento de retorno. Conviene reservar capacidad para crecimiento y documentar las exclusiones y eventuales IP fijas asignadas por usuario o RADIUS.

Validación	Criterio	Riesgo evitado
Unicidad	El pool PPPoE no se solapa con redes ya utilizadas.	Direcciones duplicadas y rutas ambiguas.
Capacidad	Total User Count no supera la planificación de direcciones.	Autenticación correcta sin IP disponible.
Salida	Rutas, NAT y reglas contemplan el rango PPPoE.	Conexión PPP establecida sin Internet.
DNS	Los resolvedores anunciados son accesibles desde el rango.	Fallos de nombres con conectividad IP válida.

49.12. Description: identificación de instancias

Description añade un texto opcional para localizar el servicio en el listado y en procedimientos de administración. Es útil emplear una denominación funcional, asociada al propósito del segmento o a su política de acceso, pero sin nombres personales, contraseñas o información sensible. En instalaciones con varias instancias, una descripción homogénea reduce la probabilidad de editar accidentalmente la equivocada.

49.13. DNS Servers: entrega de servidores DNS al cliente

DNS Servers permite indicar resolvedores específicos a los que los clientes podrán consultar. Si el campo queda vacío, el comportamiento documentado depende de los servicios del propio firewall: si DNS Forwarder o DNS Resolver está habilitado, se proporciona la IP del firewall; si ambos están deshabilitados, se emplean los DNS definidos en la configuración general. Esta selección debe alinearse con los controles de escucha de DNS, sus ACL y las reglas de firewall: entregar una IP DNS no garantiza por sí mismo que responda.

49.14. Usuarios locales: Username, Password e IP Address

La sección Users permite definir credenciales individuales cuando no se usa RADIUS. Username identifica la cuenta y Password autentica al cliente. IP Address es un valor opcional para entregar una IP fija a ese usuario. Cada IP fija necesita coordinación con el conjunto dinámico y la política de direcciones: evitar duplicidades, reservar suficiente capacidad y retirar cuentas inactivas. La autenticación local de PPPoE se administra aquí, no en System → User Manager.

49.15. Botón Add User y política de cuentas

Add User añade entradas al bloque Users del servidor. Crear cuentas de uso individual, establecer límites de sesión coherentes y probar la combinación usuario/contraseña desde un cliente compatible. Un cambio de contraseña puede requerir que el cliente cierre y reabra la sesión antes de utilizar la nueva credencial. Mantener un registro externo de propietarios y autorizaciones sin almacenar claves en texto claro ni en el propio manual.



Figura 49.2. Alternativas de autenticación local o RADIUS para la instancia PPPoE.

49.16. RADIUS: ventajas y arquitectura AAA

Use RADIUS Authentication sustituye la autenticación con usuarios locales por al menos un servidor RADIUS. Resulta útil si se desea mantener una base de identidades centralizada, aplicar políticas AAA o contar con autenticación replicada. El módulo PPPoE posee ajustes RADIUS propios y no debe confundirse con los servidores registrados en User Manager. Esta separación está documentada explícitamente por Netgate. Asegurar una ruta privada o VPN entre firewall y servidor de autenticación.

49.17. Use RADIUS Authentication: comportamiento habilitado/deshabilitado

Habilitado: la instancia consulta el servicio RADIUS configurado para aceptar o rechazar credenciales, conforme a la respuesta remota. Deshabilitado: las cuentas configuradas directamente en el bloque Users son la fuente local de autenticación. Antes del cambio comprobar que se dispone de usuarios de prueba válidos, conectividad al RADIUS y un procedimiento de reversión. Cambiar el método no transforma automáticamente cuentas locales en cuentas remotas.

49.18. Primary RADIUS Server: IP y puertos

Primary RADIUS Server identifica el sistema preferente. IP Address indica su dirección; Authentication Port es el puerto de autenticación, habitualmente UDP 1812, mientras que Accounting Port suele ser UDP 1813 cuando se utiliza contabilidad. No son los EtherTypes PPPoE ni deben confundirse con los puertos de la fase de descubrimiento. Confirmar que el servidor RADIUS registra al firewall como cliente autorizado, tiene una política válida y permite los paquetes necesarios por una red protegida.

Campo RADIUS	Uso	Comprobación
IP Address	Dirección del servidor AAA.	Rutas de ida y retorno y origen previsto.
Authentication Port	Puerto de autenticación; habitualmente UDP 1812.	Política del firewall y escucha del RADIUS.
Accounting Port	Puerto de accounting; habitualmente UDP 1813.	Uso solo cuando se habilita contabilidad.
Shared Secret y Confirm	Clave compartida del cliente RADIUS.	Coincidencia exacta y custodia segura.

49.19. Shared Secret y Confirm: claves compartidas RADIUS

Primary RADIUS Server Shared Secret guarda el secreto compartido entre el firewall y el servidor remoto; el campo Confirm exige repetirlo. Si los secretos no coinciden, las peticiones pueden fallar incluso cuando la conectividad y los puertos parecen correctos. La clave no se documenta en informes, tickets ni capturas. Debe tener suficiente entropía, acceso restringido y rotación coordinada con el servidor de autenticación.

49.20. Servidor RADIUS secundario y tolerancia a fallos

Use a Backup RADIUS Authentication Server habilita un servidor secundario para utilizarlo cuando falla el primario. Secondary RADIUS Server dispone de parámetros equivalentes: IP, puertos y secreto. Se recomienda ensayar la caída real del primario en un entorno controlado y verificar el comportamiento de la autenticación. El respaldo de RADIUS no sustituye a la alta disponibilidad del firewall o de la interfaz Ethernet; cada dependencia requiere sus propias pruebas.

49.21. Use RADIUS Accounting y RADIUS Accounting Update

Use RADIUS Accounting envía datos de uso de la sesión a un servidor RADIUS, incluyendo eventos de inicio y finalización y contadores de tráfico cuando están disponibles. RADIUS Accounting Update ajusta, en segundos, el intervalo de los informes intermedios. Una frecuencia muy corta incrementa mensajes y registros; una frecuencia excesiva reduce granularidad. Accounting facilita trazabilidad y facturación en algunos escenarios, pero necesita un criterio de conservación, correlación e información de privacidad para los usuarios.

49.22. NAS IP Address: identificación del concentrador

NAS IP Address permite determinar qué dirección se transmite en el atributo RADIUS NAS-IP-Address. Puede ayudar a identificar el concentrador ante servidores AAA que atienden a múltiples equipos. La dirección anunciada debe ser coherente con la política de clientes RADIUS y ser única cuando el entorno lo necesite. No tiene por qué ser la dirección que recibirá el cliente PPPoE ni equivale a Server Address. Confirmar el atributo recibido del lado RADIUS si hay rechazos de política.

49.23. RADIUS Issued IP Addresses: asignaciones centralizadas

RADIUS Issued IP Addresses autoriza que se asignen direcciones IP a usuarios a partir de atributos de respuesta RADIUS, en lugar de depender solo del rango local. Es necesario validar que el servidor devuelva direcciones válidas, sin solapamientos, y que las rutas y el filtrado admitan esos valores. Si la infraestructura no garantiza el control del inventario de direcciones, es preferible comenzar con un pool local estable antes de activar esta opción.

49.24. Reglas de firewall para clientes PPPoE

La autenticación PPPoE establece la sesión, pero no implica autorización universal para circular entre redes. pfSense dispone de macros y grupos relacionados con clientes PPPoE que permiten diseñar reglas de filtrado aplicables al tráfico recibido por esas sesiones. Construir reglas por mínimo privilegio: acceso DNS y servicios autorizados, denegación de destinos sensibles y registros de auditoría selectivos. Las reglas se procesan al ingreso de cada flujo conforme a la metodología de pfSense.

49.25. Enrutamiento y NAT de salida para clientes PPPoE

Una sesión PPPoE activa solo garantiza que el enlace y la autenticación hayan funcionado; no configura de forma automática todas las políticas de salida. Revisar rutas de retorno, DNS y, si la red de clientes sale a Internet a través de una WAN con direcciones privadas, las reglas de Outbound NAT pertinentes. En modo NAT híbrido/manual, el rango PPPoE puede requerir una regla expresa. Evitar políticas generales que permitan a clientes PPPoE alcanzar redes de administración.

49.26. Aislamiento físico y VLAN: alcance capa 2

La fase Discovery utiliza tramas Ethernet y, por tanto, el concentrador debe estar presente en el mismo dominio de capa 2 accesible para el cliente. Una VLAN no etiquetada correctamente, un trunk incompleto, un puerto del switch diferente o un filtrado de EtherTypes puede impedir recibir PADO. La ruta IP hacia el firewall no reemplaza esta contigüidad Ethernet para el descubrimiento. Por seguridad, dedicar a PPPoE un segmento controlado y limitar quién puede originar sesiones.

49.27. MTU/MRU: sobrecarga PPPoE y pruebas de fragmentación

La encapsulación PPPoE habitual reduce a 1492 bytes la carga IP disponible sobre Ethernet estándar de 1500 bytes. Algunas redes admiten configuraciones de mayor MTU mediante extensiones adecuadas, pero no deben asumirse. Problemas de rutas con PMTUD bloqueado pueden provocar páginas incompletas o

sesiones con ping exitoso y servicios fallidos. Ajustar MTU/MSS solo tras comprobar requisitos en ambos extremos y la trayectoria; documentar la reversión.

49.28. Rendimiento, escalabilidad y límites de la solución

El número de sesiones, cifrado de otros servicios, paquetes por segundo, reglas PF y carga RADIUS influyen en la capacidad real. Dimensionar Total User Count junto a recursos de CPU, memoria, rangos IP y rendimiento del enlace. La implementación del servidor no debe inferirse de las notas de aceleración de clientes WAN PPPoE; las recomendaciones de if_pppoe descritas por Netgate se refieren específicamente a conexiones de tipo WAN. Medir carga, latencia y estabilidad con escenarios representativos.

49.29. Seguridad de credenciales y ausencia de cifrado nativo

PPPoE proporciona encapsulación y un procedimiento de autenticación, pero no debe presentarse como un túnel cifrado de extremo a extremo. El mecanismo concreto de autenticación PPP debe ser compatible con cliente y servidor, y las redes no confiables requieren controles adicionales. Proteger los secretos RADIUS, limitar usuarios concurrentes, aislar el dominio Ethernet, revisar políticas de acceso y gestionar cuentas inactivas. Cuando se requiere confidencialidad del tráfico, emplear TLS, IPsec u otras capas apropiadas.

SEGURIDAD No confundir “conexión PPPoE autenticada” con “tráfico cifrado”. Los servicios sensibles necesitan protección adicional, y el tramo hasta RADIUS debe discurrir por una red segura o túnel.

49.30. Procedimiento 1: crear una instancia local de pruebas

1. Crear una copia de seguridad previa y seleccionar un segmento Ethernet/VLAN aislado para la prueba.
2. En Services → PPPoE Server, pulsar Add y marcar Enable solo cuando la topología esté preparada.
3. Seleccionar Interface y planificar Server Address que no coincida con ninguna IP del firewall.
4. Definir Remote Address Range, Subnet Mask y capacidad Total User Count / User Max Logins.
5. Indicar DNS Servers si se necesitan direcciones específicas y redactar una Description neutral.
6. Añadir un usuario de prueba con Add User (Username y Password; IP fija solo si procede).
7. Guardar, aplicar los cambios requeridos por la interfaz y comprobar la sesión desde un cliente PPPoE autorizado.
8. Verificar dirección asignada, DNS, rutas, filtrado y cierre limpio de la conexión.

49.31. Procedimiento 2: activar RADIUS sin perder la alternativa anterior

1. Comprobar alcance al RADIUS por una red de confianza o VPN y registrar el firewall como cliente permitido.
2. Establecer puertos de autenticación/contabilidad y configurar secretos coincidentes en ambos extremos.
3. En la instancia PPPoE, activar Use RADIUS Authentication y definir Primary RADIUS Server.
4. Si existe, configurar Backup RADIUS Authentication Server y ensayar su disponibilidad.
5. Activar Accounting únicamente si se necesita, con un intervalo de actualización razonable.
6. Probar un usuario autorizado y otro rechazado, contrastando el resultado con los registros RADIUS.
7. Verificar NAS-IP-Address y direcciones atribuidas por RADIUS si se utilizan; documentar la reversión.

49.32. Procedimiento 3: establecer dirección fija para un usuario

1. Seleccionar una IP no asignada y compatible con el esquema de rutas acordado.
2. Si se utilizan usuarios locales, indicar IP Address en la cuenta correspondiente; con RADIUS, definir los atributos apropiados y habilitar RADIUS Issued IP Addresses.
3. Cerrar la sesión del usuario de prueba, iniciar una nueva y comprobar que se recibió la dirección prevista.
4. Verificar reglas, NAT, DNS y ausencia de colisiones; registrar el resultado en un inventario de direcciones.

49.33. Procedimiento 4: retirar el servicio o modificar límites

1. Identificar si hay clientes conectados y servicios dependientes.
2. Programar una ventana de mantenimiento y crear una copia de seguridad exportable.
3. Reducir uso o desconectar sesiones de forma coordinada antes de deshabilitar o eliminar la entrada.
4. Deshabilitar Enable si se desea conservar la configuración; borrar solo tras confirmar que no es necesaria.
5. Verificar desaparición de sesiones, revisión de reglas y eliminación de cuentas o secretos obsoletos.

49.34. Verificación funcional: pruebas mínimas de aceptación

Prueba	Resultado esperado	Evidencia
Descubrimiento	PADI → PADO → PADR → PADS completado.	Captura en interfaz Ethernet.
Autenticación válida	Cliente obtiene sesión al usar identidad permitida.	Registro del cliente / RADIUS.
Autenticación errónea	Se rechaza cuenta inválida.	Evento AAA / ausencia de sesión.
Asignación IP	Cliente recibe IP prevista y DNS funcional.	Estado IP del cliente.
Conectividad	Solo se alcanzan destinos expresamente permitidos.	Prueba de acceso y reglas PF.
Capacidad	Se respetan límites globales y por usuario.	Pruebas de sesiones concurrentes.
Restauración	El respaldo recupera el estado anterior.	Acta de prueba de reversión.

49.35. Captura de paquetes: filtros y diagnóstico por fase

Diagnósticos → Packet Capture (o una herramienta equivalente) permite observar el tráfico en la interfaz Ethernet antes de que el cliente reciba IP. Filtrar específicamente PPPoE Discovery/Session cuando la herramienta lo admita; el análisis se apoya en EtherTypes 0x8863 y 0x8864. Un PADI sin PADO apunta al acceso L2 o al servicio; una negociación que alcanza PADS pero falla después exige revisar PPP, credenciales, RADIUS y asignación de IP. No guardar capturas con contraseñas o identificadores en documentos distribuidos.



Figura 49.3. Árbol de comprobación por capas para incidencias PPPoE.

49.36. Registro de eventos: qué revisar y qué no confundir

Consultar los registros operativos del servicio disponibles en la versión y los eventos del servidor AAA para ubicar rechazos, pérdida de enlace y errores de atribución IP. La página de Netgate “PPP Logs” está descrita para conexiones PPP tipo WAN, no para servidores PPPoE locales: no debe citarse como fuente universal de registros del servidor. Para diagnóstico de cliente PPPoE local se recomiendan la captura Ethernet, los logs del concentrador y los del RADIUS si corresponde.

49.37. Errores frecuentes: síntoma, causa probable y solución

Síntoma	Comprobar	Corrección sugerida
El cliente no ve el servidor	VLAN, puertos, NIC, Enable, PADI/PADO.	Restaurar L2 y segmento adecuado.
Se ve oferta pero falla la conexión	PADR/PADS y negociación PPP.	Revisar compatibilidad de cliente y servicio.
Credenciales rechazadas	Método local/RADIUS, usuario y secreto.	Corregir identidad y política AAA.
Conecta sin IP correcta	Server Address, pool, IP fija / RADIUS.	Eliminar solapamientos y revisar atributos.
Conecta sin navegar	Reglas, DNS, rutas y NAT.	Permitir solo flujos autorizados y revisar traducción.
Cortes intermitentes	Enlace, MTU, sesiones máximas, recursos.	Medir carga y comprobar estabilidad de capa 2.
No funciona respaldo RADIUS	Conectividad, puerto, secreto y fallos primarios.	Probar failover controlado y revisar logs.

49.38. Escenario práctico A: usuarios de un segmento de acceso

Una zona de acceso gestionado puede exigir cuentas PPPoE individuales para permitir conexión a recursos determinados. Diseñar una interfaz o VLAN exclusiva, asignar una capacidad realista, dar a cada usuario credenciales propias y aplicar reglas por mínimo privilegio. Evitar mezclar dispositivos sin soporte PPPoE en el mismo acceso a menos que existan segmentos separados. Comprobar tiempos de autenticación, recuperación ante errores y política de baja de usuarios.

49.39. Escenario práctico B: autenticación centralizada con AAA

Cuando varios concentradores o puntos de acceso necesitan una gestión común de identidades, RADIUS permite centralizar control de cuentas y llevar contabilidad de sesiones. Antes de migrar, definir el NAS IP de cada firewall, secretos distintos y una red de gestión protegida. El servicio secundario RADIUS ofrece tolerancia frente a una caída de AAA, pero el acceso continúa dependiendo de la disponibilidad física y del propio firewall. Registrar un ensayo de caída y retorno.

49.40. Escenario práctico C: entorno de prácticas y pruebas de operadores

En una red de laboratorio aislada, el servidor facilita estudiar fases PPPoE, errores deliberados de credenciales, límites de sesiones y asignación IP. Es útil contrastar el paquete Discovery con las reglas IP posteriores y medir comportamiento con diferentes MTU. Las pruebas no deben realizarse en una red corporativa en producción ni mezclarse con puertos de usuarios reales. Un entorno virtual puede ser válido si el hipervisor permite el paso íntegro de tramas Ethernet PPPoE.

49.41. Buenas prácticas de seguridad y administración

Control	Recomendación	Justificación
Segmentación	Exponer PPPoE solo en la VLAN de acceso prevista.	Reduce clientes no autorizados y alcance accidental.
Identidades	Una cuenta por usuario; límite de sesiones coherente.	Facilita bajas y auditoría de uso.
RADIUS	Tramo protegido y secretos fuertes, sin revelar.	Evita acceso indebido a AAA.
Filtrado	Políticas explícitas sobre clientes PPPoE.	Autenticación no equivale a confianza total.
Inventario	Mapeo de rangos, IP fijas y rutas.	Previene solapamientos.
Cambio	Respaldo, horario aprobado y ensayo de retorno.	Reduce cortes por ajustes del servidor.

49.42. Plan de reversión ante fallo tras un cambio

Si una modificación deja clientes fuera de servicio, detener cambios adicionales y verificar la última configuración funcional. Recuperar los valores de interfaz, Server Address y rango, método de autenticación y secretos RADIUS; comprobar que el switch entrega el dominio Ethernet previsto. Restaurar desde copia cuando la corrección manual no sea segura, con especial cuidado al no impactar otros servicios del firewall. Finalizada la recuperación, validar al menos una sesión autenticada y los servicios empresariales dependientes.

49.43. Ficha de aceptación de servicio para explotación

Verificación	Criterio de aprobación	Estado
Alcance	Interfaz local y VLAN correctas.	☐
Capacidad	Total User Count y Max Logins dimensionados.	☐
Direccionamiento	Server Address único; rango libre de conflictos.	☐
AAA	Autenticación positiva/negativa y backup probado.	☐
Seguridad	Reglas y acceso a DNS/NAT auditados.	☐
Operación	Diagnóstico y procedimiento de reversión disponibles.	☐

49.44. Lista de preproducción: compatibilidad de equipos de acceso

Antes de activar un servidor PPPoE en una red real conviene ensayar un equipo representativo de cada familia de clientes. Comprobar si puede descubrir concentradores PPPoE en la VLAN prevista, si permite guardar credenciales de manera segura, si reconecta tras un corte breve y si conserva la configuración IP/DNS necesaria al volver a conectarse. Algunas estaciones o dispositivos industriales no incorporan cliente PPPoE: no hay que deducir que todos los equipos Ethernet podrán participar. Para estos casos se debe diseñar un segmento de acceso alternativo, independiente y autorizado.

Tipo de prueba	Criterio de aceptación	Acción si falla
Arranque en frío	El cliente descubre servidor y recibe IP.	Revisar VLAN, cliente y credenciales.
Reconexión	Recupera la sesión tras cerrar la conexión.	Revisar comportamiento LCP y reintentos.
Dos equipos	Respetan Total User Count y Max Logins.	Corregir los límites antes de producción.
Fallo DNS	El equipo conserva conectividad IP verificable.	Comprobar resolvedores y políticas.
Fallo RADIUS	No quedan sesiones nuevas sin autorización.	Verificar primario, secundario y políticas.
Mantenimiento	Se restablece el servicio tras revertir.	Documentar pasos y respaldos.

49.45. Gobierno del servicio: altas, cambios y bajas

La operación diaria debe prever un procedimiento formal de altas: solicitud aprobada, identidad individual, asignación de acceso y validación de alcance. Los cambios comprenden rotación de contraseña, modificación de IP fija, ajustes de concurrencia y alteraciones de perfiles RADIUS; todos se registrarán sin revelar secretos. Para bajas, desactivar la identidad, comprobar sesiones aún abiertas, retirar asignaciones estáticas que no se reutilizarán de inmediato y verificar la caducidad de permisos. Si se utiliza RADIUS Accounting, la organización deberá fijar un plazo de conservación de registros que sea proporcional a su finalidad y normativa aplicable.

49.46. Mantenimiento periódico y controles preventivos

Con periodicidad planificada, verificar que la instancia está activa solo en la interfaz requerida, que el número de usuarios y el pool disponible mantienen margen de capacidad y que los servidores RADIUS responden con latencia aceptable. Revisar cuentas inactivas, bloqueos repetidos, aumentos anómalos de sesiones y cambios de perfil de tráfico. Conviene también probar la restauración de la configuración y una reconexión completa después de actualizaciones del firewall. No confundir una sesión estable durante unos segundos con una aceptación funcional sostenida: validar DNS, aplicaciones y desconexiones en sesiones más largas.

49.47. Glosario técnico

Término	Definición breve
LAC / Access Concentrator	Equipo que acepta sesiones PPPoE sobre Ethernet.
PADI / PADO / PADR / PADS	Mensajes principales de descubrimiento PPPoE.
PADT	Mensaje para terminar una sesión PPPoE.
LCP / IPCP	Protocolos PPP de control del enlace y de IPv4.
AAA / RADIUS	Autenticación, autorización y contabilidad centralizadas.
NAS-IP-Address	Atributo RADIUS que identifica al dispositivo de acceso.
MTU / MRU	Tamaños máximos de unidad transmitida y recibida.
EtherType	Identificador del protocolo transportado en una trama Ethernet.

49.48. Referencias oficiales y normas utilizadas

Netgate. “PPPoE Server”: https://docs.netgate.com/pfsense/en/latest/services/pppoe-server.html. Referencia principal de todos los campos del formulario de servidor, RADIUS, usuarios y creación de instancias.

Netgate. “RADIUS Authentication Servers”: https://docs.netgate.com/pfsense/en/latest/usermanager/radius.html. Separación de RADIUS del User Manager, transporte protegido y puertos habituales.

Netgate. “Configuring Firewall Rules”: https://docs.netgate.com/pfsense/en/latest/firewall/configure.html. Macros PPPoE Clients, filtrado y reglas de interfaz.

Netgate. “PPP Logs”: https://docs.netgate.com/pfsense/en/latest/monitoring/logs/ppp.html. Diferencia entre logs PPP de WAN y servicios locales.

IETF, RFC 2516. “A Method for Transmitting PPP Over Ethernet”: https://www.rfc-editor.org/rfc/rfc2516. Etapas de descubrimiento y sesión, cabeceras y EtherTypes.

Netgate. “Changing Credentials and Keys”: https://docs.netgate.com/pfsense/en/latest/recipes/changing-credentials.html. Rotación de credenciales y secretos PPPoE.

50 Services → Router Advertisement

Anuncios IPv6 · SLAAC · DHCPv6 · prioridades · DNS · PREF64

Router Advertisement (RA) es el mecanismo por el que un router IPv6 anuncia su presencia y comunica a los equipos de un segmento datos de enrutamiento y de autoconfiguración. Este capítulo explica la configuración del servicio en pfSense Plus, sus modos operativos, los tiempos de validez, los prefijos, la información DNS y su coordinación con DHCPv6 y NAT64. Se emplean exclusivamente diagramas originales y direcciones de documentación.



Figura 50.1. Papel de los anuncios del router en la configuración IPv6 del cliente.

50.1. Objetivo, alcance y funcionamiento de RA

El demonio de anuncios IPv6 utiliza mensajes ICMPv6 Router Advertisement (tipo 134) y responde a Router Solicitation (tipo 133). Los equipos descubren routers y, según los flags del anuncio, pueden configurar direcciones mediante SLAAC, consultar un servidor DHCPv6 o combinar ambos métodos. Los anuncios son locales al enlace y no deben confundirse con un protocolo de enrutamiento entre sedes. El firewall necesita reglas apropiadas para que el tráfico IPv6 de los clientes alcance sus destinos.

50.2. Por qué DHCPv6 no sustituye a los anuncios de router

A diferencia de DHCPv4, DHCPv6 no proporciona la puerta de enlace predeterminada. Los clientes IPv6 normalmente aprenden el siguiente salto mediante RA, habitualmente identificado por una dirección link-local del router. Una concesión DHCPv6 válida no garantiza salida IPv6 cuando no existe una ruta por defecto correcta. El entorno debe considerar, además, que determinados sistemas móviles solo utilizan SLAAC para obtener direcciones de host.

50.3. Ubicación y pestañas de configuración

Ruta: Services → Router Advertisement. El menú presenta una pestaña por interfaz elegible; el material de referencia incluye WAN, LAN y una interfaz adicional. Todas comparten las opciones básicas, aunque la disponibilidad concreta depende del direccionamiento y de la versión. En una conexión a Internet, pfSense suele recibir RA de un router aguas arriba; los anuncios a clientes se habilitan en las redes internas. Solo se anuncian prefijos en la WAN cuando esa interfaz da servicio deliberadamente a clientes IPv6, nunca por el mero hecho de existir la pestaña.

50.4. Arquitectura de los mensajes: RS, RA, multicast y router

Elemento	Uso	Detalle para el administrador
Router Solicitation / RS	Solicitud inicial del host al router.	ICMPv6 tipo 133; acelera descubrimiento al conectarse.
Router Advertisement / RA	Anuncio periódico o respuesta a RS.	ICMPv6 tipo 134; incluye flags y opciones.
ff02::1	Destino multicast a todos los nodos del enlace.	Alcance local a la VLAN o segmento.
Hop limit 255	Validación de proximidad de ND/RA.	Ayuda a impedir reenvío desde otros saltos.

Elemento	Uso	Detalle para el administrador
radvd	Servicio de anuncios configurado por pfSense.	Depende de interfaz y opciones elegidas.

50.5. Router Mode: significado de las seis opciones

Modo	Indicaciones RA	Comportamiento esperado
Disabled	No emite RA.	Los clientes requieren otro router u opción estática.
Router Only	Sin M/O; sin SLAAC anunciado.	Descubrir el router, pero configurar dirección por otros medios.
Unmanaged	M=0, O=0; A=1.	SLAAC para direcciones, sin DHCPv6 indicado por RA.
Managed	M=1, O=1; A=0.	Direcciones a través de DHCPv6, si el cliente lo soporta.
Assisted	M=1, O=1; A=1.	SLAAC y DHCPv6 disponibles.
Stateless DHCP	M=0, O=1; A=1.	SLAAC para dirección; DHCPv6 para opciones adicionales.

M es el indicador “Managed”, O indica información adicional (“Other configuration”) y A pertenece a la opción de prefijo e indica autoconfiguración autónoma. L (on-link) se refiere a la determinación de destinos del mismo enlace y no equivale a A. Los clientes pueden interpretar estas señales de forma distinta; debe comprobarse el comportamiento efectivo de sus sistemas operativos.



Figura 50.2. Comparativa de tres políticas habituales de direccionamiento IPv6.

50.6. Router Mode: Disabled y Router Only

Disabled detiene los anuncios en la interfaz: puede resultar apropiado si no hay clientes IPv6 o ya existe otro router anunciado. Router Only anuncia el equipo como posible router, pero no ofrece por RA un mecanismo SLAAC para autoconfigurar direcciones. Úsese únicamente cuando la asignación de direcciones está resuelta por un método separado. Cambiar a Disabled en una red dependiente de RA puede suprimir la puerta de enlace que conocen nuevos clientes y degradar la conectividad de los existentes al expirar las entradas.

50.7. Router Mode: Unmanaged, Managed y Assisted

Unmanaged es adecuado cuando se desea que los hosts formen direcciones mediante SLAAC. Managed orienta la obtención de direcciones hacia DHCPv6, apropiado cuando se necesitan concesiones y reservas en sistemas compatibles; por sí solo no convierte a todos los clientes en compatibles con DHCPv6. Assisted combina la autoconfiguración SLAAC con DHCPv6; útil en redes heterogéneas y cuando se necesitan datos o inventario DHCPv6 para una parte de los dispositivos. En todos los modos deben verificarse opciones de DNS y rutas.

50.8. Router Mode: Stateless DHCP

Stateless DHCP conserva la dirección obtenida mediante SLAAC y señala la disponibilidad de configuración adicional por DHCPv6, como servidores DNS u otras opciones compatibles. No equivale a

“Managed”: no pretende que DHCPv6 asigne la dirección del host. Es relevante para redes en las que la mayoría de dispositivos generan sus propias direcciones, pero existe una necesidad de publicar parámetros adicionales. La compatibilidad depende de cada sistema operativo.

50.9. Router Priority: Low, Normal y High

Router Priority influye en la preferencia de la ruta predeterminada cuando existen varios routers anunciándose en un mismo segmento. High indica preferencia más alta; Normal, la intermedia; Low, la menor. Mantener Normal con un solo equipo. Una prioridad alta no sustituye a un mecanismo completo de alta disponibilidad ni garantiza conmutación instantánea: la detección del fallo y el mantenimiento de las rutas dependen de tiempos RA y del cliente.

50.10. RA Interface: anuncio mediante una VIP CARP (opción condicional)

RA Interface aparece cuando existen VIP CARP adecuadas y permite anunciar una dirección de router específica en lugar de la link-local propia de cada nodo. En alta disponibilidad IPv6 suele ser preferible una VIP CARP link-local para que la ruta predeterminada apunte al nodo activo. Comprobar la disponibilidad del control y revisar topología, roles y reglas antes de configurar CARP.

50.11. Valid Lifetime: validez del prefijo

Valid Lifetime controla el tiempo durante el que el prefijo anunciado sigue siendo válido, expresado en segundos desde la emisión del RA. Valor indicado en la pantalla: 86400 s (24 horas). En SLAAC afecta también a la validez de direcciones originadas del prefijo. Un valor demasiado largo puede prolongar el uso de un prefijo retirado; uno demasiado corto exige continuidad de anuncios para evitar envejecimiento prematuro. Al renumerar, no se debe suprimir abruptamente el prefijo antiguo sin plan de transición.

50.12. Preferred Lifetime: período preferido de direcciones SLAAC

Preferred Lifetime determina cuánto tiempo las direcciones SLAAC generadas del prefijo siguen siendo preferidas para nuevas conexiones. Valor indicado: 14400 s (4 horas). Una dirección que deje de ser preferida puede continuar siendo válida hasta agotar Valid Lifetime, pero los clientes procurarán no elegirla para conexiones nuevas. En condiciones habituales Preferred Lifetime no debe exceder Valid Lifetime. Este mecanismo facilita transiciones de prefijo ordenadas.

50.13. Minimum y Maximum RA Interval: periodicidad

Minimum RA Interval establece el mínimo entre anuncios multicast no solicitados; la pantalla indica 200 s. Maximum RA Interval fija el máximo, indicado como 600 s. El demonio emite RA dentro de ese rango, además de poder responder a solicitudes de los clientes. Acortar ambos límites aumenta la señalización y puede ayudar a converger antes, pero no debe hacerse sin motivo; introducir valores extremos o incompatibles puede causar fallos del servicio o comportamientos inesperados.

50.14. Router Lifetime: vigencia de la ruta por defecto

Router Lifetime indica por cuántos segundos el cliente puede considerar a este router como salto predeterminado. Por defecto equivale a tres veces Maximum RA Interval: con 600 s, 1800 s. El valor cero indica que el equipo no se anuncia como router por defecto, aunque se puedan mantener otras opciones en RA. Debe elegirse en consonancia con Maximum RA Interval, la redundancia existente y el tiempo aceptable de pérdida de ruta ante un fallo.

Temporizador	Predeterminado indicado	Lectura operativa
Valid Lifetime	86400 s	24 horas de validez para el prefijo.
Preferred Lifetime	14400 s	4 horas durante las que la dirección es preferida.
Minimum RA Interval	200 s	Cadencia mínima de anuncios multicast.
Maximum RA Interval	600 s	Cadencia máxima de anuncios multicast.

Temporizador	Predeterminado indicado	Lectura operativa
Router Lifetime	1800 s (3 × 600)	Caducidad anunciada de la ruta por defecto.
NAT64 Prefix Lifetime	1800 s (3 × 600)	Vigencia de PREF64 si se habilita.

50.15. PREF64: anuncio de prefijo NAT64

PREF64 (RFC 8781) informa a clientes compatibles del prefijo que se utiliza para representar destinos IPv4 en IPv6. La opción Advertise a NAT64 prefix se utiliza cuando se ha desplegado una solución NAT64 real. Normalmente el prefijo estándar es 64:ff9b::/96. Su activación no crea por sí sola una traducción funcional: hacen falta el mecanismo NAT64, las reglas correspondientes, rutas y DNS64 cuando se usa resolución de nombres.

ADVERTENCIA NAT64 PREF64 únicamente anuncia información. No habilites esta opción como sustituto de configurar NAT64 y DNS64; los clientes podrían intentar rutas de acceso que no funcionan.

50.16. NAT64 Prefix Lifetime: vigencia de PREF64

NAT64 Prefix Lifetime define durante cuánto tiempo sigue vigente el prefijo NAT64 divulgado, contado desde la emisión del anuncio. El valor predeterminado indicado es tres veces Maximum RA Interval. Si cambia el prefijo de traducción, coordinar el tiempo con la actualización de los clientes y la política de DNS64. El administrador debe conservar el mismo prefijo lógico en PREF64, DNS64 y las reglas de traducción para evitar discrepancias.

50.17. RA Subnet(s): alcance de prefijos anunciados

RA Subnet(s) permite añadir una o varias subredes IPv6 en notación CIDR que el demonio anunciará en la interfaz. La máscara debe corresponder al prefijo real y a su enrutamiento, siendo /64 la longitud habitual para SLAAC. Si la lista queda vacía, la documentación indica que se anuncia el prefijo asociado a la propia interfaz. No sirve introducir aquí una red ajena o inexistente: podría inducir a los clientes a tratar un prefijo como local o a autoconfigurarse con direcciones sin ruta de retorno.

50.18. Control Add RA Subnet y validación de máscaras

La documentación de Netgate describe Add RA Subnet para incorporar filas adicionales. Introducir el prefijo y su longitud con los mismos criterios que en Interfaces: la red debe pertenecer al segmento de clientes o estar correctamente asociada a él. El desplegable de longitud puede mostrar numerosas máscaras, pero que una máscara sea seleccionable no significa que sea apropiada para SLAAC; emplear /64 en los casos ordinarios y validar el diseño antes de aplicar. Eliminar subredes puede afectar clientes que ya hayan generado direcciones.

50.19. DNS Configuration: Enable DNS (RDNSS/DNSSL)

Enable DNS activa el envío de opciones DNS mediante los anuncios RA, concretamente RDNSS (servidores recursivos) y DNSSL (dominios de búsqueda). Desactivarlo suprime esa información en los anuncios y puede dejar a clientes SLAAC sin DNS, aunque la conectividad IPv6 y la ruta funcionen. El texto de la interfaz advierte que deshabilitarlo puede ser problemático para la compatibilidad normativa según el escenario. Verificar el soporte en los sistemas cliente y disponer de un mecanismo alternativo para los que ignoran RDNSS/DNSSL.

50.20. Mirror DHCPv6: coherencia de parámetros DNS

Mirror DHCPv6 copia automáticamente la configuración DNS principal del servidor DHCPv6 a los anuncios RA. Se aconseja cuando ambos mecanismos coexisten y se desea mantener una única fuente de parámetros para clientes heterogéneos. Si DHCPv6 no está preparado, deshabilitado o publica servidores incorrectos, el reflejo puede provocar resultados indeseados. Antes de utilizarlo comprobar que el servicio DHCPv6 y los datos DNS que ofrece son los previstos.

50.21. DNS Server 1, 2, 3 y 4

Los cuatro campos permiten publicar direcciones IPv6 de servidores DNS concretos en las opciones RA. En blanco, pfSense puede emplear la dirección de interfaz del propio firewall si DNS Resolver o DNS Forwarder están habilitados, o tomar servidores del sistema y de enlaces dinámicos según la lógica del producto. No se debe suponer que cualquier DNS externo resolverá nombres internos: en redes con dominios corporativos, optar por resolutores apropiados para esa zona y probar consultas de nombres internos y externos.

50.22. Domain Search List: orden y formato

Domain Search List ofrece sufijos de búsqueda DNS por RA (DNSSL): permite resolver nombres cortos probando dominios definidos en el orden de la lista. La descripción suministrada termina de forma incompleta, pero la documentación de Netgate remite al comportamiento de la opción homónima de DHCP, que acepta varios dominios separados por punto y coma. Evitar publicar sufijos no autorizados o ambiguos; usar nombres reservados para documentación cuando se ejemplifiquen formatos y comprobar que el cliente utiliza efectivamente la lista.

50.23. DNS suministrado por RA frente a DNS suministrado por DHCPv6

Método	Qué aporta	Limitaciones prácticas
RA + RDNSS/DNSSL	Servidores DNS y búsqueda incluidos en ICMPv6 RA.	No todos los clientes implementan del mismo modo.
DHCPv6 (stateful)	Opciones DNS junto a la gestión DHCPv6 de direcciones.	Algunos dispositivos móviles carecen de cliente DHCPv6.
DHCPv6 (stateless)	Opciones DNS sin asignación DHCPv6 de dirección.	Requiere que el cliente siga O=1 y tenga SLAAC.
Configuración manual	DNS estático por equipo.	Coste de mantenimiento; cambios menos ágiles.

50.24. Particularidades de las pestañas de interfaz: WAN, LAN y opcionales

Aunque el menú puede presentar pestañas de una interfaz WAN y otras adicionales, esa existencia no implica que deban transmitir anuncios RA. Una WAN conectada al operador normalmente actúa como cliente de anuncios recibidos del proveedor; publicar un RA hacia un segmento ascendente puede alterar rutas de equipos de ese segmento. La LAN o una VLAN de usuarios es el lugar típico donde se anuncia el router interno. Para una interfaz opcional, decidir según si conecta clientes propios o un enlace upstream; no por el nombre de la pestaña.

RIESGO DE CONECTIVIDAD Activar anuncios en una interfaz equivocada o cambiar de Assisted/Unmanaged a Managed sin comprobar la compatibilidad de los clientes puede provocar pérdida de direcciones o rutas IPv6. Preparar copia de configuración y acceso administrativo alternativo antes del cambio.

50.25. SLAAC y prefijos delegados mediante Track Interface

En instalaciones que reciben una delegación IPv6 por DHCPv6-PD en la WAN, la LAN puede obtener su prefijo mediante Track Interface. Los anuncios RA deben corresponder al prefijo activo de esa LAN y no a un prefijo inventado. Si el proveedor renumera la delegación, cambiarán los prefijos y las direcciones SLAAC; las duraciones Valid/Preferred Lifetime y el DNS deberán tenerse en cuenta en el diseño. El prefijo de documentación 2001:db8::/32 nunca debe desplegarse como red pública real.

50.26. Alta disponibilidad: routers redundantes y VIP IPv6

En un clúster con CARP, la ruta por defecto IPv6 puede basarse en una VIP link-local compartida, difundida por RA Interface cuando el campo está disponible. Debe comprobarse el cambio de MASTER a BACKUP, la recepción de anuncios desde el nodo activo y la conectividad de los clientes al conmutar. La prioridad High/Low por sí misma no aporta el estado de sesión, NAT, sincronización ni comportamiento de CARP. Dimensionar también Router Lifetime y la consistencia de prefijos y DNS en los nodos.

50.27. PREF64, DNS64 y NAT64: escenario IPv6-only

En una VLAN exclusivamente IPv6, los clientes pueden acceder a servicios IPv4 a través de NAT64 si toda la cadena está preparada. El firewall debe tener conectividad IPv4 de salida, reglas de NAT64 en la interfaz interna, un DNS Resolver con DNS64 y prefijo coherente, y PREF64 divulgado en RA para los clientes que sepan interpretarlo. La guía oficial contempla Managed, Assisted o Stateless DHCP para este ejemplo y aconseja anunciar DNS por RA además de DHCPv6 para mejorar compatibilidad.

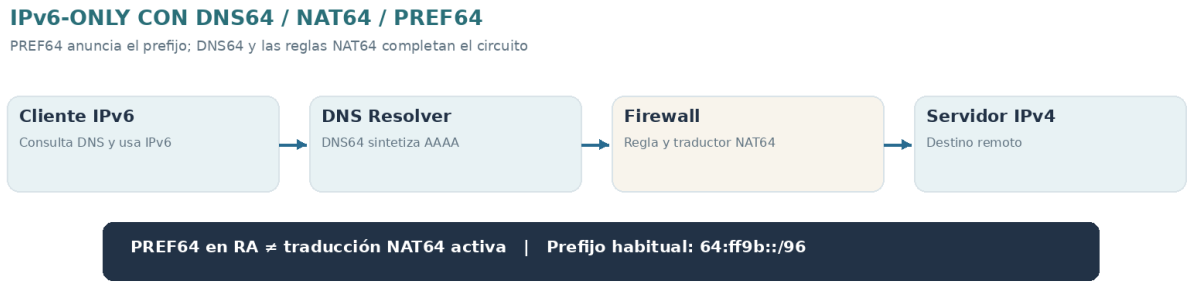


Figura 50.3. Relación entre descubrimiento de prefijo NAT64, DNS64 y la traducción de tráfico.

50.28. Procedimiento 1: habilitar SLAAC y DNS en una red interna

1. Guardar una copia de configuración y comprobar que la interfaz interna tiene un prefijo IPv6 válido y correctamente enrutado.
2. Abrir Services → Router Advertisement y seleccionar la pestaña de la interfaz interna prevista.
3. Seleccionar Router Mode = Unmanaged para direccionamiento SLAAC y mantener Router Priority = Normal si solo hay un router.
4. Conservar inicialmente los tiempos predeterminados indicados por la GUI, salvo una necesidad documentada.
5. Mantener RA Subnet(s) vacío si basta con anunciar el prefijo ya configurado en la interfaz.
6. Activar Enable DNS y verificar DNS Servers o los valores que utilizará el firewall al dejar los campos vacíos.
7. Guardar y comprobar en un cliente compatible la nueva dirección global IPv6, router por defecto y servidor DNS.
8. Probar navegación IPv6, resolución AAAA, conectividad interna y las reglas del firewall aplicadas al segmento.

50.29. Procedimiento 2: clientes DHCPv6 con RA Managed

1. Comprobar que el servidor DHCPv6 de esa LAN está habilitado y posee un rango válido sin solapamientos.
2. Seleccionar Router Mode = Managed y verificar que la opción de prefijo no promueva SLAAC como método de dirección.
3. Si se desea reutilizar DNS de DHCPv6, activar Mirror DHCPv6 y comprobar los valores reales que ofrecerá.
4. Guardar, renovar configuración del cliente e inspeccionar la concesión, dirección, ruta por defecto y DNS.
5. Repetir el ensayo con los sistemas operativos soportados antes de migrar una red heterogénea.

50.30. Procedimiento 3: red mixta mediante Assisted

1. Verificar simultáneamente la red SLAAC y la disponibilidad del servidor DHCPv6 para esa interfaz.
2. Elegir Router Mode = Assisted; conservar un prefijo /64 adecuado para los equipos SLAAC.
3. Habilitar DNS por RA y, si conviene, copiar la configuración del DHCPv6 mediante Mirror DHCPv6.
4. Probar por separado un cliente con DHCPv6 y uno que dependa de SLAAC; revisar rutas y resolución DNS.

5. Registrar el comportamiento real de ambos tipos de cliente y revertir a la política anterior si hay incompatibilidad.

50.31. Procedimiento 4: publicar PREF64 sin confundirlo con NAT64

1. Verificar que existe la ruta IPv4 de salida y una regla NAT64 operativa en el segmento IPv6-only.
2. Habilitar DNS64 en DNS Resolver con el mismo prefijo utilizado por NAT64.
3. Acceder a Router Advertisement en la interfaz de clientes y utilizar un modo compatible con la solución NAT64.
4. Activar PREF64, confirmar el prefijo previsto y comprobar la duración NAT64 Prefix Lifetime.
5. Habilitar los parámetros DNS por RA y comprobar la resolución y conectividad hacia un host remoto IPv4-only.
6. Si falla, separar las comprobaciones DNS64, NAT64 y PREF64 antes de modificar múltiples servicios.

50.32. Verificación en sistemas Linux y Windows

En Linux, los comandos “ip -6 address”, “ip -6 route” y “resolvectl status” permiten inspeccionar direcciones, ruta y DNS. Una captura limitada con “tcpdump -ni <interfaz> icmp6” o “rdisc6 <interfaz>” (si está instalado) ayuda a observar RS/RA. En Windows, “ipconfig /all”, “netsh interface ipv6 show route” y “Get-DnsClientServerAddress -AddressFamily IPv6” permiten revisar parámetros. Ninguna prueba debe incluir en el libro una dirección o nombre capturado de una instalación real.

50.33. Comprobación de paquetes en pfSense: Packet Capture

Abrir Diagnostics → Packet Capture, seleccionar la interfaz del segmento y filtrar ICMPv6. Verificar presencia de Router Solicitation (tipo 133) y Router Advertisement (tipo 134); comprobar los flags M/O y opciones de prefijo, DNS y PREF64 si se utilizan. Como los mensajes son de alcance local, una captura en otra VLAN puede no mostrarlos. Acompañar el análisis de una consulta a Diagnostics → NDP Table para visualizar vecinos IPv6, sin considerar NDP como inventario completo de clientes SLAAC.

50.34. Registro y diagnóstico: causas frecuentes

Síntoma	Causa probable	Prueba prioritaria
El cliente no recibe ruta IPv6.	RA desactivado o filtrado; interfaz incorrecta.	Captura ICMPv6, Router Lifetime y tabla de rutas.
Hay IPv6, pero no DNS.	RDNSS desactivado o cliente sin soporte.	Ver datos DNS del cliente y DHCPv6.
Solo fallan dispositivos móviles.	Managed sin SLAAC; falta cliente DHCPv6.	Probar Assisted/Unmanaged en entorno controlado.
Prefijo inesperado.	RA de otro router o subred configurada mal.	Examinar origen MAC/link-local del RA.
Hay DNS64 pero no acceso IPv4.	NAT64 o reglas de traducción ausentes.	Validar prefijo, estado y reglas NAT64.
Failover IPv6 lento.	Router Lifetime y elección del cliente.	Medir cambio de ruta al desconectar nodo.

50.35. Rogue RA, RA Guard y seguridad de la LAN

Un router no autorizado puede enviar RA y hacer que los clientes cambien ruta o prefijos, incluso si el DHCPv6 está correctamente configurado. Implementar protección de capa 2 (RA Guard en switches compatibles), limitar puertos de infraestructura y supervisar los anuncios reales. No bloquear indiscriminadamente ICMPv6: Neighbor Discovery, detección de ruta y otras funciones esenciales dependen de él. Separar redes de invitados y administración mediante VLAN y reglas de acceso, evitando publicar prefijos en interfaces no deseadas.

50.36. Rendimiento, periodicidad y compatibilidad de dispositivos

RA es un mecanismo liviano, pero la frecuencia de anuncios, cambios de prefijo, múltiples routers y sistemas con soporte parcial pueden aumentar incidencias. Los intervalos predeterminados suelen ser apropiados para redes normales; para necesidades especiales medir tráfico y tiempos de detección de fallos. No diseñar una infraestructura únicamente desde el comportamiento de un sistema operativo: validar con equipos Windows, Linux y los dispositivos móviles previstos en la organización.

50.37. Plan de cambios y reversión

Antes de modificar Router Mode, Router Lifetime, DNS Servers o subredes, registrar el estado previo y realizar una copia cifrada de la configuración. Identificar equipos que dependen de DHCPv6, SLAAC o servidores DNS por RA. Aplicar primero a una VLAN piloto; conservar una sesión de administración independiente y, si la red pierde conectividad IPv6, restaurar el modo y los parámetros anteriores. Tras revertir, algunos clientes requieren esperar la expiración del RA anterior o renovar manualmente su configuración.

50.38. Matriz de aceptación operativa

Prueba	Resultado aceptable	Evidencia neutra
RS / RA en VLAN	Se reciben anuncios con el modo previsto.	Captura sin direcciones reales.
Dirección IPv6	Cliente forma/recibe dirección válida.	Prefijo y tipo de asignación.
Ruta predeterminada	Siguiente salto correcto y operativo.	Resumen de rutas sin identificadores.
DNS por RA/DHCPv6	Resuelve nombre interno y externo previsto.	Éxito de consultas A/AAAA.
Transición de prefijo	Dirección nueva y caducidad antigua coherentes.	Prueba piloto de renumeración.
HA / doble router	Cambio al equipo disponible dentro del objetivo.	Tiempo medido y estados.
NAT64 opcional	Alcanza servidor IPv4-only desde IPv6.	Verificación de flujo de traducción.

50.39. Reglas de firewall e ICMPv6 imprescindibles

Router Advertisement y Router Solicitation forman parte de ICMPv6 y no requieren abrir un puerto TCP o UDP. La protección de entrada debe impedir anuncios de routers no autorizados pero permitir los mensajes de Neighbor Discovery necesarios para que los clientes localicen el router y mantengan vecinos. En una VLAN interna, permitir únicamente la conectividad IPv6 que requieran los usuarios, aplicando reglas de paso específicas a servicios y destinos. Evitar bloquear todo ICMPv6 para “endurecer” la red: rompe funciones esenciales y dificulta el diagnóstico de Path MTU Discovery.

50.40. Interoperabilidad: selección orientativa por perfil de dispositivos

Perfil de clientes	Modo candidato	Comprobación antes de producción
Equipos de escritorio compatibles con DHCPv6	Managed o Assisted	Concesión DHCPv6, RA y resolución DNS.
Móviles con direccionamiento SLAAC	Unmanaged o Assisted	Autoconfiguración de GUA y RDNSS.
Segmento mixto de dispositivos	Assisted	Convergencia de DNS y reglas por sistema operativo.
Infraestructura con direcciones estáticas	Router Only (según diseño)	Router aprendido y dirección configurada manualmente.
Sin clientes IPv6 gestionados	Disabled	Ausencia de anuncios no previstos.

Perfil de clientes	Modo candidato	Comprobación antes de producción
IPv6-only con salida IPv4 por NAT64	Managed/Assisted/Stateless DHCP	Prefijo, DNS64, NAT64 y RDNSS operativos.

50.41. Procedimiento de renumeración IPv6 sin interrupciones innecesarias

1. Inventariar el prefijo de salida y el nuevo prefijo asignable, sin retirar todavía el utilizado por los clientes.
2. Comprobar rutas, DNS y firewall para el nuevo prefijo en un entorno piloto, manteniendo coexistencia temporal donde sea viable.
3. Publicar el nuevo prefijo por RA y verificar que los clientes forman nuevas direcciones y rutas coherentes.
4. Reducir Preferred Lifetime del prefijo antiguo según la estrategia de renumeración, manteniendo Valid Lifetime suficiente para conexiones existentes.
5. Revisar DNS de registros AAAA, ACLs, VPN y servicios publicados; validar acceso desde redes externas y locales.
6. Retirar el prefijo antiguo únicamente tras comprobar el fin de las dependencias y los tiempos de caducidad.

50.42. Hoja de comprobación de cambios de Router Advertisement

Cada modificación debería registrar: interfaz y VLAN funcional, motivo del cambio, modo antes/después, origen del prefijo, elección de DNS, valor de los cinco temporizadores, existencia de NAT64/HA, equipos de prueba, responsable de validación y método de vuelta atrás. Las evidencias deben conservar únicamente datos anonimizados. Una incidencia de “IPv6 lento” exige distinguir fallo de DNS, pérdida de ruta, prefijo caducado y bloqueo de tráfico, no únicamente reiniciar el servicio.

50.43. Glosario de términos esenciales

Término	Significado
RA / RS	Anuncio / Solicitud ICMPv6 de router.
SLAAC	Autoconfiguración de direcciones IPv6 sin concesión DHCPv6.
M, O, A, L	Flags de gestión, otras opciones, autoconfiguración y alcance on-link.
RDNSS / DNSSL	Publicación de DNS y sufijos de búsqueda dentro de RA.
DHCPv6-PD	Delegación de prefijos desde una red aguas arriba.
PREF64 / DNS64 / NAT64	Anuncio del prefijo, síntesis DNS y traducción de familias IP.
CARP / link-local	Dirección virtual redundante y dirección local al enlace.

50.44. Lectura práctica de un anuncio Router Advertisement

Para analizar un RA conviene separar cuatro niveles: el encabezado ICMPv6 identifica la presencia del router; Router Lifetime y Router Preference condicionan la ruta por defecto; las opciones de prefijo aportan A y L junto con Valid/Preferred Lifetime; por último, RDNSS, DNSSL y PREF64 comunican funciones opcionales. Una dirección IPv6 visible en el equipo no demuestra que el RA sea correcto: puede proceder de configuración estática, de un anuncio previo o de otro router. Registrar de forma anónima los campos y comparar con la política esperada.

Dato observado en RA	Interpretación	Qué comprobar
M=1, O=1, A=0	Se solicita configuración de direcciones con DHCPv6.	Hay DHCPv6 disponible y compatible con los clientes.

Dato observado en RA	Interpretación	Qué comprobar
M=0, O=0, A=1	Dirección SLAAC sin indicación de DHCPv6.	Prefijo /64 válido; RDNSS si se necesita DNS.
Router Lifetime = 0	El emisor no debe usarse como router predeterminado.	Existe otra ruta prevista o configuración manual.
Preferred < Valid	Dirección puede quedar obsoleta antes de invalidarse.	Renumeración y continuidad de las conexiones.
DNS RDNSS presente	El RA anuncia servidores DNS.	Cliente interpreta la opción y DNS responde.
PREF64 presente	El RA comunica el prefijo de traducción.	Existe traductor NAT64 y DNS64 coherentes.

50.45. Laboratorio de validación comparada sin afectar a producción

1. Preparar una VLAN aislada, con un único router anunciador y direccionamiento de laboratorio para documentación.
2. Arrancar dos sistemas cliente con capacidades IPv6 diferentes y comprobar que ambos reciben Router Advertisements.
3. Ensayar Unmanaged: registrar dirección SLAAC, ruta por defecto y la presencia o ausencia de DNS por RA.
4. Ensayar Managed con DHCPv6 disponible y comprobar si los clientes pueden obtener dirección y opciones; documentar incompatibilidades.
5. Ensayar Assisted y observar si coexisten direcciones SLAAC y concesiones DHCPv6; registrar la fuente del DNS.
6. Cambiar de forma controlada Router Priority y Router Lifetime en un entorno de dos routers; medir convergencia.
7. Devolver el laboratorio a su estado inicial y validar que no quedan rutas, prefijos ni servidores DNS anunciados indebidamente.

50.46. Criterios de puesta en producción: decisión y responsabilidad

Un cambio RA se considera correctamente implantado cuando se verifican, por separado, dirección del cliente, ruta por defecto, resolución DNS, conectividad a destinos IPv6 y accesos internos. Si existen clientes que solo soportan SLAAC, los modos Managed o Router Only pueden producir pérdida de servicio aunque el servidor DHCPv6 informe concesiones correctas para otros equipos. Si la red depende de NAT64, la prueba debe incluir también un destino exclusivamente IPv4, para distinguir fallos de prefijo PREF64, síntesis DNS64 y reglas de traducción. La aceptación debe considerar el comportamiento con cortes del router, reinicio de un cliente y caducidad de los tiempos anunciados.

50.47. Referencias técnicas y documentación oficial

Netgate. IPv6 Router Advertisements (servicio, modos, DNS y tiempos). Abrir documentación oficial

Netgate. DHCPv6 Server y requisitos de anuncios RA. Abrir documentación oficial

Netgate. Configuring NAT64 for IPv6-only Clients. Abrir documentación oficial

Netgate. High Availability Configuration Example. Abrir documentación oficial

Referencias normativas: IETF RFC 4861 (Neighbor Discovery), RFC 4862 (autoconfiguración SLAAC), RFC 8106 (DNS por RA) y RFC 8781 (PREF64). Los campos efectivos pueden variar entre versiones de pfSense Plus y sus valores deben confirmarse en el equipo antes de cambiar una red operativa.

51 Services → SNMP

Supervisión de sistemas · consultas · traps · MIB · seguridad de acceso

El servicio SNMP integrado de pfSense Plus permite supervisar desde una plataforma centralizada el estado y diversos contadores del firewall. El administrador decide qué módulos MIB activar, en qué interfaz responder y si emitir notificaciones de eventos. Una implantación correcta exige, además de habilitar el daemon, limitar de forma estricta quién puede consultarlo.



Figura 51.1. Diferencia entre polling del supervisor y notificaciones SNMP de un dispositivo.

51.1. Objetivo y alcance de la funcionalidad

SNMP (Simple Network Management Protocol) permite leer objetos organizados por identificadores OID. En pfSense Plus, el servicio base se implementa mediante bsnmpd, que expone información del sistema y de módulos cargables. Es útil para obtener visibilidad de interfaces, consumo de recursos, contadores de PF y disponibilidad del servicio, pero no sustituye los registros, los flujos IPFIX ni las comprobaciones activas de aplicaciones.

51.2. Ruta exacta de administración y estructura de pantalla

Ruta: Services → SNMP. La página se organiza en SNMP Daemon, SNMP Daemon Settings, SNMP Traps Enable, SNMP Modules e Interface Binding. La descripción siguiente distingue expresamente los campos entregados de las opciones que aparecen al activar las traps, contrastadas con la documentación oficial de Netgate.

Sección	Finalidad	Elemento principal
SNMP Daemon	Arrancar o detener el servicio.	Enable
SNMP Daemon Settings	Definir puerto e identificación legible.	Polling Port, Location, Contact, Community
SNMP Traps Enable	Autorizar avisos salientes.	Enable y parámetros condicionales
SNMP Modules	Seleccionar conjuntos de métricas.	MibII, Netgraph, PF, Host Resources, UCD, Regex
Interface Binding	Restringir IPs locales de escucha.	Internet Protocol y Bind Interfaces

51.3. Fundamentos: manager, agente, OID y MIB

El manager o NMS consulta a intervalos regulares al agente SNMP que se ejecuta en el firewall. Un OID identifica un elemento concreto (por ejemplo, uptime, una interfaz o su volumen de tráfico). Una MIB describe el significado de esos objetos. Una tabla de OIDs puede cambiar de disponibilidad dependiendo de los módulos cargados y de la versión del sistema.

Concepto	Qué significa	Uso operativo
Manager / NMS	Herramienta central de supervisión.	Consulta, almacena series y dispara alertas.
Agente	Daemon bsnmpd del firewall.	Responde a consultas autorizadas.

Concepto	Qué significa	Uso operativo
GET / GETNEXT	Obtiene una variable o avanza en una tabla.	Sondeo selectivo.
WALK	Recorre una rama mediante sucesivas consultas.	Descubrimiento de OIDs.
TRAP	Aviso espontáneo del agente al receptor.	Eventos según módulos y configuración.
MIB / OID	Definición y dirección de objetos de gestión.	Interpretación de métricas.

51.4. Puertos, direcciones y diferencia entre consulta y trap

La consulta SNMP del servicio integrado utiliza UDP/161 de manera predeterminada. Los avisos trap se envían normalmente a UDP/162, que debe estar escuchando en el colector, no necesariamente en pfSense. La captura contiene opciones de escucha en IPv4, IPv6 o ambos; la disponibilidad efectiva depende de las interfaces configuradas.

ATENCIÓN — No exponer el servicio a Internet
Una comunidad compleja no protege frente a la interceptación de SNMPv1/v2c. Limite la escucha a una red de gestión y cree reglas que permitan únicamente el supervisor autorizado. No abra UDP/161 desde redes no confiables.

51.5. SNMP Daemon → Enable

“Enable the SNMP Daemon and its controls” activa bsnmpd. Desmarcarlo detiene la respuesta del agente y la emisión de traps asociadas. Tras cambiar este control debe guardarse la configuración y comprobar Status → Services. No afecta a las funciones normales de enrutamiento del firewall, aunque sí genera una interrupción de observabilidad para la herramienta NMS.

51.6. SNMP Daemon Settings → Polling Port

Determina el puerto UDP en que bsnmpd recibe consultas; el valor estándar es 161. Si se utiliza uno no estándar, la plataforma supervisora debe consultar explícitamente ese puerto y las reglas del firewall deben reflejarlo. Cambiarlo sin coordinar el NMS provoca errores de conexión que pueden confundirse con una caída del firewall.

51.7. SNMP Daemon Settings → System Location

Texto descriptivo que un cliente puede recuperar en la variable de localización del sistema. Es útil para clasificar equipos por centro lógico o ubicación genérica. Evite nombres internos sensibles, armarios exactos, direcciones físicas o cualquier detalle innecesario: el contenido es información que el servicio revela a quien puede consultar el agente.

51.8. SNMP Daemon Settings → System Contact

Cadena informativa para identificar al equipo o grupo responsable. Puede ser un alias funcional no identificativo. No habilita notificaciones ni crea usuarios: es solo un campo de información visible vía SNMP. Conviene mantenerlo coherente con el inventario de activos.

51.9. SNMP Daemon Settings → Read Community String

Secreto compartido que permite consultar al agente por SNMP basado en comunidad. No es una cuenta individual y, en las versiones SNMPv1/v2c, no proporciona confidencialidad criptográfica ni identidad por operador. Debe ser largo, distinto del valor conocido “public”, mantenerse en un gestor de secretos y configurarse exactamente igual en el sistema supervisor. Esta interfaz expone una comunidad de lectura y no constituye un sistema de usuarios SNMPv3.

ATENCIÓN — Evitar credenciales reales en documentación
No copie comunidades de producción en manuales, capturas, sistemas de tickets ni comandos almacenados en el historial. Los ejemplos de este capítulo usan marcadores ficticios y direcciones TEST-NET reservadas para documentación.

51.10. SNMP Traps Enable → Enable

“Enable the SNMP Trap and its controls” permite que el daemon origine avisos hacia un receptor. No supone que el firewall genere alarmas por cualquier incidente: los eventos disponibles dependen del módulo cargado y de sus implementaciones. Por ejemplo, Netgate cita cambios de estado de enlaces cuando está activo MibII.

51.11. SNMP Traps → campos condicionales al activar el envío

Campo documentado	Significado	Precaución
Trap server	Servidor receptor, expresado como hostname o IP.	Verificar resolución DNS y ruta de salida.
Trap server port	Puerto UDP del colector; normalmente 162.	Debe coincidir con el listener real.
SNMP trap string	Cadena enviada en las traps.	Tratar como un valor secreto y no publicarlo.

Estos tres controles no figuran desplegados en el escenario descrito porque la opción de traps está inicialmente cerrada; su existencia y descripción proceden de la documentación oficial. Para asegurar la recepción hay que probar el evento real y verificar el registro del colector; la disponibilidad de un campo no demuestra por sí sola que se estén enviando avisos.

51.12. SNMP Modules: activación y coste operativo

Los módulos añaden árboles MIB. Cada módulo introduce objetos y cierta carga de memoria, procesamiento o consulta; Netgate recomienda habilitar solo los necesarios. Una aplicación supervisora puede necesitar MIBs específicas para traducir OIDs en descripciones legibles. Tras desactivar un módulo, los OIDs dependientes dejarán de responder o desaparecerán del descubrimiento.

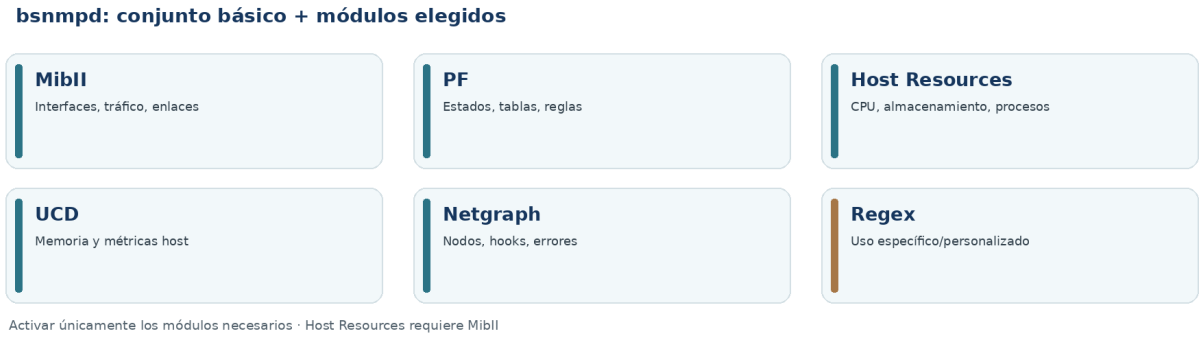


Figura 51.2. Seis módulos de bsnmpd y familias de información que proporcionan.

51.13. MibII: estadísticas estándar e interfaces

MibII implementa información de red e interfaces: estado de enlaces, direcciones, contadores de bytes y errores, entre otros. Constituye la base del descubrimiento de puertos por muchos sistemas NMS. Los índices de interfaz deben verificarse periódicamente, especialmente después de modificaciones de hardware o asignaciones virtuales.

51.14. Netgraph: nodos, enlaces lógicos y errores

Ofrece métricas del subsistema netgraph de FreeBSD, como nombres de nodos, estados, hooks, peers y errores. Puede ser útil en diagnósticos de funciones que emplean este mecanismo. No debe asumirse que todos los módulos o túneles de la plataforma se representan mediante netgraph.

51.15. PF: reglas, estados, tablas y colas

Expone información relacionada con el motor PF, incluyendo conjuntos de reglas, estados, interfaces, tablas y colas ALTQ. Resulta especialmente valioso para vigilar consumo de estados y comportamiento de filtrado. Los OIDs concretos dependen de las MIB disponibles; una métrica vista en un NMS debe cotejarse con Diagnostics → States o los paneles del firewall antes de utilizarse para alertas críticas.

51.16. Host Resources: inventario y recursos del host

Aporta información de uptime, carga, procesos, almacenamiento y dispositivos, según el soporte del agente. Netgate establece que Host Resources requiere MibII: si este último está desmarcado y se activa Host Resources, se activará automáticamente MibII. Esta dependencia debe quedar documentada al optimizar módulos.

51.17. UCD: contadores complementarios

El módulo UCD publica valores de la familia UCD-SNMP-MIB: memoria, capacidad de almacenamiento y ciertos indicadores del sistema. Puede complementar a Host Resources. Su existencia no equivale a disponer de todo el árbol NET-SNMP ni de cualquier contador ofrecido por otros sistemas operativos.

51.18. Regex: uso especializado y limitaciones

Módulo reservado por Netgate para casos avanzados o personalizaciones, con capacidad para extraer contadores desde archivos de registro y otros textos. No es un motor de expresiones regulares utilizable desde este formulario ni una opción recomendable para habilitar de forma indiscriminada. Requiere conocer el código y el origen de las métricas.

51.19. Interface Binding → Internet Protocol

Selección	Comportamiento esperado	Cuándo utilizar
IPv4	Escuchar consultas por IPv4.	NMS únicamente IPv4.
IPv6	Escuchar consultas por IPv6.	Gestión y ruta IPv6 validadas.
IPv4+IPv6	Atender por ambas familias.	Supervisor dual-stack y ACL de firewall para ambas.

Seleccionar IPv6 no abre por sí solo el tráfico: se necesita conectividad, direcciones de escucha y reglas apropiadas. Si la supervisión no utiliza una familia IP, conviene no ampliar innecesariamente la exposición del servicio.

51.20. Interface Binding → Bind Interfaces

La selección restringe las IP locales a las que se asocia el daemon. En la pantalla copiada aparecen All, WAN, LAN y Localhost; en otros entornos pueden verse interfaces adicionales y direcciones virtuales IP Alias/CARP con IP válida. Elegir All puede ampliar la superficie de escucha. Localhost facilita pruebas desde el propio firewall, pero no una consulta directa del NMS desde otro host.

El enlace a una interfaz específica también ayuda en supervisión a través de VPN, evitando problemas de dirección de origen al responder. Binding no sustituye a las reglas de Firewall → Rules: hay que aplicar ambos controles.

51.21. Diagrama de defensa: binding, firewall y comunidad



Figura 51.3. Tres capas para restringir las consultas y alternativa para necesidades SNMPv3.

51.22. SNMPv1, SNMPv2c y SNMPv3: decisión de arquitectura

Versión / implementación	Seguridad	Recomendación
SNMPv1/v2c con bsnmpd	Comunidad sin cifrado; los datos pueden ser observados en tránsito.	Solo gestión controlada o protegida por VPN.
SNMPv3 con paquete NET-SNMP	Admite autenticación y cifrado según perfil configurado.	Preferible para redes de gestión exigentes.
Consultar por VPN	Protege transporte de v1/v2c dentro de un túnel adecuadamente configurado.	No sustituye a reducir acceso o rotar secretos.

NET-SNMP es un paquete independiente de la pantalla integrada; su instalación y administración tienen su propio procedimiento. Antes de emplearlo, revisar la compatibilidad de la versión y evitar que dos daemons intenten escuchar en el mismo puerto/IP.

51.23. Procedimiento 1: habilitar supervisión exclusivamente en la red de gestión

- Identificar el host NMS autorizado y la interfaz interna de administración; registrar una copia de la configuración.
- En Services → SNMP activar Enable; conservar UDP/161 salvo requisito documentado.
- Establecer System Location/Contact genéricos y una comunidad larga almacenada de forma segura.
- Activar MibII, PF y solo los módulos adicionales exigidos por la plataforma supervisora.
- Seleccionar IPv4, IPv6 o ambos según el NMS; en Bind Interfaces elegir únicamente la IP/interfaz de gestión.
- En Firewall → Rules permitir UDP/161 desde el supervisor al firewall y denegar el acceso desde otras redes.
- Guardar; comprobar Status → Services; probar un snmpget y un snmpwalk desde el supervisor autorizado.
- Desde un origen no autorizado comprobar que las consultas no reciben respuesta y registrar el resultado.

51.24. Procedimiento 2: activar avisos SNMP trap hacia un colector

- Confirmar un receptor que escucha UDP/162 y su capacidad para analizar los OIDs de la plataforma.
- Habilitar SNMP Traps Enable y completar Trap server, Trap server port y Trap string.
- Cargar el módulo adecuado para el evento esperado; por ejemplo, MibII para cambios de enlace.
- Validar DNS/ruta y reglas de red si el colector está en otra subred o VPN.
- Guardar los cambios y generar únicamente un evento de prueba autorizado, sin interrumpir enlaces productivos.
- Confirmar que el colector recibe la notificación con fecha y contexto; documentar lo observado.

51.25. Procedimiento 3: supervisar por VPN sin exponer SNMP en WAN

Mantener el agente ligado a una dirección interna alcanzable por el túnel. Permitir en las reglas de la VPN únicamente al NMS remoto hacia la IP del firewall con destino UDP/161. Verificar ruta de retorno y que la respuesta usa la dirección esperada. Un diagnóstico de error por “timeout” debe comenzar por una captura en la interfaz correspondiente y la comprobación de reglas. Evite publicar UDP/161 en NAT para resolver un problema de conectividad a través de VPN.

51.26. Procedimiento 4: pasar de SNMP básico a SNMPv3

Diseñar la migración en el NMS antes de retirar la configuración actual: identificar OIDs realmente utilizados, verificar que el paquete NET-SNMP está disponible y planificar credenciales SNMPv3 de tipo authPriv. Configurar el nuevo agente en una IP/puerto que no colisione, validar métricas y alertas, y retirar

el acceso basado en comunidad. La interfaz de Services → SNMP no muestra campos de usuarios, algoritmos de autenticación ni claves SNMPv3; no debe presentarse como si fuera capaz de configurarlos.

51.27. Prueba controlada mediante snmpget y snmpwalk

Los comandos de ejemplo se ejecutan desde un equipo supervisor de prueba. 192.0.2.1 pertenece al rango TEST-NET-1 reservado para documentación y NO corresponde a ninguna instalación real. La comunidad mostrada es un marcador, no un secreto utilizable.

```
snmpget -v2c -c 'COMUNIDAD_DE_EJEMPLO' 192.0.2.1 1.3.6.1.2.1.1.3.0
snmpwalk -v2c -c 'COMUNIDAD_DE_EJEMPLO' 192.0.2.1 1.3.6.1.2.1.2.2
snmpwalk -v2c -c 'COMUNIDAD_DE_EJEMPLO' 192.0.2.1 1.3.6.1.2.1.25.2.3
```

La primera consulta obtiene el tiempo de actividad. Las siguientes recorren información de interfaces y almacenamiento si el módulo que expone esas ramas está habilitado. Un fallo “No Such Object” no equivale a un timeout: puede significar que el OID no existe, no está implementado o no está cargado.

51.28. Comprobación de OIDs y continuidad histórica de contadores

OID de referencia	Información	Interpretación
1.3.6.1.2.1.1.3.0	sysUpTime.0	Tiempo de actividad del agente; reinicios reinician la serie.
1.3.6.1.2.1.2.2	ifTable	Interfaces; validar que las etiquetas del NMS apuntan a la interfaz correcta.
1.3.6.1.2.1.25.2.3	hrStorageTable	Almacenamiento, cuando Host Resources está cargado.

Los contadores de 32 bits pueden desbordarse en enlaces rápidos. No asumir disponibilidad de contadores High Capacity de 64 bits: comprobar con snmpwalk que el agente y el módulo ofrecen el OID requerido. También conviene reconstruir las asociaciones de ifIndex cuando se añaden o reemplazan interfaces, y utilizar nombres/descripciones para una correlación robusta.

51.29. Diseño empresarial: métricas y alertas prioritarias

Objeto supervisado	Métrica básica	Alerta orientativa
Interfaces WAN/LAN	ifOperStatus, octetos, errores.	Cambio de enlace o errores anormales.
Filtro PF	Estados, tablas y uso de reglas.	Crecimiento sostenido o acercamiento a umbrales.
Recursos	CPU, memoria, disco.	Saturación o tendencia persistente.
Disponibilidad	Respuesta SNMP y sysUpTime.	Pérdida de visibilidad o reinicio.
Traps	Eventos emitidos por módulos.	Aviso inmediato, sujeto a verificación.

No derive alarmas únicamente de un valor instantáneo: combine umbrales, persistencia y tendencias. Una falta de respuesta SNMP no demuestra necesariamente que el firewall esté apagado; puede deberse a rutas, reglas, cambios de comunidad o a un agente detenido.

51.30. Frecuencia de sondeo, capacidad y carga

Un intervalo razonable de partida para indicadores generales es de unos 60 segundos, ajustándolo al número de objetos y a la carga observada. Evitar los snmpwalk completos muy frecuentes: pueden recorrer cientos de valores y consumir recursos del agente o de la red. Las traps complementan el polling, pero no lo reemplazan porque usan UDP y no garantizan entrega.

51.31. Resolución de problemas: el supervisor recibe timeout

Comprobación	Síntoma	Corrección
Estado bsnmpd	El daemon figura detenido.	Revisar Enable y Status → Services.

Comprobación	Síntoma	Corrección
Bind Interfaces	Solo escucha en otra IP.	Seleccionar dirección apropiada.
Protocolo IP	NMS IPv6 y binding solo IPv4.	Alinear Address Family y conectividad.
Firewall Rules	UDP/161 bloqueado.	Permitir desde NMS hacia This Firewall.
Puerto	NMS sondea puerto distinto.	Sincronizar port/ACL.
Ruta VPN	Paquetes llegan, respuestas no retornan.	Comprobar rutas, IP de origen, captura.
Comunidad	Agente no acepta consulta.	Verificar la coincidencia con secreto seguro.

51.32. Resolución de problemas: OID ausente o valor incoherente

Si una consulta llega y obtiene respuesta, pero falta un árbol, verificar si el módulo correspondiente está activado y si el OID es compatible con bsnmpd. No usar una plantilla de Zabbix, PRTG u otro NMS que presuponga NET-SNMP sin comprobarla. Para variables que no coinciden con la GUI, verificar la cadencia de actualización, los índices de interfaz y las unidades de medida, en especial bytes frente a bits.

51.33. Resolución de problemas: traps sin recepción

Confirmar que están habilitadas, que existe al menos un evento susceptible de generarse, que el receptor escucha UDP/162 (o puerto alternativo configurado) y que el firewall puede alcanzar su dirección. Revisar la configuración del colector, los filtros de red y el protocolo en tránsito. Usar Diagnostics → Packet Capture permite observar si los datagramas salen realmente del firewall.

51.34. Comprobaciones mediante Diagnostics → Packet Capture

En Diagnostics → Packet Capture elegir la interfaz por la que se espera que circule el tráfico y un filtro ajustado a UDP y al puerto de consulta o traps. Una captura en la entrada ve paquetes incluso si la regla del firewall los bloqueará; por ello conviene cotejar la captura con el registro de reglas y, cuando proceda, una segunda captura de salida. Evitar capturar tráfico innecesario en redes productivas.

51.35. Seguridad: inventario, mínimos privilegios y rotación

- Elegir una interfaz de gestión y limitar quién tiene acceso a UDP/161 mediante Firewall → Rules.
- No utilizar “public”, secretos reutilizados ni comunidades impresas en documentación.
- Separar la gestión del resto de segmentos y preferir un túnel autenticado cuando el NMS esté remoto.
- Rotar la comunidad ante sospecha de exposición y coordinar el cambio con el supervisor.
- Revisar después de cambios de VLAN, VPN y Multi-WAN qué interfaces han quedado escuchando.
- Restringir el acceso al receptor de traps y evitar nombres, contactos o ubicaciones excesivamente precisas.

51.36. Recomendaciones para equipos virtualizados y sistemas de monitorización

En máquinas virtuales, los contadores de red dependen de los adaptadores virtuales y del hipervisor; su correlación debe comprobarse. La carga percibida por el invitado puede diferir del consumo del host. En una plataforma como Zabbix o PRTG, usar plantillas calibradas para OIDs realmente disponibles, establecer dependencias de alarma y evitar duplicar alertas por pérdida del agente y pérdida completa de ruta.

51.37. Plan de cambio seguro y reversión

Antes del cambio, anotar el puerto, el binding de escucha y la configuración de monitorización (sin documentar la comunidad real). Probar desde el NMS autorizado. Si se pierde la supervisión, revertir únicamente las opciones SNMP modificadas y la regla específica, sin deshabilitar las reglas generales de

administración. Tras una rotación de comunidad, actualizar los monitores antes de retirar el secreto anterior. Si se desactiva el servicio, dejar constancia para no interpretar una caída prevista como incidente.

51.38. Ficha de verificación antes de poner SNMP en producción

Prueba	Criterio de aceptación	Resultado
Servicio	bsnmpd en Running con módulo requerido.	☐ Conforme ☐ Revisar
Consulta autorizada	snmpget y snmpwalk responden por la IP correcta.	☐ Conforme ☐ Revisar
Consulta no autorizada	Sin respuesta por políticas de acceso.	☐ Conforme ☐ Revisar
Contadores	Valores plausibles y mapeo de interfaces correcto.	☐ Conforme ☐ Revisar
Traps	Colector recibe evento de prueba si se utilizan.	☐ Conforme ☐ Revisar
Recursos	Sin incremento significativo tras sondeo.	☐ Conforme ☐ Revisar
Reversión	Procedimiento aprobado y practicable.	☐ Conforme ☐ Revisar

51.39. Errores habituales que conviene evitar

- Confundir tener SNMP habilitado con tener reglas de acceso restrictivas.
- Asumir que “Read Community String” cifra las respuestas.
- Publicar UDP/161 por la WAN sin necesidad empresarial.
- Activar módulos indiscriminadamente o interpretar un OID ausente como avería general.
- Dar por garantizada la entrega de traps sin verificar el colector.
- Usar una plantilla de métricas sin validar OIDs, unidades e índices después de cambios.

51.40. Elegir entre SNMP, syslog, captura e IPFIX

Fuente	Qué permite observar	Limitación principal
SNMP	Estados, recursos y contadores comparables en el tiempo.	No guarda el detalle de cada paquete ni sustituye los logs.
Traps SNMP	Avisos rápidos de determinados cambios del agente.	UDP no garantiza recepción y la cobertura depende del módulo.
Syslog	Mensajes de eventos, errores y servicio.	Puede requerir correlación y retención central.
IPFIX / NetFlow	Flujos y conversaciones agregadas en el firewall.	No revela contenido de paquetes.
Packet Capture	Prueba puntual de paquetes y protocolos en tránsito.	No resulta adecuado como histórico permanente.

Un sistema de observabilidad maduro combina estas fuentes. SNMP es apropiado para disponibilidad y capacidad; los registros permiten investigar errores y la captura verifica tráfico específico. Una alerta de interfaz caída debe cotejarse con su contexto: no toda falta de respuesta SNMP equivale a una interrupción real del servicio.

51.41. Criterios para fijar alarmas y umbrales fiables

Defina una línea base antes de crear alarmas: frecuencia de sondeo estable, carga habitual, pérdida ocasional de paquetes, evolución de memoria y comportamiento normal del enlace. Para evitar falsos positivos, utilice varias muestras consecutivas y aplique periodos de mantenimiento cuando se realizan

cambios programados. Documente un responsable funcional, el impacto y el procedimiento de escalado de cada alarma; nunca convierta un simple OID ausente en una alerta de caída total.

51.42. Glosario esencial

Término	Definición
SNMP	Protocolo de supervisión de parámetros de dispositivos.
NMS	Network Management System; supervisor de equipos.
MIB	Descripción estructurada de variables de gestión.
OID	Identificador numérico de una variable o rama MIB.
Polling	Consulta programada iniciada por el supervisor.
Trap	Notificación no solicitada emitida por el agente.
bsnmpd	Agente SNMP integrado de FreeBSD utilizado por pfSense.
Community	Secreto compartido de acceso de SNMPv1/v2c.
Binding	Asociación del servicio a interfaces o IP locales.

51.43. Referencias técnicas y normativas

Documentación oficial de Netgate consultada:

- SNMP (servicio integrado, parámetros, traps, módulos y binding): https://docs.netgate.com/pfsense/en/latest/services/snmp.html
- Paquetes disponibles, net-snmp y soporte SNMPv3: https://docs.netgate.com/pfsense/en/latest/packages/list.html
- Estado de servicios: https://docs.netgate.com/pfsense/en/latest/monitoring/status/services.html
- Captura de paquetes y diagnóstico: https://docs.netgate.com/pfsense/en/latest/diagnostics/packetcapture/webgui.html
- Prácticas recomendadas de reglas: https://docs.netgate.com/pfsense/en/latest/firewall/best-practices.html
- IETF RFC 3411 y RFC 3418 (arquitectura y MIB SNMP); RFC 2790 (Host Resources MIB).

El contenido refleja los campos indicados en la pantalla de referencia y las opciones adicionales descritas por Netgate. La disponibilidad exacta de funciones puede variar según edición, versión y paquetes instalados.

52 Services → UPnP IGD & PCP

Mapeo automático de puertos · NAT · STUN · listas de acceso · supervisión y seguridad

El servicio UPnP IGD & PCP de pfSense Plus permite que determinados dispositivos y aplicaciones soliciten asignaciones temporales de puertos de entrada sin que un administrador cree manualmente cada redirección. Esta comodidad debe equilibrarse con un control explícito de interfaces, clientes y puertos: una petición aceptada puede modificar dinámicamente la exposición de servicios hacia Internet.

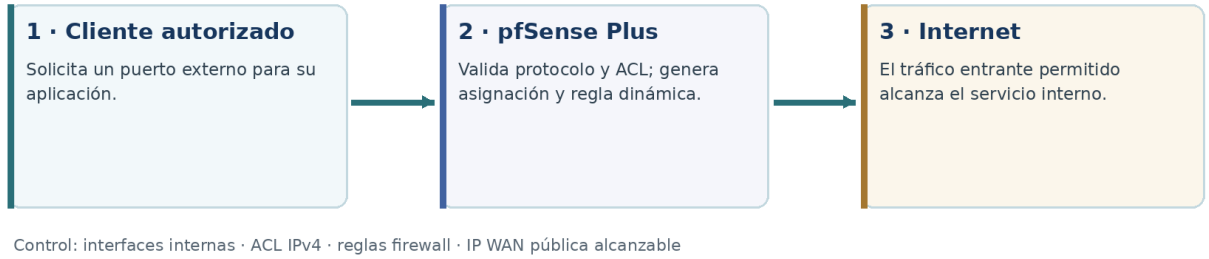


Figura 52.1. Esquema lógico: petición local, autorización del servicio y alcance de la asignación dinámica.

52.1. Objetivo, alcance y criterio de uso

Este capítulo explica Services → UPnP IGD & PCP, su motor miniupnpd, las condiciones de direccionamiento, los controles de acceso, la puesta en servicio y las comprobaciones posteriores. La función permite a ciertas aplicaciones negociar puertos variables; en entornos corporativos debe habilitarse solo para una necesidad delimitada y verificable.

52.2. Qué es un mapeo dinámico y qué modifica

Un mapeo vincula un puerto y protocolo de una dirección externa con un destino y puerto interno. El cliente solicita crear, renovar o eliminar esa relación; si la petición se admite, miniupnpd programa las entradas necesarias para el paso de tráfico en pfSense. No equivale a una regla NAT estática editada a mano: su presencia depende de la solicitud, la duración y el estado del servicio. El servicio también puede contemplar el tratamiento de NAT saliente que utiliza esos mismos puertos.

Elemento	Papel técnico	Implicación de administración
Cliente	Aplicación o dispositivo que solicita asignación.	Confiar solo en dispositivos concretos.
miniupnpd	Daemon que procesa UPnP IGD y PCP/NAT-PMP.	Revisar su ejecución y sus mensajes.
NAT/Firewall	Traducción y paso de conexiones admitidas.	No presuponer que una ACL sustituye al firewall.
Puerto externo	Puerto publicado en la dirección pública.	Evitar exposiciones no justificadas.
Puerto interno	Puerto del servicio que escucha en el destino.	Comprobar servicio y firewall del host.

52.3. Diferencia entre UPnP IGD, PCP y NAT-PMP

UPnP IGD se apoya en descubrimiento SSDP y en consultas de control HTTP/SOAP. PCP fue diseñado para solicitar información y cambios de mapeo a dispositivos de red; NAT-PMP es su predecesor y también se admite mediante la opción conjunta PCP/NAT-PMP. No son protocolos equivalentes ni todos los clientes implementan ambos. UPnP IGD se utiliza habitualmente en consolas y sistemas compatibles; PCP/NAT-PMP también está presente en dispositivos y aplicaciones del ecosistema Apple.

Tecnología	Canal de control	Uso más frecuente
UPnP IGD	SSDP/UDP 1900 y consultas HTTP/SOAP.	Descubrimiento y mapeos desde equipos y consolas.

Tecnología	Canal de control	Uso más frecuente
PCP	UDP 5351.	Solicitud explícita de mapeos por clientes compatibles.
NAT-PMP	Compatibilidad de PCP; UDP 5351.	Clientes anteriores a PCP.

52.4. Puertos utilizados y reglas que pueden ser necesarias

El daemon miniupnpd usa los siguientes puertos indicados por Netgate. Son puertos de control entre clientes y firewall, no los puertos de aplicaciones publicados dinámicamente. Si se ha eliminado la regla permisiva de LAN, existe una política de mínimos privilegios o se usa bridging, las reglas de entrada en el firewall deben permitir expresamente el tráfico de control requerido.

Transporte	Puerto	Función	Dónde se permite
UDP	1900	SSDP; descubrimiento UPnP IGD.	Desde el segmento de clientes autorizado, según destino multicast/broadcast.
TCP	2189	Servicio HTTP/SOAP del daemon.	Entre clientes UPnP autorizados y firewall.
UDP	5351	PCP y NAT-PMP.	Desde dispositivos PCP/NAT-PMP autorizados al firewall.

ATENCIÓN — No abrir los puertos de control desde Internet
Los puertos UDP/1900, TCP/2189 y UDP/5351 corresponden al plano de control local. No deben exponerse sin necesidad a WAN ni confundirse con los puertos de servicio que los clientes solicitan publicar.

52.5. Ruta de administración y organización de la pantalla

Abrir Services → UPnP IGD & PCP. Netgate sitúa esta opción en el menú Services cuando existe más de una interfaz asignada. La pantalla documentada contiene Service Description, Service Settings, External Address Settings, Advanced Settings y Service Access Control List. El botón Save guarda la configuración e inicia el servicio si está habilitado. El nombre y número de interfaces del selector dependen del equipo; este libro emplea únicamente denominaciones genéricas.

Bloque	Finalidad	Controles visibles
Service Description	Resumen del propósito del servicio.	Texto informativo, sin valores editables.
Service Settings	Activación, protocolos e interfaces.	Enable; UPnP IGD; PCP/NAT-PMP; External Interface; Internal Interfaces.
External Address Settings	Identificación de dirección externa.	Enable STUN; STUN Server; STUN Port; Override WAN Address.
Advanced Settings	Anuncio, colas y registro.	Download Speed; Upload Speed; Traffic Shaping; URL; Model; Logs; Uptime.
Service Access Control List	Política de solicitudes IPv4.	Default Deny; ACL Entries; Add.

52.6. Service Description: texto explicativo

Este apartado informa de que UPnP IGD y PCP facilitan coordinación local y creación autónoma de reglas NAT dinámicas. No habilita por sí mismo ningún protocolo. La capacidad de gestionar mapeos depende del control maestro, de los protocolos seleccionados, de las interfaces, del direccionamiento externo y de la autorización de cada solicitud.

52.7. Service Settings → Enable port mapping service

Control maestro «Enable». Marcado: permite iniciar miniupnpd, pero solo prestará el servicio de mapeo si se habilita al menos uno de los protocolos siguientes. Desmarcado: deshabilita las funciones del formulario según Netgate y deja de atender solicitudes de mapeo. Es recomendable mantenerlo desactivado como configuración inicial en redes sin consumidores identificados. Tras guardar, verificar Status → Services y la lista de asignaciones.

52.8. Service Settings → Allow UPnP IGD Port Mapping

Al marcar «UPnP IGD» se admiten peticiones de mapeo de clientes compatibles con Universal Plug and Play Internet Gateway Device. Si se desmarca, esa vía no acepta nuevas solicitudes, aunque el servicio maestro o PCP permanezcan habilitados. Activarlo únicamente cuando los equipos concretos lo requieran; una aplicación maliciosa del segmento podría aprovechar la misma capacidad si no existen restricciones.

52.9. Service Settings → Allow PCP/NAT-PMP Port Mapping

Al marcar «PCP/NAT-PMP» se admiten peticiones por PCP y el protocolo anterior NAT-PMP. Desmarcarlo inhibe ese canal de mapeo independientemente de UPnP IGD. La combinación de casillas depende del parque real de clientes: no existe obligación de activar ambos protocolos. Asegurar que el dispositivo o la aplicación pueda efectuar la solicitud y que la red permite UDP/5351.

52.10. Service Settings → External Interface

Selecciona la interfaz WAN de salida que contiene la puerta de enlace predeterminada. La documentación oficial exige una única WAN en ese papel; no se trata de un selector de grupo de gateways ni de un mecanismo automático de balanceo. El desplegable del equipo puede mostrar diferentes interfaces asignadas, pero no debe interpretarse que todas son válidas como WAN externa. Revisar dirección pública, puerta de enlace y ruta antes de guardar.

ATENCIÓN — Limitación importante con Multi-WAN
La configuración documentada vincula el servicio a una única interfaz WAN correspondiente a la ruta por defecto. En escenarios de balanceo, failover o policy routing, una solicitud local no garantiza que el retorno del tráfico siga la WAN elegida; comprobar rutas, NAT y entrada por la misma dirección antes de dar por válida la publicación.

52.11. Service Settings → Internal Interfaces

Selector múltiple de las interfaces donde residen los clientes que pueden comunicarse con miniupnpd: normalmente LAN o una VLAN de dispositivos autorizados. La interfaz puede mostrar varias opciones, incluidas interfaces de tránsito o loopback, que no deben seleccionarse simplemente por aparecer en la lista. Ctrl (Windows/Linux) o Command (macOS) permite seleccionar más de una. En un bridge, Netgate recomienda seleccionar únicamente la interfaz bridge que posee dirección IP.

Una interfaz incluida amplía la superficie desde la que el firewall atiende solicitudes. Para una red de invitados, dispositivos IoT o DMZ no confiables, la opción más segura es excluirla salvo requisito excepcional y debidamente aislado. No confundir «Internal Interfaces» con una ACL por equipo: la primera limita redes de escucha, la segunda limita peticiones IPv4 por parámetros.

52.12. Matriz de activación y resultado esperado

Maestro	UPnP IGD	PCP/NAT-PMP	Resultado general
No	Indiferente	Indiferente	Servicio desactivado.
Sí	No	No	Sin protocolo habilitado: no hay canal útil de mapeo.
Sí	Sí	No	Admite mapeo por UPnP IGD.
Sí	No	Sí	Admite solicitudes PCP y NAT-PMP.
Sí	Sí	Sí	Admite las dos familias; requiere ACL y perímetro adecuados.

52.13. Necesidad de dirección IP pública y NAT aguas arriba

La publicación entrante requiere una dirección IPv4 pública enrutable que reciba paquetes externos. Si la WAN de pfSense ya tiene esa dirección, el servicio puede identificarla directamente y los campos externos se dejan vacíos o desactivados. Si la WAN usa direccionamiento no público, miniupnpd rechaza mapeos hasta configurar una forma válida de identificar la dirección externa. Identificarla, sin embargo, no significa que exista una vía de entrada desde Internet: el equipo aguas arriba debe reenviar realmente el tráfico.

En accesos con NAT del operador o CGNAT sin redirección entrante disponible, ni STUN ni una dirección escrita manualmente convierten la conexión en accesible. En una red con NAT 1:1 o paso sin filtrado, sí puede funcionar si todas las entradas llegan a pfSense y se anuncia una dirección pública correcta.

52.14. External Address Settings → Enable STUN

«Use STUN to determine the external interface address and NAT type» consulta un servidor STUN externo para averiguar qué dirección pública ve el exterior y evaluar el comportamiento del NAT precedente. Es apropiado cuando existe NAT 1:1 con dirección pública dinámica y el equipo superior permite el tráfico entrante. Marcado: realiza la detección y prueba indicada; desmarcado: no efectúa esas consultas. Netgate advierte que el servicio desactiva el mapeo cuando el test concluye que las entradas no llegan a este firewall.

52.15. External Address Settings → STUN Server

Admite nombre DNS o dirección IP de un servidor STUN accesible. La documentación oficial cita, como ejemplos públicos, «stun.3cx.com» y «stun.counterpath.com»; la disponibilidad de servicios de terceros puede cambiar y debe comprobarse antes de su uso. Elegir un servidor autorizado por la política empresarial, considerar la consulta externa como un flujo de metadatos y garantizar resolución DNS y salida UDP desde pfSense.

52.16. External Address Settings → STUN Port

Puerto UDP del servidor STUN. El valor predeterminado indicado es 3478; debe coincidir con el servicio real del servidor elegido. La revisión oficial de pfSense Plus 25.07 indica que el campo STUN Port pasó a ser opcional; por ello, una interfaz concreta puede permitir dejarlo vacío. No interpretar vacío como puerto arbitrario: verificar el comportamiento en la versión instalada y confirmar en los logs que la detección funciona.

52.17. External Address Settings → Override WAN Address

Permite escribir manualmente la dirección pública enrutable que el servicio anuncia para las conexiones entrantes. Es aplicable, por ejemplo, a una IP estática pública en un router superior que redirige todas las entradas necesarias a pfSense, o a una IP pública alternativa configurada como Virtual IP. Si la WAN cambia de dirección y la excepción continúa fija, el servicio puede anunciar una IP equivocada. Este campo no crea por sí mismo rutas, direcciones virtuales, NAT 1:1 ni reglas en el router superior.

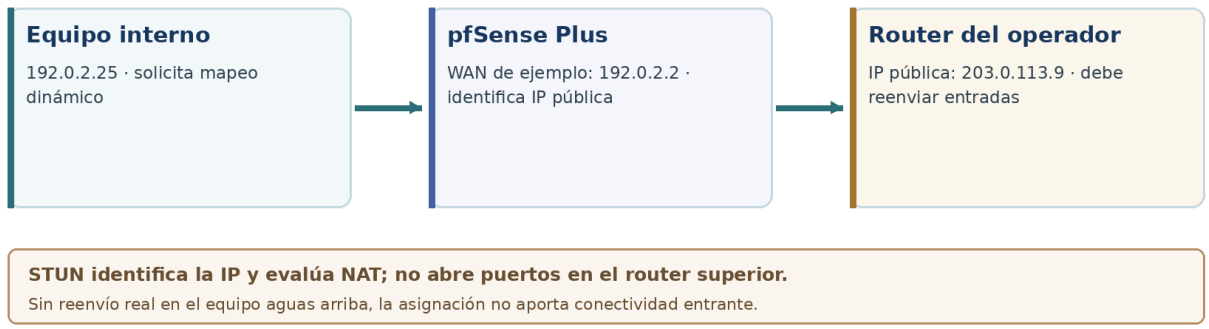


Figura 52.2. Doble NAT: la detección de dirección y el reenvío entrante son condiciones distintas. Todas las IP son ficticias y de documentación.

52.18. Advanced Settings → Download Speed

Valor de velocidad máxima de descarga comunicado a los clientes cuando consultan la capacidad del enlace, expresado en kbit/s. Si se deja sin establecer, se comunica la velocidad de enlace de la interfaz según Netgate. No configura el ancho de banda contratado, no garantiza caudal real ni aplica un límite de tráfico. Utilizar un valor declarado solo cuando el comportamiento del cliente lo justifique y documentar su unidad.

52.19. Advanced Settings → Upload Speed

Equivalente a Download Speed para la capacidad de subida, también en kbit/s. El valor predeterminado comunicado corresponde a la velocidad de enlace de la interfaz. No debe confundirse con un limitador, una reserva de calidad de servicio ni un test de capacidad. En accesos asimétricos, declarar valores estimados no sustituye al diseño de colas ni al control real de congestión.

52.20. Advanced Settings → Traffic Shaping

Campo para el nombre de una cola ALTQ de Traffic Shaping válida; las reglas dinámicas creadas por UPnP IGD & PCP dirigirán a ella el tráfico correspondiente. La opción documentada acepta ALTQ, no un Limiter. Las reglas generadas por miniupnpd existen fuera del conjunto normal de reglas de usuario y no pueden editarse individualmente como reglas manuales. Una cola de alta prioridad aplicada indiscriminadamente puede perjudicar servicios críticos; una cola de baja prioridad puede afectar a sesiones interactivas.

52.21. Advanced Settings → Custom Presentation URL

Dirección URL que el servicio presenta cuando un cliente consulta el enlace de administración del dispositivo, por ejemplo al navegar por dispositivos de red. En blanco, miniupnpd comunica la URL de la GUI del firewall. Cambiar este valor modifica la referencia anunciada, no la dirección en que realmente escucha el panel ni las ACL de acceso. Evitar divulgar una URL de gestión accesible desde segmentos innecesarios.

52.22. Advanced Settings → Custom Model Number

Texto personalizado presentado como número de modelo. En blanco, se comunica la versión de firmware vigente del equipo, según documentación oficial. Cambiar el dato anunciado no modifica el hardware ni la versión real. Puede utilizarse una etiqueta neutra por inventario, pero no debe presentarse como una medida de seguridad suficiente ni como ocultación garantizada de la versión.

52.23. Advanced Settings → Firewall Logs

La casilla «Log mapped connections» habilita el registro de las conexiones coincidentes con las reglas dinámicas creadas por el servicio. Desmarcada, esas conexiones no se registran por este ajuste concreto, aunque pueden existir otros logs o registros de denegación. Para consultarlos ir a Status → System Logs → Firewall. En fases de prueba es útil activarlo; en escenarios con tráfico elevado, evaluar el volumen de entradas y la retención antes de mantenerlo continuamente.

52.24. Advanced Settings → Uptime

Con «Report system uptime» marcado, las consultas de clientes devuelven el tiempo transcurrido desde el arranque del sistema. Desmarcado, que es el comportamiento predeterminado descrito, la respuesta refleja el tiempo activo del daemon. La selección solo modifica el dato anunciado y no reinicia el sistema ni el servicio. Al comparar métricas de disponibilidad conviene registrar qué semántica se eligió.

52.25. Service Access Control List → Default Deny

Cuando «Deny access to port mapping service by default» está activado, solo se aceptan peticiones que concuerden con reglas ACL permitidas. Si está desactivado, la política deja de ser denegación por defecto, lo que amplía el riesgo. La propia documentación oficial recomienda aplicar controles de acceso para restringir equipos y puertos. Antes de activar Default Deny debe existir al menos una entrada allow correcta para los clientes requeridos; de otro modo, estos perderán capacidad de solicitar mapeos.

52.26. Service Access Control List → ACL Entries: sintaxis y semántica

Las entradas se escriben como una orden de permiso o denegación, un puerto externo o intervalo, una dirección IP interna o red CIDR, y un puerto interno o intervalo. Restringen solicitudes de mapeo IPv4, NO tráfico IPv6. Es esencial distinguir el puerto solicitado en el exterior del puerto del servicio interno; pueden ser iguales o diferentes. Antes de guardar, verificar que los intervalos previstos corresponden al caso de negocio.

```
allow|deny  <puerto_externo_o_rango>  <IP_interna_o_CIDR>  <puerto_interno_o_rango>
```

Campo ACL	Ejemplo documental	Significado
Acción	allow	Autoriza la solicitud coincidente (deny la rechaza).
Puerto externo	20000-20020	Intervalo de puertos publicados solicitado.
IP/red interna	192.0.2.25	Destino interno autorizado; /CIDR admite segmento.
Puerto interno	20000-20020	Puertos internos que pueden mapearse.

52.27. Service Access Control List → Add y administración de entradas

El control «Add», identificado en la documentación con un icono de suma, incorpora otra línea ACL. Es imprescindible introducir en cada línea una regla íntegra y sintácticamente correcta. El listado resultante debe revisarse tras Save y probarse tanto con una solicitud aceptada como con otra que deba rechazarse. No se presupone un orden concreto de precedencia entre entradas solapadas sin comprobarlo en la versión operativa: evitar reglas contradictorias y superposiciones ambiguas.

52.28. Ejemplos reproducibles de ACL IPv4

Las direcciones de estos ejemplos pertenecen al bloque TEST-NET-1, reservado para documentación; no representan instalaciones reales ni son valores destinados a copiarse en producción.

```
allow 20000-20020 192.0.2.25 20000-20020
```

Autoriza al destino de ejemplo un conjunto reducido de puertos. El alcance exacto debe adecuarse al protocolo de la aplicación y a las peticiones reales.

```
deny 80 192.0.2.0/24 80
```

Ejemplo de rechazo de un mapeo que coincida con los puertos 80 externo e interno en una red documental. Por sí solo no constituye una política completa de puertos privilegiados.

```
allow 1024-65535 192.0.2.25 1024-65535
```

Ejemplo amplio comparable al de Netgate para puertos no privilegiados. Conviene preferir rangos más reducidos cuando el software y la operación lo permitan. Con Default Deny, una entrada allow debe cubrir explícitamente las solicitudes deseadas.

ATENCIÓN — Las ACL de esta pantalla no sirven para IPv6
Netgate indica expresamente que las ACL de UPnP IGD & PCP se aplican únicamente a solicitudes de clientes IPv4. No asumir que Default Deny y estas líneas filtran de la misma manera las solicitudes IPv6; emplear reglas firewall específicas y pruebas por familia de direcciones.

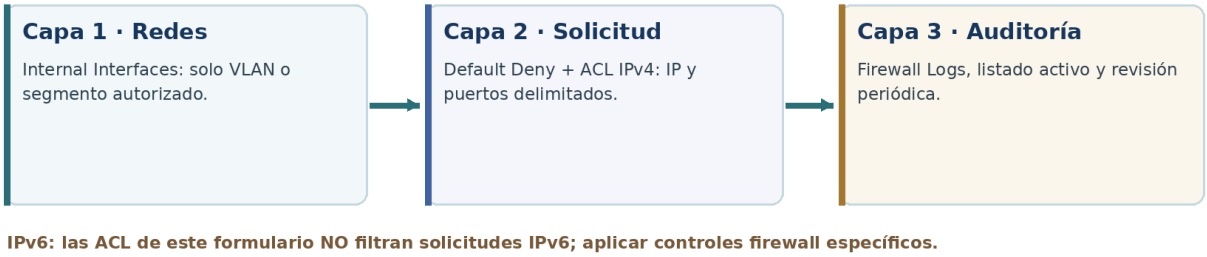


Figura 52.3. Defensa por capas: selección de interfaces, ACL para IPv4, controles del firewall y observabilidad.

52.29. Comportamiento de IPv6 y multicast

Las versiones actuales documentadas por Netgate admiten tráfico UPnP IGD & PCP relacionado con IPv6, pero su implementación por clientes continúa siendo limitada. Los paquetes de control pueden salir desde una dirección link-local hacia un destino multicast, combinación que las reglas normales de una interfaz quizá no permiten. Se requieren reglas explícitas cuando se habilite IPv6. En IPv6 nativo, muchas comunicaciones no requieren NAT; por eso deben estudiarse las reglas de paso, el encaminamiento y el alcance de los permisos sin trasladar automáticamente los supuestos de IPv4.

52.30. Relación con Firewall → Rules y Firewall → NAT

UPnP IGD & PCP no reemplaza el diseño de seguridad del firewall. El daemon gestiona reglas dinámicas; las reglas que gobiernan qué clientes pueden contactar con el propio servicio siguen siendo necesarias. Cuando el requisito es un servidor fijo o una publicación de larga duración, una regla manual de Port Forward con origen restringido suele ofrecer mayor trazabilidad. No esperar que las asignaciones dinámicas aparezcan como entradas editables ordinarias en Firewall → NAT → Port Forward.

52.31. Procedimiento 1: puesta en marcha limitada en un segmento controlado

- Documentar la aplicación cliente, sus puertos, si utiliza UPnP IGD o PCP/NAT-PMP y el responsable de la autorización.
- Comprobar que la WAN elegida dispone de IP pública de entrada, o que la traducción aguas arriba es funcional.
- Ir a Services → UPnP IGD & PCP; marcar Enable y solamente el protocolo requerido.
- Elegir como External Interface la WAN con la puerta de enlace predeterminada.
- Seleccionar únicamente la interfaz o VLAN con los clientes que necesitan el servicio.
- Activar Default Deny y crear con Add entradas allow IPv4 ajustadas al equipo y puertos necesarios.
- Mantener STUN y Override desactivados o vacíos cuando la WAN ya tiene dirección pública reconocible.
- Activar Firewall Logs temporalmente si se necesita evidencia de las pruebas; pulsar Save.
- Revisar Status → Services, Status → UPnP IGD & PCP, registros y pruebas desde un cliente autorizado.
- Intentar una solicitud desde un host sin permiso y documentar que la petición no crea un mapeo.

52.32. Procedimiento 2: política corporativa para pocos dispositivos

Definir una VLAN de equipos autorizados, impedir la comunicación desde segmentos no confiables hacia los puertos de control y configurar ACL individualizadas en lugar de permitir la subred completa. Comprobar que las direcciones de los destinos permanecen estables (por ejemplo, mediante reservas DHCP gestionadas). Establecer un ciclo de revisión de mapeos y avisos al detectar nuevos puertos o destinos no contemplados.

52.33. Procedimiento 3: doble NAT con entrada pública conocida

- Confirmar que existe una IP pública realmente enrutable y que el operador ofrece entrada de conexiones.
- Identificar si el router superior realiza NAT 1:1 o redirección de la entrada hacia la WAN de pfSense.
- Comprobar el reenvío desde un origen remoto, no solo con pruebas internas a la misma red.
- Si la pública es fija, evaluar Override WAN Address con esa IP; si es dinámica y hay NAT compatible, evaluar STUN.
- Configurar STUN Server y su puerto real cuando se active Enable STUN y verificar el resultado en Routing logs.
- Aplicar el resto de controles de seguridad (interfaces, protocolo, ACL IPv4 y reglas firewall).
- Ejecutar una solicitud cliente; verificar mapeo, respuesta y conectividad externa. Si el NAT superior no reenvía, detener el procedimiento y rediseñar la publicación.

52.34. Procedimiento 4: revisión de Multi-WAN y conmutación

Antes de confiar en un mapeo dinámico, identificar qué WAN contiene el gateway predeterminado y si existen gateways por política para los clientes. Probar en condiciones normales y después de un cambio de ruta controlado, sin provocar caídas en producción. Si la IP pública, la salida o la ruta de retorno cambian, las publicaciones previas pueden dejar de ser válidas. Para necesidades multioperador persistentes, considerar un diseño explícito con NAT/Firewall por WAN en lugar de asumir conmutación automática del servicio.

52.35. Escenarios empresariales y decisión de habilitación

Escenario	Valor potencial	Recomendación
Sala de videoconferencia o laboratorio	Asignaciones puntuales y variables.	Habilitar solo en segmento acotado, con permisos y pruebas.
Consolas en área recreativa controlada	Reduce administración de puertos efímeros.	Aislar VLAN, limitar clientes y revisar mappings.
Puesto corporativo con datos sensibles	Comodidad a costa de exposición.	Preferir deshabilitar salvo necesidad aprobada.
Servidor web o aplicación empresarial fija	No depende de negociación dinámica.	Preferir NAT y reglas manuales auditables.
Red invitados/IoT heterogéneo	Gran superficie de solicitudes.	No seleccionar como interfaz interna de forma general.
Conexión detrás de CGNAT	No resuelve ausencia de entrada.	Solicitar alternativa pública, VPN o publicación intermediada.

52.36. Comprobación 1: estado del daemon y asignaciones vivas

Ir a Status → Services y localizar el daemon UPnP IGD & PCP para confirmar si está en ejecución; allí Netgate documenta controles de inicio, parada y reinicio. En Status → UPnP IGD & PCP se muestra la lista de redirecciones activas con clientes y puertos. Una pantalla sin mapeos no prueba por sí sola un error: los clientes deben solicitar activamente una asignación y esta puede tener vida limitada.

52.37. Comprobación 2: extremo remoto y dirección anunciada

Desde un equipo de prueba externo a la organización, verificar que la aplicación está escuchando en el puerto interno, que el servicio anuncia la dirección externa correcta y que la conexión llega al destino. No utilizar exclusivamente pruebas desde la misma LAN: pueden involucrar NAT reflection y dar falsos positivos o falsos negativos. Documentar IP pública de prueba solo en registros internos autorizados, nunca en material formativo distribuido.

52.38. Comprobación 3: logs del firewall y del servicio

Consultar Status → System Logs → Firewall para tráfico registrado o bloqueado, especialmente UDP/1900 y los flujos entrantes mapeados. El registro de miniupnpd se recoge en los logs de Routing (Status → System Logs → System/Routing, conforme a la documentación vigente); examinar mensajes de arranque, pruebas STUN y errores «Failed to add». Usar Diagnostics → Packet Capture sobre la interfaz adecuada cuando sea preciso comprobar llegada real de paquetes.

Síntoma	Evidencia esperada	Dónde comprobar
No aparece el servicio	Daemon detenido o Enable apagado.	Status → Services; configuración.
No se descubre UPnP IGD	SSDP o HTTP/SOAP filtrado.	Firewall logs; captura LAN.
PCP sin respuesta	UDP/5351 bloqueado o protocolo no marcado.	Firewall logs; cliente; configuración.
Failed to add	Dirección no pública o STUN/NAT incompatible, entre otras causas.	Routing logs y topología WAN.
Mapa activo sin entrada real	Aplicación, WAN, ruta o upstream sin entrada.	Prueba remota; capturas; host destino.
Solicitud rechazada	Default Deny/ACL o interfaz no autorizada.	Revisión de ACL y segmento del cliente.

52.39. Diagnóstico: cliente no ve el dispositivo UPnP

Verificar que se seleccionó la interfaz interna correcta, que UPnP IGD está marcado y que el cliente escucha y envía SSDP en su segmento. Inspeccionar UDP/1900 con atención al destino multicast o broadcast real; Netgate advierte que una regla hacia la IP del firewall puede ser insuficiente, por lo que puede requerirse una regla para broadcast o destino any estrictamente limitada al segmento. Comprobar también TCP/2189 y restricciones del host. No abrir los puertos de control en WAN para solucionar un problema de LAN.

52.40. Diagnóstico: hay solicitud pero no se crea el mapeo

Revisar Default Deny y sintaxis ACL, vigencia de rangos y puertos ocupados; confirmar que el cliente pide el puerto previsto y utiliza IPv4 cuando la prueba depende de ACL. A continuación, verificar que External Interface es la WAN correcta y que posee IP pública o direccionamiento externo validado. Si se usa STUN, comprobar DNS, salida UDP, respuesta del servidor y resultado del test de NAT. El texto «Failed to add» puede acompañar imposibilidad de crear la asignación, pero debe interpretarse con el resto del log.

52.41. Diagnóstico: mapeo visible pero conexión entrante fallida

Una asignación visible no demuestra conectividad extremo a extremo. Confirmar servicio escuchando en el cliente, firewall local del sistema operativo, número y transporte del puerto, dirección anunciada, entrada real al router superior, NAT, rutas simétricas y pruebas remotas. En accesos móviles o CGNAT, obtener una IP de salida pública aparente no garantiza que terceros puedan iniciar sesiones entrantes.

52.42. Puertos de origen y NAT saliente: Static Port y alternativas

Algunas aplicaciones, especialmente determinados juegos o protocolos sensibles al puerto de origen, pueden fallar aunque la asignación entrante sea válida. Netgate propone revisar Firewall → NAT → Outbound y utilizar Static Port para un host y tráfico muy concretos cuando sea necesario. En versiones que ofrecen EIM-NAT (Port Restricted Cone NAT), este comportamiento es experimental y NO debe combinarse con Static Port en una misma regla. Evitar modificar todo el NAT saliente para una incidencia individual; una configuración manual global puede afectar a otros equipos.

52.43. Riesgos de seguridad y controles mínimos

Cada cliente autorizado dispone de capacidad para solicitar la publicación temporal de un servicio. El riesgo aumenta si el segmento contiene equipos no administrados, si se permiten todos los puertos o si la organización desconoce qué aplicaciones utilizan esta vía. La temporalidad del mapeo puede reducir aperturas permanentes frente a algunas reglas manuales excesivas, pero no reemplaza la gestión de vulnerabilidades del servicio expuesto ni una revisión periódica.

- Mantener el servicio apagado cuando ningún caso de uso lo justifique.
- Seleccionar interfaces internas mínimas y excluir segmentos de invitados e IoT genérico.
- Activar Default Deny para IPv4 y limitar direcciones y rangos de puertos mediante ACL.
- Definir reglas firewall de control y revisar explícitamente IPv6/link-local/multicast.
- No exponer los puertos de miniupnpd a WAN; proteger también la GUI administrativa.
- Vigilar altas, eliminaciones y cambios de mapeos; registrar la excepción operativa y su responsable.
- Mantener pfSense y aplicaciones cliente actualizados y verificar el cierre real de servicios publicados.

52.44. VPN, VLAN, bridging y alta disponibilidad

La existencia de túneles o VLAN no implica que miniupnpd deba atender solicitudes en esas redes. Evaluar la proximidad de los clientes, rutas, filtrado multicast y política de confianza. En bridging, seleccionar únicamente el bridge con IP. En alta disponibilidad con CARP y sincronización de configuración, no suponer que las asignaciones temporales o las direcciones anunciadas se preservan tras failover: el comportamiento debe probarse para la versión y topología exactas, y las aplicaciones sensibles deben disponer de un método de recuperación.

52.45. Rendimiento, registros y prioridades de tráfico

El coste del servicio suele estar ligado a la frecuencia de peticiones, al número de mapeos y a la generación de logs; no existe en el formulario un límite de sesiones global ni un control de caudal por usuario. Los valores Download/Upload se anuncian, no limitan. Una cola ALTQ afecta a la prioridad del tráfico permitido y requiere dimensionamiento propio. Antes de activar Firewall Logs de forma permanente, medir el volumen de eventos y la capacidad de retención de los logs.

52.46. Cambios, reversión y plan de recuperación

Antes de modificar la configuración, conservar una copia autorizada y anotar clientes y puertos activos. Si aparece un impacto no previsto, desactivar primero el protocolo afectado o el servicio completo desde la GUI, guardar y comprobar que el daemon y las asignaciones quedan en el estado esperado. Revisar luego las reglas NAT, estados y acceso remoto de administración; planificar pruebas de reversión sin desconectar servicios críticos ni presuponer la eliminación instantánea de todas las sesiones ya establecidas.

52.47. Lista de verificación de puesta en producción

Control	Criterio de aceptación	Estado
Necesidad de negocio	Equipo, aplicación y responsable identificados.	Comprobar
WAN pública	Dirección publicada alcanzable; sin CGNAT impeditivo.	Comprobar
Protocolos	Solo UPnP IGD y/o PCP realmente necesario.	Comprobar
Interfaces	Solo segmentos internos autorizados; WAN correcta.	Comprobar
ACL IPv4	Default Deny y allow mínimos probados.	Comprobar
IPv6	Reglas específicas, o servicio restringido según diseño.	Comprobar
Logs y estado	Daemon y mapeos validados; evidencias conservadas.	Comprobar
Prueba externa	Puerto publicado accesible solo como se diseñó.	Comprobar
Reversión	Plan y copia de configuración disponibles.	Comprobar

52.48. Glosario técnico esencial

Término	Definición operativa
UPnP IGD	Mecanismo UPnP de descubrimiento y control de un gateway de Internet.
SSDP	Protocolo de descubrimiento usado por UPnP sobre UDP/1900.
PCP	Protocolo para gestionar mapeos de puertos en dispositivos de red.
NAT-PMP	Protocolo anterior a PCP para solicitar mapeos NAT.
miniupnpd	Servicio que implementa estas funciones en pfSense.
STUN	Método de consulta a un servidor externo para conocer dirección y propiedades NAT.
ACL	Lista de reglas que permiten o deniegan peticiones según parámetros.
ALTQ	Mecanismo de colas de conformación/priorización de tráfico.
CGNAT	Traducción de direcciones realizada por el operador que puede impedir entrada directa.
Static Port	Modo de NAT saliente que conserva el puerto de origen del cliente.

52.49. Referencias técnicas y normativas de Netgate

Fuentes oficiales consultadas para la redacción. Las opciones corresponden a la interfaz descrita y a la documentación vigente consultada en noviembre de 2026; algunas etiquetas y comportamientos de validación dependen de la versión exacta de pfSense Plus, que debe comprobarse en el equipo antes de actuar.

- UPnP IGD & PCP — descripción, campos, puertos, configuración y diagnóstico
- Services — guía de navegación
- UPnP IGD & PCP Traffic Shaping
- Outbound NAT — modos, Static Port y EIM-NAT
- NAT — conceptos de NAT entrante y saliente
- Configuring pfSense Software for Online Gaming
- Routing Logs — mensajes de miniupnpd
- Status — vista de servicios y mapeos
- Notas de versión pfSense Plus 25.07 — revisión GUI y puerto STUN opcional

53 Services → Wake-on-LAN

Magic Packets · interfaces · inventario de dispositivos · arranque remoto · diagnóstico

Wake-on-LAN (WOL) permite solicitar el encendido o la reactivación de equipos compatibles desde pfSense Plus. Su utilidad depende de la alimentación de la interfaz de red, de los estados de energía admitidos y de la configuración del hardware, el firmware y el sistema operativo. La acción envía una señal de red: no establece por sí sola que el equipo haya arrancado ni que sus aplicaciones estén disponibles.



Figura 53.1. Recorrido conceptual de una orden WOL dentro del segmento de red seleccionado.

53.1. Objetivos y alcance administrativo

Este capítulo desarrolla la página Services → Wake-on-LAN, el envío individual inmediato, el inventario reutilizable de direcciones MAC, las acciones por fila y el envío masivo. También explica el formulario de alta/edición documentado oficialmente y las integraciones con Dashboard y DHCP Leases. Se distinguen las opciones de la pantalla principal de las funcionalidades que se abren al acceder a otras páginas.

53.2. Qué es Wake-on-LAN y para qué sirve

WOL es un mecanismo de activación remota de interfaces de red que permanecen preparadas para reconocer una secuencia específica aun cuando el ordenador está suspendido o apagado en un estado que admite reactivación. Puede reducir el tiempo que estaciones y equipos auxiliares permanecen en funcionamiento, facilitar tareas de mantenimiento y recuperar temporalmente un puesto de trabajo para soporte remoto. No sustituye a un sistema de administración de energía, de inventario o de disponibilidad de servicios.

Situación	Utilidad	Condición necesaria
Puesto de usuario suspendido	Activar para asistencia a demanda	NIC y sistema autorizan reactivación
Equipo de administración	Encender antes de mantenimiento	Permitir el estado de energía requerido
Laboratorio o aula	Activación coordinada de equipos	Inventario MAC correcto y red alcanzable
Servidor auxiliar	Arranque manual de contingencia	Arranque seguro y dependencias verificadas

53.3. Funcionamiento técnico: Magic Packet

El Magic Packet clásico contiene seis octetos 0xFF consecutivos seguidos por 16 repeticiones de los seis octetos de la dirección MAC de destino: 6 + (16 × 6) = 102 bytes de patrón. Suele transportarse en un datagrama UDP de difusión, aunque el mecanismo depende principalmente de la detección del patrón por la NIC y no de una sesión de aplicación. Los puertos UDP 7 y 9 son convenciones utilizadas por herramientas WOL, no requisitos universales del protocolo ni campos configurables en esta pantalla.



Figura 53.2. Estructura del patrón clásico de 102 bytes. Ejemplo MAC enteramente ficticio.

53.4. Condiciones previas: NIC, firmware, sistema y alimentación

Antes de configurar pfSense, comprobar que el equipo objetivo admite WOL en la NIC y que existe alimentación de espera para mantener su circuito de escucha. En BIOS/UEFI buscar la opción equivalente a Wake on LAN, Power on by PCI-E/PCI o similar. En tarjetas de expansión antiguas puede existir un cable WOL físico; no es un requisito general de equipos modernos.

- Conexión: preferentemente Ethernet cableado; WOL por Wi-Fi (WoWLAN) es distinto y depende del dispositivo y del fabricante.
- Energía: las opciones ErP/EuP, modo de bajo consumo y un corte total de alimentación pueden deshabilitar la escucha.
- Sistema operativo: habilitar el despertar por paquete mágico en el controlador cuando exista esa posibilidad.
- Estados S3/S4/S5: la compatibilidad no debe suponerse igual para todos los equipos y tipos de apagado.
- En máquinas virtuales, el arranque lo gestiona normalmente el hipervisor; una MAC virtual no garantiza WOL físico.

PRECAUCIÓN Un mensaje de pfSense que indique envío correcto no constituye confirmación de que el destino se haya encendido. El arranque, la red y el servicio de acceso remoto deben verificarse por separado.

53.5. Ruta exacta y elementos visibles de la página

Ruta de administración: Services → Wake-on-LAN. La pantalla principal contiene un aviso informativo superior, el bloque «Wake-on-LAN» para enviar una orden directa y la sección «Wake-on-LAN Devices» para gestionar destinos guardados. El signo de ayuda (?) de la parte superior remite a la documentación contextual cuando está disponible.

Sección / control	Función precisa	Ámbito de comprobación
Aviso azul informativo	Indica que se envían Magic Packets y que la NIC necesita WOL.	Disponible en el formulario
Interface	Interfaz del cortafuegos hacia el equipo de destino.	Visible en formulario principal
MAC address	MAC del equipo, formato xx:xx:xx:xx:xx:xx.	Visible en formulario principal
Send	Ordena el envío inmediato.	Visible en formulario principal
Wake-on-LAN Devices	Lista de entradas persistentes.	Visible, inicialmente vacía
Add	Abre el alta de un dispositivo guardado.	Visible y verificado en Netgate
Wake All Devices	Envía un paquete por cada dispositivo guardado.	Visible y verificado en Netgate
Acciones por fila	Editar, eliminar y despertar una entrada.	Verificado en documentación oficial

53.6. Campo «Interface»: función, alcance y selección

El desplegable selecciona la interfaz de pfSense desde la que puede alcanzarse el segmento en que reside el equipo. En la captura aparece «LAN» como valor seleccionado; los valores ofrecidos dependen de las interfaces configuradas en cada firewall y no existe una lista universal fija. Conviene elegir la interfaz cuya red de capa 2 contiene la NIC destino. Las VLAN asignadas pueden aparecer como interfaces lógicas independientes y requieren seleccionar el segmento adecuado.

En implementaciones donde el tráfico WOL se emite a la dirección de difusión de la subred de la interfaz, seleccionar una WAN externa, una interfaz errónea o una VLAN distinta puede impedir que la trama llegue al equipo. No se deben abrir puertos entrantes de Internet ni crear NAT hacia una dirección de difusión como solución habitual: el envío local desde el cortafuegos es la vía más controlada.

53.7. Campo «MAC address»: formato, obtención y validación

El campo solicita una dirección física de seis octetos, representados por pares hexadecimales y separados por dos puntos, por ejemplo «02:11:22:33:44:55» (ficticia). No se introduce una dirección IP, un nombre DNS ni la MAC del gateway. Debe corresponder a la interfaz que realmente recibe el patrón WOL, normalmente la tarjeta Ethernet del equipo objetivo.

Puede obtenerse del inventario del fabricante, de la configuración del sistema, del estado de la NIC o de registros DHCP/ARP, con las precauciones habituales: una MAC observada por pfSense puede ser la de otra interfaz, un adaptador virtual o una dirección aleatoria. El código de la interfaz web de pfSense normaliza las MAC escritas con guiones a la notación con dos puntos y las convierte a minúsculas, pero es mejor introducirlas ya en el formato de la ayuda.

53.8. Botón «Send»: resultado y límites de la confirmación

«Send» ejecuta el intento de envío de un Magic Packet por la interfaz seleccionada. Si los datos son válidos y la herramienta de envío termina correctamente, pfSense muestra un aviso de éxito. No hay un mecanismo de respuesta de la NIC que certifique que arrancó: para validar el resultado es necesario comprobar presencia de enlace, DHCP/ARP, respuesta de red y finalmente el servicio esperado.

Al activar Send no se incorpora automáticamente el equipo a «Wake-on-LAN Devices»; el envío inmediato y el registro persistente son acciones distintas.

53.9. Bloque «Wake-on-LAN Devices»: columnas e inventario

El listado presenta las columnas «Interface», «MAC address», «Description» y «Actions». Cuando está vacío solo se muestran los títulos y los controles inferiores; esto no significa que el cortafuegos esté incapacitado para enviar Magic Packets. Las entradas registradas sirven como agenda operativa sin necesidad de volver a escribir la dirección física.

Columna	Qué muestra	Uso administrativo
Interface	Segmento elegido para enviar WOL	Comprobar que no cambió la asignación de VLAN.
MAC address	Destino en notación hexadecimal	El enlace de la MAC despierta ese equipo.
Description	Etiqueta descriptiva de la entrada	Usar nombre genérico y rol funcional, no secretos.
Actions	Iconos por entrada guardada	Editar, eliminar y enviar WOL.

53.10. Formulario «Add» / «Edit WOL Entry»

Al pulsar «Add» se abre el formulario «Edit WOL Entry», documentado por Netgate y confirmado por el código del módulo. Contiene «Interface» (obligatorio), «MAC address» (obligatorio) y «Description» (opcional), seguido del control de guardado. No debe confundirse con el formulario superior de envío inmediato: aquí se crea o modifica una entrada persistente.

Campo del alta / edición	Requisito	Comportamiento
Interface	Obligatorio	Segmento del equipo; ofrece interfaces configuradas.
MAC address	Obligatorio	Dirección de seis octetos; valida formato.
Description	Opcional	Texto administrativo; no se procesa para el envío.
Save	Acción	Valida, guarda y vuelve al listado.

El software evita duplicados de la pareja «Interface + MAC address» al guardar y ordena el inventario por la descripción en el código consultado. Estas son observaciones de implementación que pueden cambiar entre versiones; deben confirmarse tras una actualización importante.

53.11. Iconos y acciones de una entrada ya almacenada

Con dispositivos guardados se muestran controles por fila: el icono de lápiz permite editar, la papelera elimina la entrada del inventario y el icono de encendido emite un Magic Packet. El valor enlazado de la columna MAC tiene el mismo propósito de despertar ese equipo. Borrar una entrada no desactiva WOL en su BIOS ni apaga físicamente el dispositivo; solo elimina el acceso directo configurado en pfSense.

53.12. Botón «Wake All Devices»: alcance real y riesgos

«Wake All Devices» recorre todas las entradas guardadas y envía solicitudes de despertar para cada una de ellas. No significa encender todos los hosts de una subred ni descubrirlos automáticamente: solo actúa sobre lo que figura en el inventario. Puede activar puestos fuera de horario, provocar picos de consumo y poner en marcha equipos que comparten infraestructura eléctrica o dependencias.

En la implementación examinada se muestra una confirmación antes de enviar el conjunto de órdenes. Para entornos sensibles conviene usar entradas individuales o segmentar previamente el inventario mediante procedimientos operativos y autorizaciones de acceso.

RIESGO OPERATIVO No utilizar Wake All Devices como prueba rutinaria cuando el inventario incluya puestos, sistemas de control, laboratorios o servidores cuya activación simultánea pueda tener impacto.

53.13. Matriz: acción, persistencia y efecto

Acción	¿Guarda configuración?	¿Emite Magic Packet?	¿Asegura el arranque?
Send	No	Sí, intento inmediato	No
Add + Save	Sí	No	No
Editar + Save	Sí	No	No
Clic en MAC guardada	No	Sí	No
Icono encendido	No	Sí	No
Wake All Devices	No	Sí, a todas las entradas	No
Eliminar entrada	Sí, elimina registro	No	No

53.14. Procedimiento 1: enviar una orden puntual

01 Confirmar con el propietario del equipo que existe autorización para activarlo y que no hay trabajos de mantenimiento eléctrico en curso.

02 Comprobar que la tarjeta Ethernet soporta WOL y que BIOS/UEFI y controlador están preparados.

03 Abrir Services → Wake-on-LAN y escoger «Interface» del segmento correcto.

04 Introducir en «MAC address» la MAC de la NIC física en formato xx:xx:xx:xx:xx:xx.

05 Pulsar «Send» y leer el mensaje de la interfaz.

06 Esperar el tiempo de arranque, verificar conectividad y comprobar la disponibilidad del servicio que motivó el encendido.

53.15. Procedimiento 2: crear y mantener el inventario

01 Abrir Services → Wake-on-LAN y pulsar «Add» en la sección de dispositivos.

02 Seleccionar «Interface» del equipo. Evitar asociar por comodidad todos los registros a LAN si existen VLAN distintas.

03 Introducir la «MAC address» correcta y usar «Description» para distinguir su función, por ejemplo «Puesto de laboratorio 01».

04 Pulsar «Save»; comprobar que aparece la fila correspondiente en la lista.

05 Probar una sola entrada mediante el enlace de MAC o el icono de encendido y verificar el arranque.

06 Actualizar o eliminar las entradas obsoletas cuando se sustituya una NIC, un equipo o una VLAN.

53.16. Procedimiento 3: activar dispositivos almacenados

01 Revisar el listado y comprobar que la interfaz y la MAC corresponden al destino previsto.

02 Para un único equipo, pulsar su dirección MAC o el icono de encendido de la fila.

03 Para el conjunto, revisar expresamente el alcance y utilizar «Wake All Devices» únicamente si está autorizado.

04 Interpretar el aviso de transmisión como resultado del envío, no como un control de presencia.

05 Validar en el sistema de monitorización qué equipos arrancaron y documentar los que requieran intervención.

53.17. Integración con «Status → DHCP Leases»

La documentación oficial describe accesos directos WOL en la vista de concesiones DHCPv4. El icono de encendido permite intentar despertar un host marcado como desconectado; el icono de añadir permite copiar los datos de una concesión a un nuevo registro WOL, completando la información pendiente antes de guardar.

La marca de equipo desconectado se relaciona con su ausencia en la tabla ARP del cortafuegos, lo que no equivale siempre a un apagado real. Puede ser necesario esperar a que caduque la entrada ARP tras apagarlo o visualizar todas las concesiones configuradas para encontrar un destino antiguo. Estas acciones no sustituyen la verificación de su NIC de destino.

53.18. Integración con el widget «Wake On LAN» del Dashboard

El Dashboard ofrece un widget opcional «Wake On LAN» que muestra los dispositivos registrados y un acceso directo para emitir el Magic Packet. Puede mostrar el estado del equipo cuando la información de red lo permite. El widget reutiliza el inventario de Services → Wake-on-LAN; no crea por sí mismo un servicio de encendido adicional.

53.19. WOL y segmentos VLAN: tráfico de difusión

WOL clásico funciona de forma natural dentro de un dominio de difusión de capa 2. Cuando pfSense tiene una interfaz asignada en cada VLAN, el administrador selecciona la del destino para que el paquete salga por ese segmento. La configuración que funciona para LAN no tiene por qué funcionar en otra VLAN, en una red enlazada por túnel o en un segmento tras un router adicional.

Para redes remotas sin interfaz local en el mismo dominio de difusión, una alternativa de diseño es un agente WOL situado en el segmento remoto, accesible mediante administración segura. Evitar habilitar indiscriminadamente la retransmisión de difusión dirigida entre redes.

53.20. WOL desde una conexión VPN: modelo de acceso seguro

La VPN sirve para que el administrador alcance la interfaz web de pfSense de manera protegida. Una vez autenticado, es el propio cortafuegos quien origina el envío por su interfaz local seleccionada. No es necesario encaminar la trama de difusión a través del túnel del administrador ni publicar un receptor WOL en Internet.

SEGURIDAD Restringir las páginas de WOL a los operadores autorizados mediante los permisos de usuario de pfSense. No exponer la interfaz web de administración en WAN solo para disponer de encendido remoto; utilizar VPN y autenticación fuerte.

53.21. Ciclo de energía: suspensión, hibernación y apagado

Estado	Interpretación habitual	Expectativa sobre WOL
S0	Equipo funcionando	No hay nada que despertar; evaluar conectividad.
S3	Suspensión tradicional	Suele ser el escenario más predecible con soporte de NIC.
S4	Hibernación	Depende de controlador/firmware y transición efectuada.
S5	Apagado lógico (soft off)	No asumir soporte; algunas placas lo implementan vía firmware.

Estado	Interpretación habitual	Expectativa sobre WOL
G3	Sin alimentación física	No funciona; requiere energía de espera.

Microsoft documenta que el WOL desde suspensión S3 y desde hibernación S4 explícita puede estar admitido, mientras que el apagado híbrido (Inicio rápido) y S5 no se consideran rutas oficialmente compatibles en Windows en los supuestos descritos. Algunas placas base pueden manejar el encendido desde S5 por su firmware. Debe distinguirse compatibilidad del sistema operativo de capacidad eléctrica del hardware.

53.22. Windows: controlador, Inicio rápido y comprobación local

En Windows, revisar el Administrador de dispositivos → adaptador Ethernet → Propiedades → Administración de energía / Opciones avanzadas, si la NIC presenta esas pestañas, para buscar opciones equivalentes a «Wake on Magic Packet» y permitir la reactivación. Los nombres varían entre fabricantes y versiones de controlador. Comprobar el resultado con suspensión real antes de probar hibernación y apagado.

Una orden de apagado que utilice Inicio rápido puede desarmar la NIC aunque la suspensión funcione correctamente. No deshabilitar Inicio rápido en todos los equipos como recomendación general; realizar una prueba controlada y evaluar el efecto sobre tiempos de arranque, políticas de energía y soporte del fabricante.

53.23. Linux y otros equipos: driver, WoL y validación

En Linux, herramientas como ethtool pueden mostrar las capacidades WOL de interfaces Ethernet y su estado efectivo, por ejemplo «Supports Wake-on» y «Wake-on: g» en controladores compatibles. La sintaxis y la persistencia de los ajustes dependen del sistema y del gestor de red; no se asume que estos valores se mantengan tras cada reinicio. En NAS, estaciones y dispositivos embebidos se debe utilizar la documentación del fabricante y su perfil de administración de energía.

53.24. Virtualización, hipervisores y conmutadores

En entornos virtualizados puede ser el hipervisor quien decide iniciar una VM apagada. El envío a la MAC virtual solo es eficaz si existe un mecanismo explícito que intercepte o utilice el evento; no equivale a encender una máquina física. En equipos físicos, observar el enlace del switch durante suspensión o apagado puede ayudar a diagnosticar si la NIC sigue alimentada, pero el LED no constituye una prueba universal de soporte WOL.

53.25. Ejemplo empresarial A: puesto de soporte remoto

Un puesto ficticio «Puesto de laboratorio 01» conectado a la red de documentación 192.0.2.0/24 puede registrar la MAC ficticia «02:11:22:33:44:55» en la interfaz LAN correspondiente. El técnico, conectado mediante VPN a la administración de pfSense, lo activa antes de su sesión de soporte y verifica posteriormente que el sistema inicia, obtiene red y acepta el servicio de asistencia autorizado.

El direccionamiento y la MAC del ejemplo son de carácter exclusivamente ilustrativo: la conectividad real depende de los valores propios de cada despliegue.

53.26. Ejemplo empresarial B: aula con encendido controlado

Registrar varios puestos del aula en la misma interfaz de la VLAN apropiada, con etiquetas funcionales. Probar WOL individual antes de plantear una activación masiva. En un inicio coordinado, considerar consumo eléctrico, arranque simultáneo, capacidad DHCP y disponibilidad de almacenamiento o servicios de dominio. Una operación ordenada puede requerir limitar manualmente los grupos de equipos, porque el control «Wake All Devices» no presenta una cola avanzada de orquestación.

53.27. Ejemplo empresarial C: sede aislada y administración central

Para una sede que se conecta a la central por túnel, no se debe suponer que la difusión enviada en una LAN central recorrerá la VPN hacia otra LAN. Una solución verificable es usar el pfSense de la sede destino (si existe y administra su segmento local) o un agente WOL local, accesible solo a técnicos autorizados. Separar la seguridad de acceso a la administración de la entrega local del Magic Packet.

53.28. Comprobación por capas: señal enviada, arranque y servicio



Figura 53.3. Secuencia de diagnóstico: envío, alcance local, respuesta del equipo y servicio final.

01 Revisar el mensaje devuelto por «Send» o por el icono del dispositivo.

02 En Diagnostics → Packet Capture, seleccionar la interfaz de salida y capturar tráfico próximo al momento del envío. No fijar un puerto UDP sin conocer la implementación concreta.

03 Comprobar alimentación residual, compatibilidad del estado de energía y configuración de NIC/firmware.

04 Verificar si aparece actividad de DHCP/ARP o el host responde a pruebas apropiadas tras el arranque.

05 Comprobar finalmente la aplicación de destino (RDP, SSH, servicio interno, monitorización), evitando confundir que no responda ICMP con que el sistema siga apagado.

53.29. Diagnóstico de incidentes: matriz de causa y verificación

Síntoma	Posibles causas	Comprobación / corrección
pfSense rechaza el envío	MAC mal formada o interfaz no válida.	Revisar sintaxis e interfaz asignada.
Mensaje enviado, sin reacción	NIC sin energía, WOL desactivado o estado no admitido.	Probar S3, revisar UEFI/driver/ErP.
Funciona en LAN, falla en otra VLAN	Interfaz de salida incorrecta o ausencia de difusión local.	Seleccionar interfaz de VLAN destino.
Funciona al suspender pero no al apagar	Inicio rápido, S5 o firmware no compatibles.	Comparar transiciones energéticas.
Equipo arranca, no responde al soporte	SO aún inicializando, firewall local, servicio detenido.	Verificar DHCP, servicios y credenciales.
DHCP Leases no muestra WOL	Host aún en ARP o concesión antigua oculta.	Esperar envejecimiento ARP; mostrar concesiones.
La lista presenta MAC obsoleta	Cambio de adaptador, docking o equipo.	Actualizar el inventario y repetir prueba.
Wake All solo activa una parte	Diferencias de hardware, cableado y estados de energía.	Diagnosticar individualmente cada registro.

53.30. Diagnóstico avanzado: captura del paquete y criterios

Una captura iniciada en Diagnostics → Packet Capture antes de pulsar «Send» ayuda a determinar si pfSense emitió tráfico por la interfaz correcta. En el código público consultado, el envío calcula el broadcast de la subred seleccionada y ejecuta una utilidad WOL; el destino concreto del datagrama depende de la implementación vigente. Capturar por protocolo y momento de emisión, o visualizar el contenido de la trama en Wireshark, permite reconocer la secuencia FF × 6 + MAC × 16.

Si el paquete sale de pfSense y llega al segmento pero el equipo no reacciona, la investigación debe centrarse en alimentación, firmware, NIC, puente/VLAN y estados de energía. Si el paquete no se observa,

primero revisar selección de interfaz, dirección MAC y el resultado de ejecución local. El código de una versión concreta nunca sustituye la comprobación en la versión realmente instalada.

53.31. Control de acceso y amenazas

El paquete WOL clásico no autentica al emisor. Cualquier equipo que pueda enviar el patrón correcto por el mismo segmento de capa 2 podría activar una NIC preparada. El acceso a Services → Wake-on-LAN sí debe protegerse mediante usuarios y permisos administrativos de pfSense, pero esa medida no convierte el protocolo de red en criptográficamente seguro.

- Conceder privilegios de visualización/edición WOL únicamente a los perfiles que deban operar el encendido.
- Limitar la administración web a redes de gestión protegidas, preferiblemente accesibles por VPN.
- Habilitar WOL únicamente en equipos que lo necesiten; mantenerlo desactivado en el resto.
- Revisar la vigencia del inventario y las acciones masivas antes de mantenimiento o fuera de horario.
- Evitar receptores WOL expuestos a Internet y reglas de difusión dirigida sin diseño específico.
- Documentar prueba de encendido, ventana autorizada y mecanismo de apagado posterior.

53.32. Rendimiento, fiabilidad y continuidad del servicio

WOL no exige mantener un daemon de escucha WOL en pfSense para cada destino: la página web genera una orden cuando un administrador la solicita. La latencia percibida suele estar dominada por el tiempo de energización, POST, carga del sistema operativo y disponibilidad de servicios, no por la transmisión del Magic Packet. Para un uso operativo fiable se deben considerar inventario actualizado, capacidad del circuito eléctrico y verificación por monitorización.

Algunos equipos requieren arranque secuencial para evitar una demanda eléctrica simultánea; pfSense no proporciona aquí un programador de secuencias de encendido ni un indicador fehaciente del estado físico. El apagado ordenado debe hacerse por los mecanismos de administración del equipo, no mediante esta página.

53.33. Compatibilidad y diferencias entre versiones de pfSense

El menú y las funciones descritas forman parte de la documentación general de pfSense y aparecen en la interfaz indicada de pfSense Plus. Al no disponer de un número de versión confirmado, se mantienen los controles efectivamente visibles y los campos de edición verificados oficialmente sin atribuir comportamientos especiales de una versión concreta. Netgate documenta cambios de implementación en determinadas versiones, por lo que los iconos o mecanismos de envío pueden variar tras una actualización.

Como referencia de mantenimiento, las notas de versión de pfSense CE 2.9.0 mencionan correcciones de enlaces de envío WOL y el uso de POST en la acción «Wake All»; la aplicabilidad a una compilación concreta de pfSense Plus requiere comprobar sus propias notas de versión.

53.34. Lista de comprobación para puesta en producción

Control	Criterio de aceptación
Necesidad y autorización	Existe caso de uso documentado y operador responsable.
Destino correcto	MAC física e interfaz asignada revisadas.
Firmware/NIC	WOL soportado y preparado en el estado de energía esperado.
Prueba individual	Paquete enviado y arranque observado con verificación posterior.
Seguridad	Acceso a la GUI limitado; sin exposición WOL indiscriminada.
Inventario	Etiquetas claras, duplicados controlados y baja de obsoletos.
Recuperación	Se dispone de gestión alternativa si el equipo no arranca.

53.35. Glosario técnico

Término	Definición operativa
WOL	Wake-on-LAN; activación de un equipo mediante un patrón de red.
Magic Packet	Secuencia 0xFF × 6 seguida por MAC × 16.
MAC	Identificador de la interfaz de enlace; no dirección IP.
NIC	Network Interface Card; adaptador de red del equipo.
Broadcast	Tráfico dirigido al dominio de difusión del segmento.
UEFI/BIOS	Firmware que puede preparar el hardware para eventos de despertar.
S3 / S4 / S5	Estados de suspensión, hibernación y apagado lógico.
ErP/EuP	Opciones de ahorro eléctrico que pueden afectar energía de espera.
ARP	Resolución IPv4 a MAC; su ausencia no prueba apagado físico.
VLAN	Segmentación lógica de dominios de capa 2.

53.36. Referencias documentales verificables

Fuentes primarias para las opciones de configuración, el comportamiento de los controles y la comprobación de incidencias:

- **Netgate · Wake on LAN (guía principal) —** https://docs.netgate.com/pfsense/en/latest/services/wake-on-lan.html
- **Netgate · Menú Services —** https://docs.netgate.com/pfsense/en/latest/menuguide/services.html
- **Netgate · Status / DHCPv4 Leases —** https://docs.netgate.com/pfsense/en/latest/monitoring/status/dhcp-ipv4.html
- **Netgate · Available Widgets (Wake On LAN) —** https://docs.netgate.com/pfsense/en/latest/monitoring/dashboard-widgets.html
- **Netgate · Packet Capture GUI —** https://docs.netgate.com/pfsense/en/latest/diagnostics/packetcapture/webgui.html
- **Netgate · Acceso remoto a la GUI —** https://docs.netgate.com/pfsense/en/latest/recipes/remote-firewall-administration.html
- **Netgate · Código público: services_wol.php —** https://github.com/pfsense/pfsense/blob/master/src/usr/local/www/services_wol.php
- **Netgate · Código público: services_wol_edit.php —** https://github.com/pfsense/pfsense/blob/master/src/usr/local/www/services_wol_edit.php
- **Microsoft · Estados de energía y compatibilidad WOL —** https://learn.microsoft.com/en-us/windows/win32/power/system-power-states
- **Microsoft · Wake on LAN behavior —** https://learn.microsoft.com/en-us/troubleshoot/windows-client/deployment/wake-on-lan-feature
- **Netgate · Notas 2.9.0 (referencia de cambios) —** https://docs.netgate.com/pfsense/en/latest/releases/2-9-0.html

Parte V VPN

54 VPN → Introducción general

IPsec · OpenVPN · WireGuard · L2TP · AWS VPC · movilidad · seguridad y diagnóstico

La sección VPN de pfSense Plus reúne varias tecnologías para establecer comunicaciones privadas sobre redes no confiables. Su administración exige considerar conjuntamente el cifrado, la identidad del extremo, el direccionamiento, las rutas, las reglas de firewall, la disponibilidad y el ciclo de vida de las credenciales. Este capítulo ofrece el marco técnico para elegir y operar cada solución con criterio.

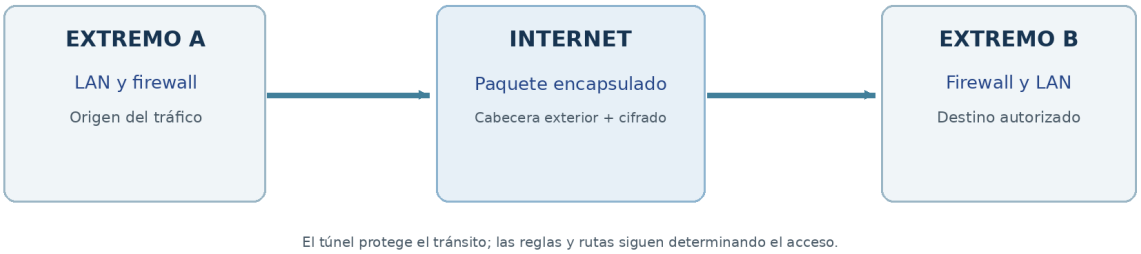


Figura 54.1. Estructura funcional de una VPN entre dos extremos a través de una red no confiable.

54.1. Objetivo, alcance y punto de acceso

Ruta exacta: VPN, en la barra superior de pfSense Plus. Al desplegar el menú aparecen AWS VPC VPN Wizard, IPsec, IPsec Export: Apple Profile, IPsec Export: Windows, L2TP, OpenVPN y WireGuard. El desplegable permite seleccionar una funcionalidad; no constituye por sí mismo una pantalla de configuración ni contiene controles de activación de túneles.

El capítulo presenta el propósito y los riesgos de los siete accesos, sus relaciones con otras áreas de pfSense y un método de planificación, implantación y auditoría. Los formularios específicos de cada opción se analizan en sus capítulos propios. Las disponibilidades pueden variar con la versión, los paquetes instalados y las funciones Plus/CE.

54.2. Qué es realmente una VPN

Una VPN (Virtual Private Network) crea un canal lógico para transportar tráfico entre extremos a través de un medio compartido, habitualmente Internet. En IPsec, OpenVPN y WireGuard, las funciones criptográficas adecuadamente configuradas aportan confidencialidad, integridad y autenticación de los extremos o de las entidades admitidas por el protocolo. Esto no equivale a proteger automáticamente todos los equipos internos ni a conceder seguridad a aplicaciones vulnerables.

Concepto	Significado práctico	Error habitual
Túnel	Encapsulación para comunicar redes o clientes por una ruta lógica.	Confundir túnel establecido con aplicación accesible.
Cifrado	Oculta la carga útil de las comunicaciones frente a terceros en tránsito.	Suponer que no existe exposición de metadatos.
Autenticación	Comprueba quién o qué extremo participa, según el protocolo.	Usar una clave compartida como autorización universal.
Autorización	Restringe orígenes, destinos y servicios mediante políticas.	Permitir todo el tráfico VPN hacia todas las VLAN.
Encaminamiento	Determina por dónde deben circular solicitudes y respuestas.	Olvidar rutas de retorno y redes solapadas.

54.3. Cómo funciona: plano de control y plano de datos

La negociación inicial puede autenticar pares, acordar claves y parámetros criptográficos, o distribuir rutas y parámetros de cliente. El plano de datos transporta después paquetes cifrados. La separación ayuda a

diagnosticar fallos: una conexión puede autenticarse correctamente y, sin embargo, no transportar tráfico por reglas, rutas, selectores, NAT, DNS o MTU.

- Plano de control: establecimiento, autenticación, rekey, detección de pares y parámetros de la VPN, según la tecnología.
- Plano de datos: encapsulación/cifrado, envío, descifrado y procesamiento de tráfico interno.
- Plano de gestión: copias de seguridad, certificados, revocación, usuarios, registros, alertas y cambios autorizados.

54.4. Topologías y necesidades empresariales

Modelo	Función	Diseño recomendable
Site-to-site	Comunica dos sedes y sus subredes.	Prefijos no solapados y rutas de ida/vuelta documentadas.
Acceso remoto	Usuarios y dispositivos se conectan a recursos internos.	Identidad individual, MFA cuando sea viable y mínimos privilegios.
Hub-and-spoke	Varias delegaciones usan un concentrador.	Control de tránsito intersede y dependencia del centro.
Malla / multisitio	Extremos establecen conexiones directas entre sí.	Automatización y gestión estricta de rutas y claves.
Híbrida / nube	Comunica instalaciones con una VPC o entorno cloud.	Coordinar túneles, rutas y filtros también en la nube.
Salida segura	El cliente dirige Internet por la sede o concentrador.	Capacidad de salida, DNS, IPv6 y política de navegación.

Una topología hub-and-spoke simplifica la gestión de sedes pequeñas, pero concentra riesgo de disponibilidad y capacidad. Una malla aporta caminos directos, a cambio de más sesiones, rutas y administración. La decisión ha de considerar la latencia, dependencias de servicios, experiencia de usuario, mantenimiento y recuperación.

54.5. Mapa del menú VPN: siete accesos, distintas naturalezas



Figura 54.2. Mapa conceptual de las siete entradas visibles y su función operativa.

Entrada del menú	Tipo	Qué permite administrar
AWS VPC VPN Wizard	Asistente Plus / paquete	Crear y coordinar una conexión VPN con una VPC de AWS.
IPsec	Funcionalidad VPN	Túneles entre sedes, acceso móvil, IKE, parámetros y asociaciones.
IPsec Export: Apple Profile	Utilidad Plus / paquete	Generar perfiles compatibles para clientes Apple.
IPsec Export: Windows	Utilidad Plus / paquete	Generar scripts/configuración para clientes Windows.
L2TP	Servicio de tunelización	Servidor y usuarios L2TP; cifrado no integrado en L2TP.

Entrada del menú	Tipo	Qué permite administrar
OpenVPN	Funcionalidad VPN	Servidores, clientes y opciones específicas de túneles TLS.
WireGuard	Paquete VPN	Túneles, peers, claves, redes permitidas y encaminamiento.

CRITERIO DE LECTURA Los nombres del menú se conservan tal y como aparecen en pfSense Plus. El significado técnico de cada entrada se contrasta con documentación de Netgate; la presencia de una entrada no prueba que un túnel esté configurado o activo.

54.6. AWS VPC VPN Wizard: vínculo con una nube pública

Este asistente, documentado por Netgate para pfSense Plus, facilita una VPN hacia una Virtual Private Cloud (VPC) de AWS y puede efectuar cambios tanto en pfSense como en recursos de AWS, de acuerdo con sus permisos. No es un protocolo independiente: automatiza una solución basada en servicios de VPN y encaminamiento. Requiere credenciales de API autorizadas y revisión de los recursos que crea o modifica.

- Aplicación: conexión híbrida entre infraestructura empresarial y redes privadas alojadas en AWS.
- Dependencias: permisos IAM adecuados, regiones y VPC correctas, prefijos compatibles, rutas, grupos de seguridad y disponibilidad de gateways.
- Riesgos: ampliación involuntaria del alcance de red, costes y cambios en recursos cloud, credenciales de API expuestas o rutas asimétricas.

PRECAUCIÓN Antes de ejecutar el asistente en producción, revisar la región, la cuenta, los permisos y los recursos AWS existentes. Una automatización que crea rutas o cambia grupos de seguridad puede alterar la accesibilidad de sistemas críticos.

54.7. IPsec: estándar, interoperabilidad y modalidades

IPsec es un conjunto de mecanismos ampliamente soportados para VPN site-to-site y acceso móvil. pfSense permite IKEv1/IKEv2, negociación de asociaciones de seguridad y diseños basados en políticas o interfaces virtuales. En implementaciones nuevas suele favorecerse IKEv2 cuando todos los extremos lo soportan; la compatibilidad y el perfil criptográfico concreto deben comprobarse con cada fabricante.

- IPsec basado en políticas: los selectores de tráfico de fase 2 determinan qué combinaciones de redes se capturan para el túnel; no se resuelve mediante una ruta estática ordinaria.
- IPsec VTI basado en rutas: utiliza interfaces virtuales y la tabla de rutas para decidir el tráfico, permitiendo rutas estáticas o protocolos dinámicos cuando se configuran correctamente.
- IPsec móvil: conecta clientes remotos y admite diferentes métodos de autenticación según la modalidad.
- NAT-T: facilita la operación tras NAT al encapsular IPsec mediante UDP/4500 cuando procede.

RIESGO DE ENCAMINAMIENTO En VTI, asignar una interfaz y dejar las puertas de enlace por defecto en modo automático puede ocasionar que una interfaz VPN sea elegida erróneamente como ruta predeterminada. Planificar gateways y rutas antes de activar.

54.8. IPsec Export: Apple Profile y Windows

Estas dos entradas proceden del paquete de exportación IPsec para pfSense Plus. Se utilizan después de configurar una VPN IPsec móvil compatible. El paquete analiza parámetros del servidor y genera material de configuración apropiado para la plataforma, sujeto a restricciones de compatibilidad; no sustituye a la VPN ni crea automáticamente el servidor.

Plataforma	Resultado habitual	Validación obligatoria
Apple (macOS/iOS)	Perfil de configuración instalable.	Identidad del servidor y SAN, certificados, contenido del perfil y usuario asociado.
Windows	Script PowerShell y archivos asociados en ZIP.	Revisar el script, procedencia, derechos de ejecución, CA y rutas split tunnel.

Los perfiles y scripts son artefactos sensibles porque pueden incorporar certificados, nombres internos, rutas o material que facilite acceder a sistemas. Deben distribuirse por canales controlados, supervisarse y

retirarse cuando se revoque un acceso. El nombre exacto «IPsec Export: Apple Profile» corresponde al menú mostrado; algunas páginas de documentación usan variantes abreviadas de la etiqueta.

54.9. L2TP: tunelización sin confidencialidad propia

L2TP transporta paquetes mediante un túnel, pero por sí solo no aporta cifrado. Puede combinarse con IPsec en modo transporte; aun así, Netgate advierte de limitaciones de interoperabilidad, especialmente con determinados clientes Windows situados detrás de NAT. No debe tratarse L2TP sin una protección criptográfica adicional como alternativa segura para acceso remoto.

SEGURIDAD No desplegar L2TP en claro sobre Internet. Para nuevas implantaciones, evaluar antes IPsec IKEv2, OpenVPN o WireGuard según requisitos de cliente, identidad, auditoría y operación.

54.10. OpenVPN: flexibilidad, TLS y operación empresarial

OpenVPN emplea un modelo servidor/cliente que sirve tanto para empleados remotos como para túneles entre sedes. Puede utilizar certificados, autenticación de usuario y servicios externos como RADIUS o LDAP según el modo. Normalmente se prefiere UDP por eficiencia; puertos y protocolos son configurables y siempre deben concordar con las reglas y la infraestructura de red.

En pfSense Plus está disponible Data Channel Offload (DCO) en versiones compatibles. Permite procesar tráfico de datos en el núcleo del sistema operativo y mejorar rendimiento, pero no es aplicable a cualquier configuración: existen restricciones de modo, cifrados, compresión, UDP y funciones de routing interno. No debe activarse sobre una VPN crítica sin revisar previamente la matriz de compatibilidad y disponer de una vía de recuperación.

54.11. WireGuard: claves, peers y rutas explícitas

WireGuard es una VPN de capa 3, con conjunto reducido de parámetros y alta eficiencia. Cada participante utiliza claves criptográficas y se describe como peer; las redes admitidas se asocian en Allowed IPs. No incluye autenticación de usuarios, contraseña, MFA ni una gestión central de identidad equivalente a OpenVPN o determinados despliegues IPsec. Esa responsabilidad puede exigir controles adicionales fuera del protocolo.

Netgate distribuye WireGuard como paquete instalable en pfSense Plus y CE compatibles. Los túneles pueden requerir rutas y reglas explícitas; la lista Allowed IPs no garantiza por sí sola que se hayan añadido todas las rutas necesarias a la tabla del sistema. La exposición WAN se permite mediante reglas configuradas por el administrador.

RIESGO La duplicación de Allowed IPs entre varios peers de un mismo túnel, las claves distribuidas sin inventario o las rutas predeterminadas mal planificadas pueden provocar tráfico hacia el peer equivocado o pérdida de conectividad.

54.12. Elección del protocolo: criterios objetivos



Figura 54.3. Árbol de decisión orientativo según interoperabilidad, identidad y sencillez técnica.

Factor	IPsec	OpenVPN	WireGuard
Interoperabilidad de fabricantes	Muy amplia	Variable	Variable

Factor	IPsec	OpenVPN	WireGuard
Identidad de usuarios	Según perfil IKE/EAP/certificados	Certificados y/o autenticación	Claves de peers; sin usuarios nativos
Modelo de túnel	Políticas o VTI	Servidor/cliente	Túneles y peers L3
Operación con NAT	NAT-T y reglas correctas	Un puerto TCP o UDP	Un puerto UDP
Multi-WAN	Admite diseños multi-WAN	Admite diseños multi-WAN	Admite diseños multi-WAN
Criterio principal	Estándar e integración	Flexibilidad de identidad y políticas	Simplicidad y eficiencia

La selección no depende solo de la velocidad teórica. Debe valorarse la existencia de clientes corporativos gestionados, la necesidad de autenticación individual, registros de acceso, compatibilidad con dispositivos de terceros, resiliencia, requisitos normativos y procedimientos de alta y baja de usuarios.

54.13. Puertos y protocolos: referencia inicial

Tecnología	Tráfico exterior típico	Observaciones
IPsec / IKE	UDP/500	Negociación IKE; configuraciones avanzadas pueden usar otros puertos.
IPsec / NAT-T	UDP/4500	Encapsulación en presencia de NAT, según negociación.
IPsec / ESP	Protocolo IP 50 (no es un puerto)	Puede viajar fuera de UDP en conexiones sin NAT-T.
OpenVPN	UDP/1194 como ejemplo común	Puerto y transporte configurables; confirmar instancia real.
WireGuard	UDP/51820 como valor habitual	Puertos de túnel y peer configurables.
L2TP	UDP/1701, según diseño	No equivale a cifrado; verificar protección IPsec adicional.

La tabla es una guía técnica, no una lista de puertos que deban abrirse indiscriminadamente. Se autorizan únicamente los necesarios, en las interfaces y orígenes apropiados. En pfSense, IPsec puede añadir reglas de establecimiento de forma automática; OpenVPN y WireGuard no abren de forma general la WAN al configurarse.

54.14. Firewall, NAT y rutas: tres planos que nunca deben confundirse

Una VPN utilizable necesita simultáneamente un plano de entrada exterior para negociar o recibir paquetes del túnel, un plano de autorización del tráfico ya descifrado y un camino de ida y vuelta entre las redes. La página Firewall → Rules y sus pestañas específicas son determinantes; también lo son System → Routing, los gateways y, si procede, Firewall → NAT.

Capa	Comprobar	Síntoma si falla
Regla WAN / establecimiento	Permitir solo el transporte exterior que corresponda.	El extremo no contacta al servicio VPN.
Reglas sobre tráfico interior	Accesos precisos a redes, puertos y segmentos de destino.	El túnel conecta pero un servicio no responde.
Rutas	Ruta local al prefijo remoto y retorno desde el destino.	Paquetes unidireccionales o asimetría.
NAT	Evitar NAT inesperado entre redes; aplicar únicamente el requerido.	Direcciones origen inesperadas y fallos selectivos.
DNS	Zonas internas, resolutores y respuestas A/AAAA coherentes.	Funciona por IP pero no por nombre.

Los detalles no son iguales en todos los protocolos: IPsec policy-based hace corresponder el tráfico con políticas; VTI, OpenVPN y WireGuard utilizan mecanismos de encaminamiento basados en rutas. Además, las reglas sobre interfaces VPN asignadas pueden diferir de las pestañas genéricas. No aplicar un mismo procedimiento sin verificar el tipo de túnel.

54.15. IPsec basado en políticas frente a VTI basado en rutas

El modelo basado en políticas decide qué tráfico se encapsula utilizando selectores de seguridad definidos en las asociaciones IPsec. Por ello, una simple ruta estática no activa un túnel policy-based. VTI crea una interfaz lógica con direccionamiento y puede incorporar routing dinámico, monitorización, reglas por interfaz y gateways, según las opciones avanzadas de filtrado. Elegir VTI solo si el extremo remoto lo soporta y se conocen sus implicaciones de NAT, reply-to y routing.

CAMBIO CRÍTICO El modo de filtrado IPsec en System → Advanced o en la configuración avanzada correspondiente puede modificar cómo se evalúan las reglas en túneles VTI. Documentar el modo actual antes de cambiarlo y mantener acceso de administración alternativo.

54.16. Split tunnel, full tunnel y prevención de fugas

Diseño	Comportamiento	Ventaja / riesgo
Split tunnel	Solo destinos corporativos seleccionados cruzan la VPN.	Menor carga central, pero requiere control de DNS y acceso dual.
Full tunnel	El tráfico del cliente, incluido Internet, se envía a la VPN.	Inspección y política central a cambio de más consumo y latencia.
Sin política IPv6	El equipo dispone de IPv6 fuera de una VPN IPv4.	Una respuesta AAAA puede favorecer una ruta directa no esperada.

Netgate advierte de rutas de fuga involuntarias en entornos dual-stack. La política debe definir explícitamente los destinos IPv4 e IPv6, la resolución DNS, la salida a Internet y el tratamiento ante caída del túnel. No suponer que cifrar IPv4 cubre también IPv6 o que habilitar una VPN implica un kill switch del cliente.

54.17. Identidad, certificados, secretos y ciclo de vida

- Emitir identidades diferenciadas por usuario o dispositivo y evitar cuentas técnicas compartidas para acceso cotidiano.
- Utilizar certificados y CA verificables cuando corresponda; comprobar nombre del servidor, SAN, caducidad y revocación.
- Aplicar MFA en las tecnologías e integraciones que lo permitan; WireGuard por sí solo no ofrece MFA nativo.
- Proteger claves privadas, archivos de exportación, PSK y copias de configuración, con acceso basado en roles.
- Documentar altas, renovaciones, revocaciones y bajas; probar la revocación y el corte efectivo de acceso.
- Registrar responsables de cada túnel, peer, prefijo autorizado y dependencia empresarial.

Cifrado fuerte no corrige credenciales robadas ni una autorización excesiva. La superficie de riesgo incluye endpoints, estaciones cliente, certificados, DNS, directorios y sistemas que reciben conexiones desde la VPN.

54.18. VPN y política de mínimo privilegio

No debe confiarse en un paquete únicamente por haber llegado descifrado desde una VPN. Las reglas deben distinguir equipos gestionados, usuarios, servicios y entornos. Para una sede remota, puede ser apropiado permitir únicamente ERP o escritorios publicados mientras se bloquea la administración del firewall, los servidores de copias y las redes industriales.

Control	Recomendación
Segmentación	Filtrar por VLAN, subnet y destino; separar usuarios, servidores, invitados y dispositivos OT.
Administración	Acceso a la GUI/SSH desde redes de gestión restringidas y controladas.
Registro	Activar registro en reglas relevantes y correlacionar eventos con identidad, túnel y tiempo.
Revisión	Auditar reglas temporales, prefijos demasiado amplios y usuarios sin vigencia.

54.19. Multi-WAN, failover y alta disponibilidad

Una instalación con dos salidas a Internet exige distinguir la interfaz de escucha, la dirección pública publicada, el gateway de respuesta y la salud de cada enlace. IPsec, OpenVPN y WireGuard pueden utilizarse en diseños Multi-WAN, pero sus mecanismos de reconexión y retorno no son intercambiables. La caída de una WAN no garantiza por sí sola que el cliente cambie a otra sin reconfiguración, DNS, rutas o mecanismos previstos.

En alta disponibilidad, el diseño debe cubrir sincronización de configuración, disponibilidad de IP virtuales, mantenimiento de estados, roles de los firewalls, rutas de los extremos y condiciones de conmutación. Probar las conmutaciones reales con tráfico sostenido: un túnel «up» no certifica que las sesiones de negocio mantengan continuidad.

54.20. Rendimiento, MTU, MSS y cifrado

El rendimiento VPN depende de potencia de CPU, aceleración criptográfica, implementación del protocolo, tamaño de paquetes, RTT, carga del firewall y características de cada acceso. La encapsulación aumenta la longitud de paquetes y puede provocar fragmentación o pérdidas si el Path MTU Discovery está roto. Ajustar MTU/MSS solo tras mediciones controladas y evitando cambios universales sin justificación.

- Medir latencia, jitter, pérdidas y throughput por dirección y por aplicación, no solo con una prueba de ancho de banda.
- Controlar saturación de CPU, uso de aceleradores, colas, errores de enlace y concurrencia.
- En OpenVPN Plus, valorar DCO únicamente en túneles y cifrados compatibles, después de probar funcionalidad y rendimiento.
- Valorar redundancia y capacidad de subida del concentrador para full tunnel y copias entre sedes.

54.21. Planificación previa: inventario técnico mínimo

Dato que se define	Preguntas de diseño
Objetivo y alcance	¿Sedes completas, usuarios móviles o acceso a una aplicación concreta?
Extremos	¿Qué productos, versiones, WAN y restricciones de NAT intervienen?
Redes	¿Prefijos sin solapamiento? ¿Hay IPv6 y VLAN internas?
Identidad	¿Certificados, cuentas, RADIUS/LDAP, MFA o claves de pares?
Rutas y NAT	¿Split/full tunnel, retorno, gateways y doble NAT?
Autorización	¿Qué orígenes acceden a qué destinos y puertos?
Operación	¿Quién monitoriza, renueva, revoca y restablece?
Continuidad	¿Plan de rollback, backups y acceso fuera de banda?

54.22. Procedimiento general para implantar una VPN nueva

01 Establecer alcance, propietario del servicio y requisitos de disponibilidad y confidencialidad.

02 Inventariar subredes, clientes, dispositivos, NAT, DNS, IPv6 y rutas de retorno; resolver solapamientos.

03 Elegir protocolo mediante interoperabilidad, identidad, rendimiento y coste operativo.

04 Comprobar que versión de pfSense Plus y paquetes soportan las opciones necesarias.

05 Realizar copia de seguridad de la configuración y documentar acceso administrativo alternativo.

06 Preparar identidades, CA/credenciales/peers con acceso mínimo y conservación segura.

07 Configurar un único túnel o usuario de prueba en ventana de mantenimiento.

08 Autorizar solo el transporte WAN necesario y aplicar las reglas internas mínimas.

09 Completar rutas, NAT requerido, DNS, split/full tunnel y tratamiento de IPv6.

10 Validar negociación, cifrado, ida/vuelta, servicios y tráfico no autorizado.

11 Medir rendimiento y comprobar reinicio, rekey, caída de WAN y recuperación.

12 Registrar configuración autorizada, alertas, responsables y procedimiento de revocación.

54.23. Tres escenarios empresariales resueltos a nivel de diseño

Escenario A · Dos sedes y servicios centrales

Necesidad: una delegación debe usar aplicaciones alojadas en un centro principal. Diseño: IPsec IKEv2 site-to-site por interoperabilidad o VTI si se desea routing dinámico y ambos extremos son compatibles. Antes de abrir acceso general, se delimitan orígenes, servidores y puertos. El éxito exige ruta de retorno, reglas específicas y pruebas de nombre y aplicación. Se incorpora supervisión de túnel y failover si existen WAN redundantes.

Escenario B · Personal móvil con identidad individual

Necesidad: acceso remoto a herramientas corporativas desde equipos gestionados. Diseño: OpenVPN con certificado individual y autenticación central, o IKEv2 según clientes compatibles. Separar subred de clientes del tráfico interno, aplicar reglas por servicio, revisar DNS y política split/full tunnel, y disponer de revocación. Una exportación de perfil o script debe almacenarse y entregarse bajo control.

Escenario C · Integración híbrida con AWS

Necesidad: comunicar servicios on-premises con una red privada cloud. Diseño: valorar AWS VPC VPN Wizard cuando los requisitos y el entorno sean compatibles. Comprobar permisos de API, región, CIDR, gateways, route tables y security groups antes de lanzar el asistente. Confirmar los cambios creados a ambos lados y probar comunicación bidireccional y failover.

54.24. Comprobación reproducible: qué significa realmente «funciona»

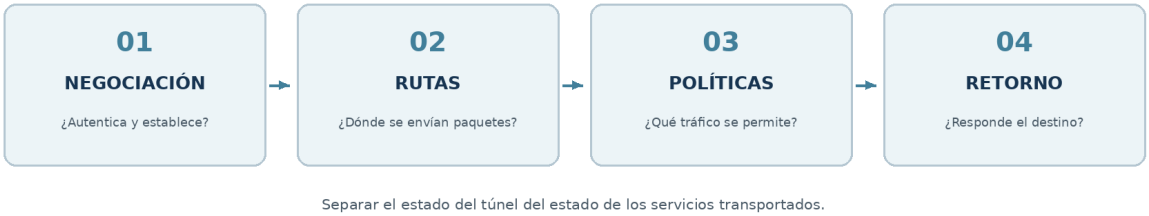


Figura 54.4. Secuencia de diagnóstico desde la negociación hasta la respuesta del servicio.

Prueba	Método	Resultado esperado
Estado del túnel	Consultar Status (IPsec/OpenVPN/WireGuard según tecnología).	Servicio y negociación correctos; peers esperados.
Transporte exterior	Capturar en WAN y revisar logs del firewall.	Se observa tráfico del protocolo/puerto previsto.
Encaminamiento	Revisar tablas de rutas, selectors IPsec y gateways.	Destino utiliza el camino VPN correcto.
Políticas	Inspeccionar Firewall → Rules y logs de bloques.	Solo pasan flujos definidos explícitamente.
Respuesta	Generar tráfico desde un host con origen apropiado.	Tráfico bidireccional sin asimetría.
Servicio real	Probar DNS, TLS y aplicación concreta.	La aplicación responde con la identidad esperada.
Recuperación	Simular cierre o caída WAN de forma controlada.	Alarma, reconexión y retorno previstos.

54.25. Diagnóstico de incidencias: síntomas, causas y comprobación

Síntoma	Posibles causas	Acción de comprobación
No hay establecimiento	WAN bloqueada, credenciales, reloj/certificado, puertos/NAT.	Revisar logs, capturas y parámetros de negociación.

Síntoma	Posibles causas	Acción de comprobación
Conecta pero no hay tráfico	ACL interna, selectors, rutas, Allowed IPs, firewall.	Probar por IP y revisar reglas, estado y rutas.
Solo funciona un sentido	Ruta de retorno, NAT o asimetría Multi-WAN.	Capturas coordinadas a ambos lados.
Por IP sí, por nombre no	DNS no accesible o registros A/AAAA inadecuados.	Consultar DNS desde cliente con su resolver real.
Velocidad baja / cortes	MTU/MSS, CPU, pérdidas, DPD/keepalive, saturación.	Pruebas con tamaños, métricas y monitorización.
Tras cambiar WAN falla	Bind, DNS público, gateway y rutas residuales.	Verificar IP exterior efectiva y reglas de cada WAN.
Fuga fuera del túnel	Split tunnel parcial, IPv6 directo, rutas locales.	Capturar WAN y verificar política IPv4+IPv6.

54.26. Cambios de alto riesgo y plan de reversión

INTERRUPCIÓN CRÍTICA Modificar gateways por defecto, filtros VTI, reglas de gestión, NAT, redes Fase 2, Allowed IPs, DNS o WAN puede cortar tanto el tráfico de usuarios como el acceso administrativo. Nunca aplicar simultáneamente cambios de varias capas sin prueba controlada.

01 Guardar backup antes del cambio, identificar un responsable y mantener una consola o vía de gestión alternativa.

02 Registrar configuración previa, objetivo, prueba de éxito y criterios precisos de rollback.

03 Modificar una única capa cada vez (túnel, ruta, regla o DNS) y observar su efecto real.

04 Validar conectividad de administración, usuarios críticos y servicios de retorno.

05 Si falla, revertir en orden inverso y confirmar recuperación, no solo cambio de estado en la GUI.

54.27. Monitorización, mantenimiento y auditoría continua

- Revisar estados de IPsec/OpenVPN/WireGuard, System Logs, estadísticas, errores y tiempos de negociación.
- Usar indicadores de disponibilidad del servicio real, no únicamente el estado Up/Connected.
- Alertar por pérdida de conectividad, rekey fallidos, vencimiento de certificados, fallos de autenticación y saturación.
- Auditar túneles inactivos, peers olvidados, reglas excesivas y excepciones temporales.
- Mantener una matriz de propiedad: extremo, redes, certificado o clave, fecha de renovación, contacto y objetivo.
- Reevaluar el diseño tras cambios de ISP, subredes, sistema operativo, hardware, nube o requisitos de acceso.

54.28. Glosario imprescindible de la sección

Término	Definición operativa
VPN	Red lógica privada construida sobre una infraestructura compartida.
IKE / IKEv2	Negociación de IPsec y asociaciones de seguridad.
ESP	Protocolo de IPsec para proteger el tráfico de datos.
NAT-T	Transporte de IPsec sobre UDP para atravesar ciertos NAT.
SA / CHILD_SA	Asociaciones que contienen parámetros de seguridad negociados.
VTI	Interfaz virtual de túnel IPsec que permite routing basado en rutas.
Peer	Extremo remoto que participa en un túnel o intercambio de datos.
Allowed IPs	Lista WireGuard asociada a un peer para selección del tráfico.

Término	Definición operativa
DCO	Data Channel Offload, aceleración del plano de datos OpenVPN.
PKI / CA	Infraestructura y autoridad para gestionar certificados digitales.
MFA	Autenticación mediante varios factores independientes.
MTU / MSS	Límites de tamaño de paquetes y segmentos que afectan al túnel.
Split tunnel	Solo determinadas rutas atraviesan la VPN.
Full tunnel	Todo o casi todo el tráfico del cliente se dirige al túnel.
DPD	Mecanismo de detección de extremos IPsec que no responden.

54.29. Lista de control previa a la puesta en producción

Antes de cerrar un proyecto VPN, verificar documentalmente: elección de tecnología; identificación de ambos extremos; inventario de redes y rutas; autenticación y revocación; reglas WAN y VPN; pruebas de DNS e IPv6; tráfico autorizado y bloqueado; monitorización; respuesta ante caídas; procedimientos de alta/baja; copias y rollback. La validación debe incluir al menos un flujo que debe funcionar y otro que debe ser denegado.

54.30. Acta de aceptación y evidencias mínimas

Una VPN no debe darse por entregada únicamente con una captura del estado Connected. La aceptación formal debe vincular cada prueba con una red de origen, un destino permitido o denegado, una hora de ejecución, un responsable y un resultado observado. Esta información facilita la auditoría, el soporte y la comparación tras actualizaciones o cambios de operador.

Evidencia de aceptación	Qué registrar y por qué
Inventario aprobado	Extremos, versión, dueño del servicio, red autorizada y finalidad.
Identidad y claves	Tipo de autenticación, caducidad y procedimiento de revocación sin revelar secretos.
Prueba positiva	Aplicación y servicio que deben funcionar desde una red concreta.
Prueba negativa	Destino/puerto deliberadamente prohibido y evidencia de bloqueo.
DNS y doble pila	Resolución interna, registros A/AAAA y ausencia de salida insegura.
WAN y recuperación	Resultado de caída controlada, alarma y reconexión si aplica.
Rendimiento base	Latencia y caudal útiles en horario o escenario acordado.
Recuperación	Backup, ventana de cambio y secuencia de reversión verificada.

Al finalizar, registrar los cambios en la documentación de red, conservar las evidencias bajo permisos apropiados y programar revisiones de credenciales, firmware, reglas y rutas. Un procedimiento probado de baja de usuario o peer debe formar parte del alcance desde el primer día.

54.31. Referencias oficiales de Netgate

Documentación oficial de referencia para funcionalidades, decisiones de diseño y advertencias. Las rutas pueden evolucionar con las versiones de pfSense Plus; consultar las notas de versión y de cada paquete antes de cambios en producción.

01. VPN: visión general

02. Guía del menú VPN

03. Escenarios comunes de VPN

04. Elección de una solución VPN

05. AWS VPC Wizard

06. Paquete IPsec Export

07. Guía IPsec

08. Diseño de túneles IPsec
09. IPsec VTI basado en rutas
10. Reglas VPN y firewall
11. IPsec: reglas exteriores e interiores
12. L2TP VPN
13. OpenVPN
14. OpenVPN DCO (pfSense Plus)
15. WireGuard
16. Configuración de WireGuard
17. IPv6 y reglas VPN
18. Diagnóstico de conexiones IPsec

55 VPN → AWS VPC VPN Wizard

Credenciales IAM · AWS VPC · IPsec · rutas · BGP · costes · validación

El asistente AWS VPC VPN Wizard integra pfSense Plus con una Amazon Virtual Private Cloud mediante una conexión IPsec site-to-site. Su principal atractivo es automatizar tanto la creación o reutilización de objetos en AWS como parte de la configuración de pfSense; precisamente por eso exige especial control de permisos, cambios y costes.



Figura 55.1. Arquitectura funcional y dos túneles proporcionados por AWS. Esquema conceptual sin datos de instalaciones reales.

55.1. Objetivo, alcance y condiciones de uso

Este capítulo explica la interfaz de credenciales, el recorrido funcional del asistente documentado por Netgate y la revisión posterior de seguridad y conectividad. Se diferencia entre controles de la interfaz descrita en este capítulo y las fases adicionales documentadas oficialmente, porque la disposición de pantallas puede variar entre versiones de pfSense Plus y del paquete.

55.2. Qué configura realmente el asistente

La VPN enlaza el cortafuegos local (Customer Gateway, en la terminología de AWS) con un Virtual Private Gateway asociado a una VPC existente. AWS entrega dos extremos de túnel, mientras pfSense utiliza información generada por AWS para montar asociaciones IPsec y, si se elige el enrutamiento dinámico, BGP mediante FRR. La conectividad funcional también depende de las rutas y de las reglas en ambos lados.

Plano	Elementos involucrados	Riesgo principal
Identidad/API	IAM, acceso a API, posibles roles asumidos	Permisos demasiado amplios o credenciales filtradas
AWS	VPC, VGW, Customer Gateway, VPN Connection	Cambios persistentes en AWS y coste recurrente
pfSense	IPsec, aliases, VIP, reglas; FRR si BGP	Rutas y políticas que alteran tráfico productivo
Operación	Comprobación de túnel, servicios, observabilidad	Considerar UP un túnel sin probar aplicaciones

55.3. Ruta de acceso y elementos generales

Ruta en pfSense Plus: VPN → AWS VPC VPN Wizard. La página se presenta como «Wizard / pfSense VPC VPN Configuration Wizard /». En el encabezado hay un icono de ayuda con signo de interrogación y una indicación de progreso («Step»), seguidos de la descripción del asistente, el bloque «AWS API Credentials» y el botón «Next». En esta primera pantalla no se muestra un botón «Back».

55.4. Primera pantalla: inventario preciso de los controles

Elemento visible	Finalidad y comportamiento esperado	Valor visible / precaución
Access Key ID	Identificador de acceso programático utilizado para firmar llamadas a AWS cuando se emplean claves.	Campo vacío; no es una contraseña de la consola web.
Secret Access Key	Parte secreta asociada al Access Key ID; permite firmar solicitudes.	Campo vacío; información de máxima sensibilidad.
Assume Role ARN	ARN de rol de IAM; el texto de ayuda alude a usar un perfil de instancia EC2 para asumir un rol en vez de claves.	Campo vacío; requiere diseñar permisos y relación de confianza.
Partition	Selecciona la partición de AWS en la que reside la VPC.	Se ve «AWS Public Cloud»; no se infieren otras opciones.
Next	Avanza hacia la fase siguiente tras procesar la entrada.	No debe pulsarse con credenciales reales no revisadas.
Ayuda / Step	Ayuda contextual e indicación visual del progreso.	No cambia por sí mismo la VPN.

55.5. Access Key ID: identidad programática

El Access Key ID identifica una clave de acceso de IAM, pero no demuestra por sí solo una autorización suficiente. Para que el asistente consulte y cree recursos se necesita una política IAM que habilite las operaciones requeridas. Las identidades deben ser dedicadas, auditables y sometidas a mínimo privilegio; la clave raíz de AWS no debe utilizarse.

Si se trabaja con claves de larga duración, establecer almacenamiento seguro, rotación planificada y revocación tras el proceso cuando deje de ser necesario. No introducirlas en documentación, tickets, registros o capturas; tampoco incorporar credenciales reales a la configuración de ejemplo.

55.6. Secret Access Key: firma y gestión segura

La Secret Access Key es el secreto criptográfico emparejado con el identificador de acceso. Una copia de esta clave junto al Access Key ID permite realizar llamadas autorizadas con los permisos de esa identidad. Debe tratarse como una contraseña de alto impacto, almacenarse en un gestor de secretos y revisarse antes de concederle acceso a recursos de red.

RIESGO No pegar jamás credenciales de producción en un documento técnico, capturas públicas, herramientas de soporte no aprobadas ni historiales de comandos. Ante una exposición, inactivar o revocar la clave y revisar CloudTrail y los recursos modificados.

55.7. Assume Role ARN: roles, perfiles y credenciales temporales

El texto de ayuda visible indica: «Use EC2 instance profile to assume role instead of keys». Este campo identifica un rol IAM por ARN; su uso requiere que la instancia tenga un perfil de instancia o credenciales fuente válidas y que la política de confianza del rol permita sts:AssumeRole. En una instalación pfSense alojada en EC2 es preferible estudiar el uso de roles y credenciales temporales antes que incrustar claves permanentes.

La prioridad entre claves y rol depende de la implementación del paquete y de las credenciales de origen disponibles. No se deben rellenar los tres campos sin conocer el método elegido ni asumir que un ARN proporciona por sí solo autenticación. Verificar los requisitos de la versión instalada.

55.8. Partition: selección de nube de AWS

La partición de AWS delimita el espacio de cuentas, recursos ARN y puntos finales de servicio. En la interfaz de este capítulo aparece «AWS Public Cloud» como opción seleccionada. Esto no equivale a elegir una región: una partición puede contener varias regiones. La documentación histórica de Netgate menciona un selector «Region» en esta primera fase; la interfaz descrita aquí expone «Partition». No deben confundirse ambos controles ni asumirse el orden de versiones anteriores.

Antes de continuar, verificar la partición a la que pertenece realmente la cuenta y la VPC. Si existe un entorno de AWS GovCloud u otra partición, validar primero soporte del paquete y endpoints compatibles. No editar archivos internos del asistente para forzar valores sin un plan de soporte y recuperación.

55.9. Botón Next: validación y comportamiento

«Next» continúa el asistente. Según la guía oficial de Netgate, al procesar la autenticación el sistema consulta AWS para localizar las VPC disponibles y comunica los errores de autenticación. Esto requiere conectividad HTTPS de salida hacia las API de AWS, DNS funcional, fecha/hora correctas y políticas IAM apropiadas. La primera pantalla por sí sola no prueba el acceso real a la cuenta.

55.10. Precondiciones antes de introducir credenciales

- VPC de destino previamente creada y identificada en la cuenta y región correctas; el asistente no crea una VPC nueva.
- Plan de direcciones sin solapamientos entre redes locales y subredes de la VPC, con IP pública de terminación conocida.
- Acceso administrativo de respaldo al cortafuegos y copia verificada de su configuración.
- Políticas IAM revisadas y registro de actividad de la cuenta AWS disponible para auditoría.
- Ruta de salida hacia endpoints de AWS, resolución DNS y sincronización NTP comprobadas.
- Responsable del coste autorizado; plan de reversión de VPN Connection y cambios de Security Groups.

55.11. Mapa completo de la secuencia funcional

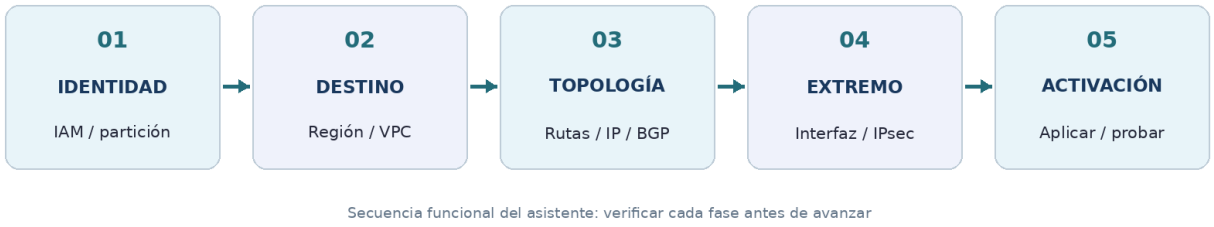


Figura 55.2. Fases de trabajo según el flujo documentado por Netgate; los formularios concretos pueden variar por versión.

El esquema siguiente separa la obtención de la identidad, la elección de destino, la planificación de rutas, la creación de los túneles y la validación. Los nombres de campos de etapas posteriores que se citan a continuación corresponden a la guía oficial publicada de Netgate; no se afirman como controles visibles en la primera página del asistente actual.

55.12. Paso siguiente: localización de VPC y región

El asistente permite consultar VPC existentes dentro de una región y seleccionar la deseada. La VPC debe crearse antes desde AWS. Si no aparece, revisar partición, región, cuenta, permisos ec2:DescribeVpcs y política de organización. Comprobar dónde se selecciona la región en el recorrido de la versión instalada.

55.13. Gateway virtual de AWS y recursos asociados

Después de elegir la VPC, el asistente busca un Virtual Private Gateway (VGW) asociado. La documentación oficial explica que, si no lo encuentra, puede crearlo y asociarlo mediante las API de EC2. AWS distingue este VGW del Customer Gateway, que representa el extremo local de la conexión. Para evitar objetos duplicados, conviene registrar los identificadores existentes antes de la operación.

55.14. Elección del tipo de enrutamiento: estático o BGP

Enfoque	Cómo se anuncian las redes	Cuándo considerarlo
Rutas estáticas	Los prefijos locales se registran explícitamente en la VPN Connection; se necesitan rutas coherentes en ambos extremos.	Entornos sencillos con pocos prefijos estables.
BGP	Se intercambian prefijos mediante sesiones BGP a través de los túneles; depende de FRR y parámetros correctos.	Entornos con cambios de rutas, necesidades de convergencia y operación vigilada.

AWS recomienda BGP cuando el equipo lo admite por su capacidad de detección de estado y apoyo al failover; sin embargo, no debe suponerse que todas las topologías o versiones del asistente proporcionen conmutación automática bidireccional. El diseño operativo debe probarse bajo fallo controlado.

55.15. BGP AS Number: significado y comprobaciones

En el formulario de routing descrito por Netgate, «BGP AS Number» identifica el sistema autónomo del extremo local. La guía publicada indica que, cuando BGP se selecciona y el campo se omite, se utiliza 65000; esa cifra es una referencia de esa guía, no un valor predeterminado confirmado para una versión no identificada. Antes de aceptar un ASN deben revisarse la política de numeración, su unicidad relevante y las reglas de importación y exportación de prefijos.

55.16. Local Public IP Address y terminación externa

El campo documentado «Local Public IP Address» designa la dirección IPv4 pública con la que AWS reconocerá el Customer Gateway. En una instancia EC2 podría ser su Elastic IP; en un appliance físico, una WAN pública asociada a la terminación del túnel. Un equipo tras NAT exige especial atención a NAT-T y a que el recurso AWS apunte a la IP pública que realmente recibe tráfico. No debe confundirse la IP privada de la WAN con su dirección visible desde Internet.

Ejemplo puramente documental: una IP pública 198.51.100.10 puede representar el extremo de un esquema, sin que tal dirección se utilice para configurar una infraestructura real.

55.17. Local subnets: anunciar únicamente las redes necesarias

El asistente documenta el campo «Local subnets» para indicar los prefijos accesibles a través del lado pfSense. Se deben incluir solo redes que deban alcanzar cargas AWS; evitar anunciar rutas de administración, invitados o servicios no autorizados. Comprobar rutas de retorno, segmentación VLAN, conflictos con rutas existentes y políticas de filtrado. El direccionamiento del ejemplo conceptual no representa ninguna instalación.

55.18. Qué acciones puede realizar el asistente en AWS

La documentación de Netgate describe llamadas de lectura y de creación/reutilización de VGW, Customer Gateway y VPN Connection; además, etiquetas, propagación de rutas, rutas estáticas y ajustes de Security Groups. Esto significa que completar el asistente no se limita a guardar datos locales: modifica recursos de una cuenta AWS con persistencia independiente del cortafuegos.

Objeto	Acción documentada	Revisión posterior
Virtual Private Gateway	Búsqueda; creación/asociación si no existe.	VGW unido a la VPC correcta.
Customer Gateway	Búsqueda por IP pública; creación si hace falta.	IP pública, ASN y cuenta correctos.
VPN Connection	Búsqueda de coincidencia o creación; devuelve XML de túneles.	Túneles, estado y cargos activos.
VPC Route Tables	Habilita propagación desde VGW; añade rutas estáticas si corresponde.	Rutas esperadas, sin desviar tráfico productivo.

Objeto	Acción documentada	Revisión posterior
Security Groups	Puede autorizar entrada desde subredes locales.	Principio de mínimo privilegio: revisar reglas ampliadas.

ATENCIÓN La guía oficial documenta modificaciones automáticas en Security Groups. Una conectividad inicial satisfactoria no garantiza que el alcance permitido cumpla la política de seguridad; revisar y ajustar el acceso por servicio y origen.

55.19. Costes: comienzo de la facturación y limpieza

Netgate advierte que la creación de VPN Connection en AWS puede iniciar cargos recurrentes mientras el recurso siga existiendo, incluso con túneles caídos o sin tráfico. La guía menciona importes históricos que pueden variar por región y fecha: consultar los precios vigentes en AWS en vez de presupuestar con cantidades antiguas. Borrar asociaciones IPsec del cortafuegos o apagarlo NO elimina automáticamente una VPN Connection de AWS.

COSTE Antes de avanzar hacia la creación de la VPN Connection, disponer de aprobación de coste y de un procedimiento para eliminar el recurso en AWS si se cancela el despliegue.

55.20. Selección de interfaz local y WAN adecuada

La documentación Netgate describe una etapa posterior donde se selecciona la interfaz pfSense sobre la cual residirán los túneles. Debe estar relacionada con la IP pública indicada. En escenarios Multi-WAN, no basta con escoger la interfaz deseada: revisar política de salida, gateway por defecto, respuestas a AWS, NAT, persistencia de rutas y comportamiento de failover. Un cambio de WAN que altere la IP pública requiere revisar el Customer Gateway en AWS.

55.21. Cambios automáticos dentro de pfSense Plus

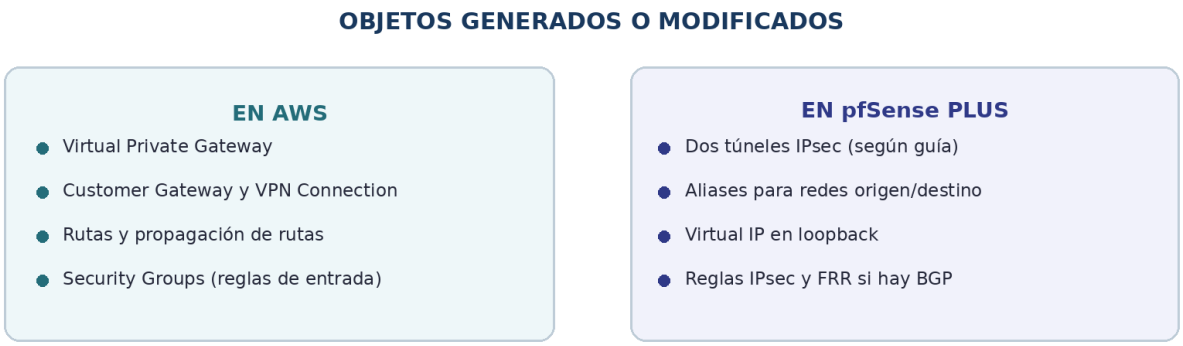


Figura 55.3. Objetos de AWS y pfSense que pueden crearse o modificarse al completar el asistente.

La documentación de Netgate describe la creación de dos configuraciones IPsec, dos aliases asociados a redes, dos direcciones virtuales de interior de túnel sobre loopback, una regla de firewall IPsec y, si se elige BGP, la instalación y configuración de FRR. El inventario resultante debe compararse con el plan de cambios aprobado antes y después de aplicar.

55.22. Direcciones internas del túnel y modo de prueba

AWS proporciona direcciones de interior de túnel en subredes /30 del espacio IPv4 link-local, utilizado para transporte interno y enrutamiento BGP. Son diferentes de las IP públicas de los peers y de los prefijos de las aplicaciones. Netgate explica que puede comprobarse un extremo mediante Diagnostics → Ping, escogiendo como origen la dirección interior local correspondiente. Las direcciones deben leerse de los recursos generados y no suponerse a partir de un patrón fijo.

55.23. Reglas de firewall y rutas: una VPN levantada no basta

La regla IPsec configurada por el asistente usa aliases para limitar pares origen/destino, pero debe validarse contra la matriz de servicios autorizados. También se necesitan reglas aplicables a la red local, tablas de rutas de la VPC, Security Groups y, cuando proceda, NACL. Revisar si el tráfico utiliza el origen esperado; una traducción NAT accidental puede hacer que AWS reciba direcciones distintas de las configuradas en el túnel.

55.24. Dos túneles: redundancia real y limitaciones documentadas

Cada AWS Site-to-Site VPN clásica dispone de dos túneles. En la FAQ del asistente Netgate se documenta una limitación concreta de configuraciones basadas en fases 2 con selectores idénticos: el tránsito saliente no siempre conmuta por sí solo al segundo túnel; puede requerir deshabilitar la fase 2 del primero y aplicar. Esa advertencia se refiere a las implementaciones descritas por la guía y debe contrastarse con la modalidad IPsec, versión y arquitectura efectivamente usada. AWS, por su parte, recomienda utilizar ambos túneles.

RIESGO No presentar la existencia de dos túneles como garantía automática de alta disponibilidad. Verificar por separado caída del túnel primario, retorno de tráfico, BGP, recuperación y rutas activas.

55.25. Aplicación de cambios y comprobación de estado

El manual oficial describe una pantalla que solicita aplicar la configuración. Después, el navegador redirige al estado IPsec. En despliegues nuevos los túneles pueden tardar varios minutos en establecerse; antes de declarar el servicio operativo deben comprobarse tanto las asociaciones IKE/CHILD-SA como la transmisión de tráfico y el acceso a aplicaciones permitidas.

01 Comprobar el inventario de cambios y las reglas que el asistente ha añadido.

02 Aplicar los cambios en una ventana de mantenimiento autorizada, conservando acceso administrativo alternativo.

03 Consultar VPN → IPsec y Status → IPsec para identificar estado de cada túnel según interfaz de la versión.

04 Revisar rutas, sesiones BGP/FRR si procede, Security Groups y registros pertinentes.

05 Probar ICMP si está permitido y después servicios reales con origen y destino conocidos.

06 Simular una interrupción de túnel solo bajo procedimiento aprobado y con plan de retorno.

55.26. Procedimiento práctico A: despliegue con rutas estáticas

Caso: una red corporativa autorizada necesita alcanzar varias instancias de una VPC existente. El método estático es apropiado cuando hay pocos prefijos y no se requiere intercambio dinámico.

01 Documentar los dos conjuntos de redes y comprobar que no se solapan.

02 Identificar región, partición, VPC, IP pública del Customer Gateway y responsables de la cuenta.

03 Preparar una identidad IAM de mínimo privilegio y un registro de cambios.

04 Abrir VPN → AWS VPC VPN Wizard, completar el método de credenciales elegido y seleccionar la partición correcta.

05 Seleccionar la VPC existente y routing estático conforme a la pantalla que presente la versión.

06 Introducir únicamente prefijos locales autorizados y la IP pública de terminación; revisar antes de avanzar.

07 Seleccionar la interfaz adecuada; documentar objetos creados en AWS y en pfSense.

08 Aplicar, validar ambos túneles, rutas, reglas y servicios; restringir Security Groups si fueran demasiado amplios.

55.27. Procedimiento práctico B: enlace con BGP y FRR

Caso: varias redes locales cambian con relativa frecuencia y se prefiere la distribución de rutas mediante BGP. Es imprescindible confirmar que el paquete y la topología seleccionada ofrecen una configuración compatible.

01 Definir ASN local apropiado, lista de prefijos autorizados y política de filtrado de rutas.

02 Confirmar que la VPC y el virtual private gateway previstos admiten la configuración deseada.

03 Elegir BGP en la etapa de enrutamiento documentada; revisar la instalación/configuración de FRR.

04 Comprobar IP internas de ambos túneles, vecinos BGP, rutas aprendidas y rutas anunciadas.

05 Hacer pruebas de convergencia y de failover sobre ambos túneles; registrar tiempos y resultados.

06 Configurar supervisión de sesiones, alertas y copias de configuración antes de producción.

55.28. Procedimiento práctico C: rol IAM con instancia EC2

Caso: el firewall pfSense Plus está desplegado como instancia EC2 y se pretende minimizar el uso de claves permanentes. El texto de ayuda del campo Assume Role ARN sugiere el empleo de un perfil de instancia para asumir un rol.

01 Crear un rol IAM orientado a la tarea con los permisos estrictamente necesarios sobre recursos definidos.

02 Configurar una relación de confianza adecuada y, si es necesario, autorización sts:AssumeRole.

03 Asociar el perfil de instancia a la EC2 según las prácticas actuales de AWS y restringir acceso a IMDS.

04 Completar el campo Assume Role ARN cuando sea el modo previsto por el paquete, sin suponer que claves y ARN son obligatorios a la vez.

05 Validar mediante registros AWS la identidad que ejecuta las acciones y retirar permisos temporales al finalizar.

55.29. Escenario Multi-WAN: contingencias y ruta de salida

Si el cortafuegos utiliza varias salidas a Internet, el túnel solo puede establecerse de forma estable si los paquetes IKE/ESP o NAT-T salen por la interfaz prevista y reciben respuesta de manera consistente. La conmutación de WAN cambia potencialmente la IP pública del Customer Gateway y puede dejar inutilizada la configuración AWS hasta actualizar el recurso y renegociar. Este asistente no debe considerarse un mecanismo general de failover Multi-WAN.

55.30. Diagnóstico por capas

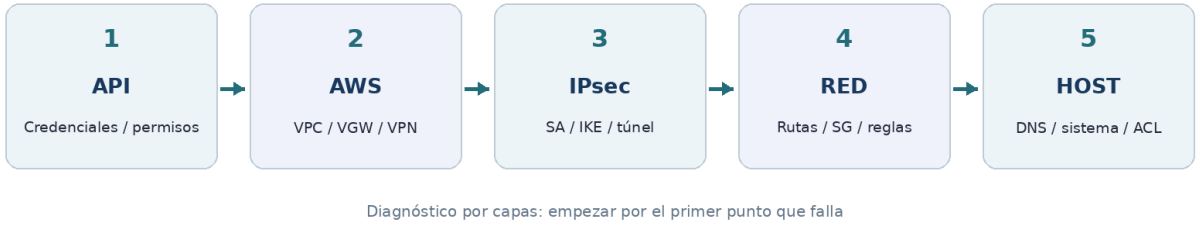


Figura 55.4. Secuencia recomendada de diagnóstico: identidad, objetos AWS, IPsec, rutas y aplicación.

Síntoma	Hipótesis inicial	Comprobación práctica
No lista la VPC	Cuenta, partición, región o permisos erróneos	IAM, DescribeVpcs, VPC existente y alcance de API.
Fallo de identidad	Clave inválida, rol no asumible o tiempo/DNS incorrectos	STS, IAM, confianza del rol, NTP, registros de AWS.
VPN creada, IKE DOWN	IP pública, NAT-T, firewall upstream o proposals	Peers, UDP 500/4500, registros IPsec y AWS.
IPsec UP, sin tráfico	Rutas, phase 2/CHILD-SA, filtros o Security Groups	Packet capture, rutas, reglas de ambos extremos.
Un túnel cae	Endpoint AWS, DPD, link o política de failover	Estado de ambos y prueba controlada de conmutación.
BGP no aprende	ASN o vecinos incorrectos, FRR parado	Status FRR, peers, IP interiores, filtros de rutas.
Se siguen cobrando recursos	VPN Connection aún creada en AWS	VPC Console, facturación y eliminación autorizada.

55.31. Supervisión y evidencias de aceptación

- Registrar los identificadores de VPC, VGW, Customer Gateway y VPN Connection en el inventario seguro de cambios, no en documentos públicos.

- Vigilar el estado de ambos túneles, errores de negociación y duración de las asociaciones, con eventos de CloudWatch si corresponde.
- En caso de BGP, supervisar vecinos, prefijos, retiradas y estabilidad de la sesión.
- Capturar datos de prueba: origen/destino simbólicos, servicio, resultado, hora, ruta y sentido, sin almacenar credenciales.
- Mantener un procedimiento claro para validar recuperación tras fallos y cambios de direccionamiento.

55.32. Cancelación, ejecución interrumpida y reversión

La FAQ de Netgate indica que, si el asistente se abandona, ejecutarlo de nuevo puede reutilizar recursos ya creados. Esto no equivale a una transacción atómica ni garantiza que no haya cambios parciales. Revisar el estado real de AWS antes de reintentarlo, especialmente VPN Connection, Security Groups y tablas de rutas. Para revertir: retirar rutas y reglas locales con cuidado, desvincular enlaces innecesarios, eliminar recursos AWS que ya no se usan y comprobar que cesan los cargos.

ATENCIÓN Borrar solo las fases IPsec de pfSense no cancela los recursos cobrables en AWS. Tampoco es seguro eliminar automáticamente gateways si los utilizan otras conexiones.

55.33. Buenas prácticas de seguridad y gobierno

- Aplicar mínimo privilegio y segmentación de redes; evitar abrir grupos de seguridad a redes locales completas cuando solo se necesita un servicio.
- Usar roles con credenciales temporales siempre que la plataforma y el flujo lo admitan; evitar claves permanentes sin necesidad.
- Proteger secretos y configuraciones exportadas; controlar acceso a backups y a registros de auditoría.
- Establecer ownership de recursos AWS, etiquetas de coste, alarmas presupuestarias y procedimiento de baja.
- Evitar solapamiento de direccionamiento, NAT implícito y confianza excesiva en un estado «UP».
- Actualizar las validaciones tras cambios del paquete, versiones pfSense Plus, plataforma AWS o algoritmos criptográficos.

55.34. Glosario operativo

Término	Definición breve
AWS Partition	Dominio lógico de AWS que agrupa cuentas, ARN y endpoints.
ARN	Identificador uniforme de un recurso de AWS.
IAM / STS	Gestión de identidades, permisos y emisión de credenciales temporales.
VPC / VGW	Red privada virtual de AWS / gateway privado virtual asociado.
Customer Gateway	Representación AWS del dispositivo extremo local y sus parámetros.
VPN Connection	Objeto AWS que vincula gateway local y gateway AWS mediante túneles.
BGP / ASN	Protocolo de intercambio de rutas / identificador de sistema autónomo.
FRR	Suite de routing usada para BGP cuando la configuración lo requiere.
NAT-T	Encapsulación IPsec a través de NAT, normalmente UDP 4500.
Security Group	Firewall con estado de AWS asociado a recursos admitidos.

Término	Definición breve
IKE / CHILD-SA	Negociación IPsec / asociaciones que transportan tráfico cifrado.

55.35. Lista de control para puesta en producción

01 Identidad autorizada y acceso API documentados sin exponer secretos.
02 Partición, cuenta, región y VPC verificadas.
03 Prefijos en ambos lados no solapados y expresamente autorizados.
04 IP pública y WAN correctas; NAT-T verificado si procede.
05 VGW, Customer Gateway y VPN Connection identificados.
06 Precio/coste recurrente y plan de baja aprobados.
07 Rutas AWS y pfSense; Security Groups y reglas revisados.
08 Dos túneles observados y failover realmente probado.
09 BGP/FRR comprobado si aplica.
10 Servicios de negocio probados en ambos sentidos; evidencias guardadas.
11 Copia de configuración y procedimiento de reversión archivados.

55.36. Matriz de responsabilidades y evidencias de cumplimiento

Aunque el asistente automatice la creación de recursos, las decisiones sobre permisos, filtrado, rutas y presupuesto siguen perteneciendo al equipo operador. El responsable de la cuenta AWS y el administrador de red deben coordinar las autorizaciones y conservar evidencias verificables.

Responsable	Decisión que debe controlar	Evidencia recomendada
Seguridad / IAM	Qué identidad usa el asistente y durante cuánto tiempo.	Permisos concedidos, CloudTrail y revocación final.
Redes / pfSense	Qué prefijos, interfaz, IPsec y rutas pasan el túnel.	Tabla de rutas, aliases, reglas y pruebas de conectividad.
Cloud / AWS	Qué objetos y Security Groups se crean o modifican.	Inventario de VGW, Customer Gateway, VPN Connection y cambios.
Operaciones	Qué alarmas, pruebas de resiliencia y escalados quedan activos.	Panel de estado, alertas y ensayo de contingencia.
Finanzas / responsable de servicio	Qué consumo recurrente se aprueba y cuándo se elimina.	Presupuesto y procedimiento de baja de recursos.

55.37. Mantenimiento después de la puesta en servicio

Revisar de forma periódica el estado de los dos túneles, la necesidad de cada ruta propagada, los permisos efectivos en Security Groups, la continuidad de la identidad IAM y el presupuesto cloud. Después de un cambio de WAN, ASN, prefijos o topología, repetir las pruebas de tráfico y revisar objetos AWS existentes: una VPN que sigue apareciendo conectada no garantiza que la aplicación utilice el camino correcto.

En toda baja del servicio, registrar la eliminación autorizada de la VPN Connection y verificar el inventario de recursos y los cargos posteriores. Esta comprobación es tan relevante como la instalación original.

55.38. Referencias oficiales verificables

La documentación del paquete y los servicios cloud puede cambiar con el tiempo. Para la configuración en producción, contrastar la interfaz y la versión instalada con las referencias oficiales siguientes:

01. Netgate — AWS VPC Wizard (índice)
02. Netgate — Using the Wizard
03. Netgate — AWS Access Keys
04. Netgate — VPC Configuration Details

05. Netgate — pfSense Plus Configuration Details
06. Netgate — Testing Connectivity
07. Netgate — AWS VPC Wizard FAQ
08. AWS — Get started with Site-to-Site VPN
09. AWS — Routing static/dynamic
10. AWS — Temporary IAM credentials for EC2
11. AWS — Pricing Site-to-Site VPN

56 VPN → IPsec

IKEv2 · fases 1 y 2 · clientes móviles · claves · grupos · ajustes avanzados

IPsec es una de las piezas esenciales de la conectividad segura en pfSense Plus. Este capítulo analiza el menú completo y sus cinco pestañas, desde la negociación criptográfica hasta los controles avanzados del motor strongSwan, con criterios de implantación, verificación y recuperación adecuados para redes empresariales.

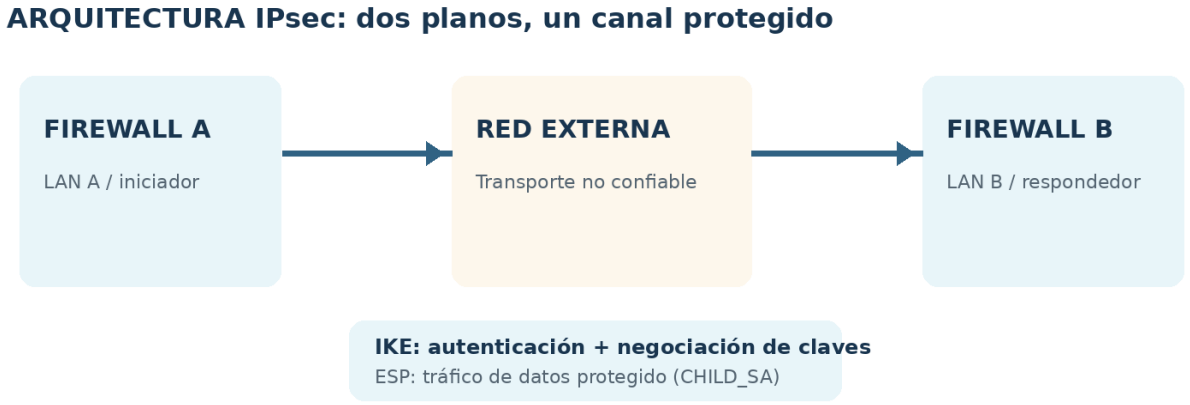


Figura 56.1. Arquitectura simplificada de control IKE y transporte ESP. Representación conceptual neutra.

56.1. Finalidad, alcance y ruta de navegación

Ruta: VPN → IPsec. La pantalla principal presenta cinco pestañas: Tunnels, Mobile Clients, Pre-Shared Keys, Mobile Group Pools y Advanced Settings. Se estudian conjuntamente porque comparten el mismo motor IPsec y sus decisiones de autenticación, direccionamiento y filtrado se condicionan mutuamente.

La vista inicial de Tunnels muestra una tabla vacía con ID, IKE, Remote Gateway, Auth/Mode, P1 Protocol, P1 Transforms, P1 DH-Group, P1 Description y Actions; el botón Add P1 inicia la creación. La segunda y tercera vistas muestran sendos listados vacíos en Pre-Shared Keys y Mobile Group Pools. Los campos de Mobile Clients y Advanced Settings se reproducen por sus etiquetas textuales, distinguiendo los desplegables efectivamente visibles de las opciones documentadas para formularios posteriores.

ALCANCE Las opciones disponibles pueden variar por versión, certificado, algoritmo, familia IP y modo de túnel. Verificar los controles y requisitos en la versión instalada antes de aplicar la configuración.

56.2. Fundamento: IKE, asociaciones de seguridad y ESP

IKE negocia identidades, autenticación, algoritmos y material criptográfico; una IKE_SA protege el intercambio de control. A continuación se establece una o varias CHILD_SA que transportan el tráfico. ESP aporta confidencialidad e integridad según la propuesta. AH ofrece autenticación de paquetes sin cifrado y rara vez se utiliza. El motor de negociación habitual en pfSense es strongSwan (charon).

IKE utiliza normalmente UDP/500. NAT Traversal (NAT-T) encapsula ESP en UDP/4500 cuando corresponde; ESP sin encapsular es el protocolo IP 50, mientras AH es el 51. No son puertos TCP. Una negociación satisfactoria no crea por sí sola rutas correctas ni reglas que permitan acceder a aplicaciones.

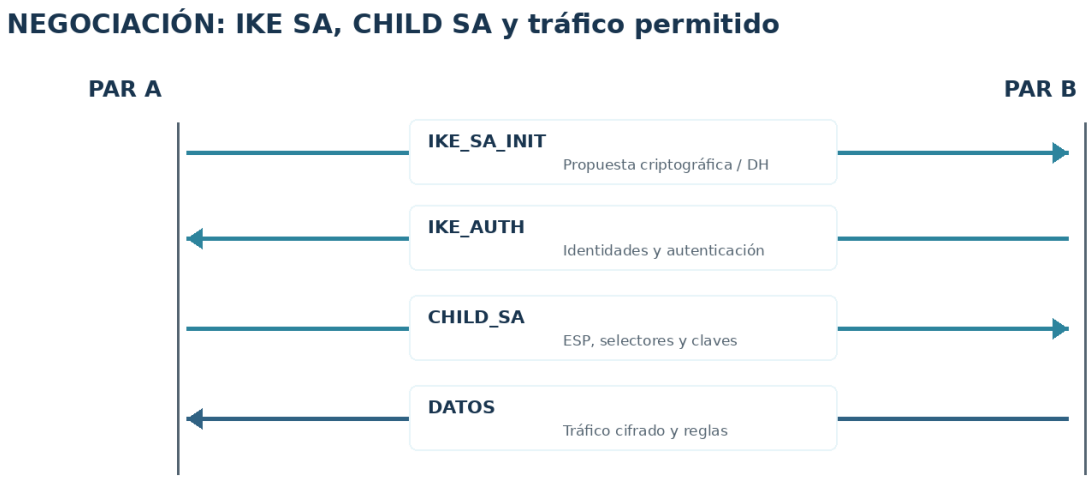


Figura 56.2. Secuencia didáctica de negociación y circulación de tráfico; no representa literalmente todos los mensajes IKE.

56.3. Tres modelos de funcionamiento: policy-based, VTI y transport

Modelo	Selección del tráfico	Aplicación más frecuente	Precaución
Tunnel IPv4/IPv6	Selectores Local Network / Remote Network	Sedes con subredes conocidas	Las redes de P2 deben concordar y no solaparse inadvertidamente
Routed (VTI)	Interfaz virtual ipsecX y tabla de rutas	Topologías con routing dinámico o múltiples rutas	Filtrado y NAT dependen del IPsec Filter Mode
Transport	Entre extremos de la propia comunicación	Protección de GRE y aplicaciones concretas	No equivale a extender una LAN completa

En modo túnel convencional el motor protege el tráfico que coincide con las políticas (SPD); en VTI el tráfico llega al interfaz virtual siguiendo las rutas. Una regla del firewall puede admitir un paquete que, por rutas o selectores incorrectos, nunca alcance el túnel. Separar política, ruta y filtrado resulta fundamental para diagnosticar.

56.4. Tunnels: columnas del listado y controles

Columna / control	Interpretación y uso
ID / IKE	Identificador interno de la fase 1 y versión de intercambio cuando hay una entrada.
Remote Gateway	Extremo remoto, IP o nombre permitido según P1.
Auth/Mode	Método de autenticación y tipo o modo expuesto por la versión.
P1 Protocol	Familia/protocolo de la negociación externa según la pantalla.
P1 Transforms	Resumen de algoritmos acordados/configurados en la fase 1.
P1 DH-Group	Grupo Diffie–Hellman de la propuesta P1.
P1 Description	Texto administrativo para localizar túneles.
Actions	Área de gestión contextual; con el listado vacío no hay iconos por fila que deban suponerse.
Add P1	Abre creación de fase 1. Una P1 agrupa una o varias P2.
Expandir P2	Con una P1 existente, se muestran los elementos Phase 2 y sus acciones, según Netgate.

La presencia de una fila indica configuración, no conectividad. El estado efectivo se comprueba en Status → IPsec. Para una modificación de producción documentar el par remoto y registrar una copia previa de configuración; al guardar y aplicar cambios pueden renegociarse conexiones.

56.5. Add P1: información general y extremo IKE

Campo documentado	Comportamiento / criterio
Description	Identifica el túnel en la GUI y los estados; conviene usar un nombre funcional neutro.
Disabled	Deshabilita esa P1 y sus P2. Útil para mantenimiento controlado.
IKE ID	Identificador informativo de la entrada; campo de solo lectura.
Key Exchange Version	IKEv1, IKEv2 o Auto. IKEv2 es preferible cuando ambos extremos lo soportan; Auto inicia v2 y puede responder a v1.
Internet Protocol	IPv4 o IPv6 exterior; independiente de que el interior pueda transportar ambas familias.
Interface	Interfaz de terminación, dirección virtual elegible o grupo de gateways si procede.
Remote Gateway	IP o FQDN del par; la resolución DNS y el comportamiento con IP dinámica requieren validación.

Un gateway 0.0.0.0 (o :: para IPv6) permite un extremo desconocido en configuraciones de túnel apropiadas, siempre que Child SA Start Action sea Responder Only y el Peer Identifier no dependa de una IP fija. Los túneles VTI necesitan un extremo concreto, por lo que esta solución no es intercambiable con VTI.

56.6. Add P1: autenticación, identificadores y certificados

Mutual PSK autentica mediante un secreto compartido; Mutual Certificate utiliza una CA y certificados, con mejor trazabilidad de identidades si se gestiona correctamente la PKI. Para movilidad hay variantes IKEv1 con Xauth (PSK, certificado, híbrida) e IKEv2 con EAP-RADIUS, EAP-MSCHAPv2 y EAP-TLS. No deben mezclarse métodos sin revisar la compatibilidad del cliente y las exigencias del servidor.

Elemento	Efecto real / riesgo
My Identifier	Identidad que presenta este firewall: IP, FQDN, E-mail, Distinguished Name, KeyID u otros tipos disponibles.
Peer Identifier	Identidad esperada del par. Seleccionar Any flexibiliza pero reduce el rigor de verificación.
Pre-Shared Key	Secreto robusto, único y protegido: no incluir en exportaciones, inventarios de ejemplo ni capturas.
CA / Certificate	Cadena de confianza, validez y coincidencia entre CN/SAN e identidad de fase 1.
IKEv1 Main / Aggressive	Main protege mejor los identificadores; Aggressive expone datos de autenticación y debe evitarse salvo legado justificado.
IKEv2 EAP	EAP-TLS autentica con certificados; EAP-RADIUS delega usuarios a RADIUS; EAP-MSCHAPv2 puede utilizar secretos tipo EAP.

SEGURIDAD No confundir el certificado del servidor con la autenticación del usuario. En EAP-RADIUS y EAP-MSCHAPv2 el cliente debe validar adecuadamente el certificado y la identidad del servidor; de lo contrario se facilita la suplantación.

56.7. Add P1: propuestas criptográficas y temporizadores

La propuesta de fase 1 describe cifrado, integridad/PRF y el grupo DH. Se prefieren suites compatibles actuales como AES-GCM y grupos DH robustos, priorizando interoperabilidad probada frente a mantener algoritmos obsoletos por comodidad. El número de opciones ofrecidas debe ser pequeño y deliberado; ofertar suites débiles puede permitir negociar una alternativa menos segura.

Control	Implicación técnica
Encryption Algorithm / Key Length	Algoritmo de protección del intercambio. AES-GCM aporta autenticación integrada.
Hash Algorithm / PRF	Autenticación o función pseudoaleatoria del IKE según la suite; PRF puede separarse en configuraciones avanzadas.
DH Key Group	Intercambio de material secreto; evitar grupos débiles y coordinar con el par.
Life Time	Vida máxima de IKE_SA en segundos. La guía emplea 28 800 s como referencia contextual, no regla universal.
Rekey Time	Renovación de claves antes de caducar; preferible en IKEv2 cuando funciona correctamente.
Reauth Time	Nueva autenticación, con mayor riesgo de interrupción que rekey.
Rand Time	Desfase aleatorio para reducir colisiones de renovación. No anular sin justificación.

La documentación también recoge Child SA Start Action (Default, Responder Only, Initiate at Start e Initiate on Demand), Close Action, DPD y otros parámetros avanzados de P1 que dependen del modo y la versión. Responder Only es habitual para clientes móviles; VTI suele iniciar al arrancar. Forzar una acción incorrecta puede dejar el túnel permanentemente pasivo o provocar reconexiones innecesarias.

56.8. Phase 2: cómo se crea y qué define

Tras guardar la P1 se despliegan sus entradas P2 mediante el control para mostrar Phase 2 y se crea una definición. En IPsec clásico una P2 equivale normalmente al conjunto de subredes que coinciden con los selectores; en VTI establece direcciones de la interfaz virtual. Una P1 puede contener múltiples P2. La pertenencia no significa que todas las CHILD_SA estén negociadas.

Grupo	Opciones verificadas y significado
General	Description; Disabled; Mode (Tunnel IPv4, Tunnel IPv6, Transport o Routed VTI); enlace a Phase 1; P2 Reqid.
Networks	Local Network, NAT/BINAT y Remote Network. En VTI determinan direcciones del enlace virtual.
SA/Key Exchange	Protocol ESP/AH; Encryption Algorithms; Hash Algorithms; PFS key group.
Expiration	Life Time, Rekey Time y Rand Time para CHILD_SA.
Keep Alive	Automatically ping host en túnel convencional, o Keep Alive de P2, según modo y compatibilidad.

Con AES-GCM en P2 no debe marcarse un hash adicional independiente. Los valores 3600 s para Rekey y 3960 s para Life Time figuran como comportamiento de referencia cuando ambos quedan vacíos en la documentación actual, pero es necesario confirmar la negociación con el remoto. PFS actúa al rekey de CHILD_SA y puede explicar fallos que no aparecen al primer establecimiento.

56.9. Procedimiento guiado: enlace site-to-site seguro

01 Preparar una copia de configuración y una ventana de cambios; confirmar IP/FQDN de ambos extremos y que no hay subredes superpuestas.

02 Definir IKEv2, interfaz de salida, Remote Gateway y autenticación (PSK aleatoria fuerte o certificados); configurar identificadores coincidentes.

03 Acordar una propuesta criptográfica y temporizadores coherentes con la configuración del par.

04 Crear P2 en Tunnel IPv4/IPv6; declarar Local Network y Remote Network inversas en ambos extremos y acordar ESP/PFS.

05 Verificar rutas, NAT y reglas en Firewall → Rules → IPsec (o interfaz VTI si el modo lo exige).

06 Guardar y aplicar cambios. Confirmar en Status → IPsec que existe IKE_SA y CHILD_SA.

07 Validar tráfico desde hosts permitidos en ambas direcciones y observar contadores, pérdida y latencia.

08 Ensayar rekey, reinicio planificado y restauración; dejar evidencia técnica y procedimiento de rollback.

INTERRUPCIÓN Al cambiar P1 o P2 es posible renegociar SAs y producir pérdidas temporales. No realizar cambios en un túnel que soporta la propia administración remota sin un canal alternativo probado.

56.10. Mobile Clients: habilitación y autenticación extendida

La pestaña Mobile Clients gobierna la autenticación y la configuración que se entrega a clientes remotos. IKE Extensions / Enable IPsec Mobile Client Support activa los controles móviles y, si aún no existe, puede ofrecer la creación de una P1 adecuada. No basta con marcarlo: deben existir P1/P2, fuente de credenciales, pool y políticas de acceso.

Control visible	Efecto y consecuencias
User Authentication	Elige origen como Local Database; también pueden existir RADIUS/LDAP previamente registrados. La captura muestra Local Database.
Group Authentication	Comprueba pertenencia/privilegios habilitados. Los grupos designados y pools deben diseñarse sin ambigüedad.
RADIUS Accounting	Registra sesiones en RADIUS; si el envío falla, los túneles pueden desconectarse.
IKE Extensions	Activa o desactiva funcionalidad móvil en la GUI y negociación asociada.

Authentication Groups permite una selección adicional cuando se utiliza autenticación por grupos. Su visibilidad depende de la configuración. La validación por grupo requiere los privilegios correspondientes, como User - VPN: IPsec with Dialin. Conceder el permiso específico mínimo y evitar privilegios administrativos generales para usuarios VPN.

ALERTA El alcance de RADIUS Accounting depende de la versión y del tipo de túnel. Comprobar si se limita a clientes móviles con IP virtual o incluye otros túneles. Los fallos de envío de contabilidad pueden provocar desconexiones: verificar la disponibilidad del servidor y el comportamiento de la versión instalada antes de activarlo.

56.11. Mobile Clients: pools, RADIUS y asignación de direcciones

Campo visible	Detalle operativo
Virtual Address Pool	Rango IPv4 virtual para clientes; nunca solapar interfaces, redes existentes u otros pools.
Virtual IPv6 Address Pool	Prefijo IPv6 independiente para clientes compatibles, con enrutamiento y reglas de ambas familias.
RADIUS IP address priority	Activado: recurrir al pool si RADIUS no asigna IP; desactivado: el cliente requiere una IP entregada por RADIUS.
RADIUS Advanced Parameters	Habilita parámetros adicionales para MFA/2FA, latencia o carga elevada.
Retransmit Base	Factor de backoff exponencial documentado: 1,4 por defecto.
Retransmit Timeout	Retardo antes del primer reintento: 2 s por defecto.
Retransmit Tries	Número de reintentos: 4 por defecto.

Campo visible	Detalle operativo
Sockets	Sockets de comunicación RADIUS: 1 por defecto; ajustar en cargas altas con pruebas.

Un pool no debe compartirse con DHCP, VPN distintas o rangos de otra sede. Las IP asignadas deben tener respuesta de retorno desde los servicios corporativos, mediante rutas o diseño de NAT explícito. La entrega de IPv6 no equivale a habilitar una política de acceso IPv6; debe evaluarse por separado.

56.12. Mobile Clients: rutas, DNS y opciones heredadas

Opción visible	Activada / desactivada y alcance
Network List	Activada: anuncia redes Local Network de P2 móvil como split-tunnel; desactivada: cliente puede intentar enviar todo el tráfico por VPN. Dependiente de cliente.
Save Xauth Password	Solicita a clientes Cisco Xauth compatibles que permitan recordar contraseña; no es generalizable a IKEv2.
DNS Default Domain	Entrega sufijo DNS, por ejemplo example.com; no garantiza resolución sin servidor accesible.
Split DNS	Dominios separados por espacios: consulta de dichos dominios por los DNS de VPN; vacío con sufijo definido suele restringir al sufijo.
DNS Servers	Envía servidores DNS. Para full tunnel, evitar que el cliente dependa de resolutores inaccesibles del ISP.
WINS Servers	Servicio heredado de resolución NetBIOS; generalmente innecesario.
Phase2 PFS Group	Sobrescribe el PFS de las P2 móviles; preferible configurarlo por cada P2 salvo necesidad documentada.
Login Banner	Texto informativo mostrado por algunos clientes Xauth tras autenticación; soporte no universal.

Una política full tunnel exige rutas de salida, NAT hacia Internet donde proceda, DNS funcional y reglas restrictivas. Split DNS y split tunnel no son equivalentes: el primero selecciona qué dominios consulta a determinados servidores, mientras el segundo decide qué destinos de red viajan por la VPN.



Figura 56.3. Cadena de autorización y direccionamiento en clientes móviles, incluida pertenencia a grupos.

56.13. Pre-Shared Keys: lista, alta y tipos de secreto

La tabla de Pre-Shared Keys muestra las columnas Identifier, Type, Pre-Shared Key y Actions y el botón Add. En vacío no puede observarse cómo se muestran las credenciales existentes ni los iconos concretos de acciones; una clave en pantalla no debe divulgarse ni reutilizarse para elaborar documentación.

Formulario Add documentado	Uso
Identifier	Nombre de usuario, host, dirección IP u otra identidad que deba coincidir con la negociación.

Formulario Add documentado	Uso
Secret Type: PSK	Clave compartida tradicional para determinados túneles IKEv1 y escenarios site-to-site.
Secret Type: EAP	Credencial para IKEv2 EAP-MSCHAPv2 en perfiles apropiados.
Pre-Shared Key	Secreto de suficiente entropía, único por contexto y protegido.
Identifier Type (EAP)	Puede forzar la interpretación del identificador cuando el modo EAP lo permite.
Virtual Address Pool (EAP)	IP individual fuera de cualquier pool global o de grupo; evita conflictos.
DNS Server (EAP)	DNS específico para ese cliente; si vacío, hereda configuración móvil.

ALMACENAMIENTO Netgate indica que los secretos de esta pestaña deben estar disponibles en texto claro para el motor IPsec. Si la política corporativa no admite esta condición, valorar autenticación RADIUS y mecanismos MFA adecuados.

56.14. Mobile Group Pools (Plus): asignación basada en grupos

Funcionalidad específica de pfSense Plus según documentación. La pantalla de lista presenta Groups, Pool y Actions con botón Add. En el formulario documentado, Groups admite nombres separados por comas, Virtual Address Pool define el bloque del grupo y DNS Server permite sobreescribir el DNS móvil general.

El mecanismo es útil con EAP-RADIUS y el atributo Class de RADIUS. Requiere Group Authentication activo y no debe solapar nombres con grupos de autenticación ni otros pools. Si un nombre de grupo coincide con un pool previamente definido o autorizado como pool por defecto, pueden operar reglas de precedencia que frustran la segmentación esperada. Se debe validar desde un cliente de prueba de cada grupo.

Decisión	Comprobación requerida
Grupos de acceso	No solapar nombres con Authentication Groups ni con otra entrada Mobile Group Pools.
Pool por grupo	No solapar con el pool general, P2 especiales ni direcciones EAP individuales.
RADIUS Class	Confirmar formato devuelto por el RADIUS real y grupo efectivo interpretado por strongSwan.
DNS por grupo	Probar que el resolutor es alcanzable y que las reglas permiten sólo los recursos previstos.

56.15. Advanced Settings: registro del daemon y sus niveles

IPsec Logging Controls permite ajustar el nivel por componente. Los valores observados en los desplegables son Silent, Audit, Control, Diag, Raw y Highest. Cuanto mayor es la verbosidad, más información se registra, con mayor consumo y riesgo de revelar metadatos. Netgate recomienda para diagnóstico un equilibrio: IKE SA, IKE Child SA y Configuration backend en Diag; el resto en Control. La vista no confirma el valor guardado de cada campo.

Componente visible	Qué ayuda a investigar
Daemon	Arranque, ejecución y actividad general de charon.
SA Manager	Administración y ciclo de vida de asociaciones de seguridad.
IKE SA	Negociación de sesión IKE, identificación y autenticación.
IKE Child SA	Creación, renovación y cierre de CHILD_SA.
Job Processing	Colas, tareas y ejecución interna del daemon.

Componente visible	Qué ayuda a investigar
Configuration backend	Carga y aplicación de parámetros de conexión.
Kernel Interface	Comunicación con el kernel y políticas IPsec.
Networking	Transporte, sockets y mensajes de red.
ASN encoding	Codificación ASN.1 y contenidos estructurados.
Message encoding	Procesamiento/codificación de mensajes IKE.
Integrity checker	Comprobaciones internas de integridad.
Integrity Verifier	Validaciones de integridad mediante módulo correspondiente.
Platform Trust Service	Eventos del servicio de confianza de plataforma.
TLS handler	Procesamiento de sesiones/funciones TLS relacionadas.
IPsec traffic	Detalles del plano de tráfico protegido.
StrongSwan Lib	Biblioteca general e infraestructura strongSwan.

Silent evita la salida de la categoría seleccionada; Audit, Control y Diag proporcionan sucesivamente más visibilidad operativa; Raw y Highest son niveles de alto detalle para ventanas acotadas de diagnóstico. No existe una equivalencia universal garantizada entre nombres de GUI y volumen exacto de eventos en cada versión de strongSwan. Después de investigar un incidente se restauran los niveles de producción.

56.16. Advanced Settings: identidad única y colisiones de sesiones

Configure Unique IDs as	Comportamiento al repetirse identidad
Yes (Replace)	La IKE_SA nueva sustituye y desconecta la anterior. Valor predeterminado indicado.
No	Acepta duplicidad, salvo que INITIAL_CONTACT provoque sustitución de la antigua.
Never	Permite simultaneidad e ignora INITIAL_CONTACT.
Keep	Rechaza la sesión nueva y conserva la anterior.

El ajuste es relevante con varios dispositivos de un mismo usuario, clientes con identidad común o configuraciones de pares repetidas. No aplicar Never como solución universal: puede ocultar identidad duplicada, aumentar sesiones concurrentes no deseadas y complicar auditoría.

56.17. Advanced Settings: IPsec Filter Mode — cambio crítico

Modo	Filtrado disponible	Consecuencia
Filter IPsec Tunnel, Transport, and VTI on IPsec tab (enc0)	La pestaña Firewall → Rules → IPsec gobierna tráfico IPsec de todos los modos.	Es el comportamiento predeterminado; limitaciones para NAT y reply-to de VTI.
Filter IPsec VTI and Transport on assigned interfaces, block all tunnel mode traffic	Se filtran VTI/transport sobre interfaces asignadas, con NAT/reply-to cuando proceda.	BLOQUEA TODO EL TRÁFICO IPsec EN TUNNEL MODE, incluido Mobile IPsec.

RIESGO ALTO No activar el segundo modo cuando haya IPsec tradicional o clientes móviles. Puede suponer una pérdida inmediata de comunicaciones entre sedes y dejar sin acceso remoto al administrador.

Antes de cambiar, inventariar todas las P2, confirmar que son VTI/transport, asignar interfaces, revisar reglas, estados y return routing. Preparar acceso alternativo por consola o red de gestión y un procedimiento de reversión.

56.18. Advanced Settings: retransmisión y rendimiento

Opción visible	Interpretación / precaución
IKEv2 Retransmission Parameters	Despliega temporizadores de reenvío para IKEv2. El texto visible no enumera sus subcampos ni valores: usar documentación de la versión antes de modificarlos.
IP Compression	Propone IPComp; Netgate advierte soporte incompleto en el sistema subyacente. Mantener desactivado salvo pruebas controladas.
PKCS#11 Support	Permite tokens PKCS#11 en P1 y servicio de tarjetas inteligentes. Reinicios de servicio pueden reiniciar IPsec.
Strict interface binding	Restringe interfaces del daemon, pero puede romper conectividad con IP dinámica; no recomendado sin laboratorio.
Maximum IKEv1 Phase 2 Exchanges	Paralelismo de rekey para una P1. Predeterminado 3; insuficiente con muchas P2.
Asynchronous Cryptography	Procesamiento paralelo de trabajos crypto(9); evaluar estabilidad en el hardware real y bajo carga.

En cuanto a IKEv2 Retransmission Parameters, la etiqueta aparece en el formulario transcrito pero no debe inventarse una lista de temporizadores ni un default genérico. Todo cambio debe documentarse con el valor real, causa y resultado de las pruebas de pérdida de paquetes y latencia del enlace.

56.19. Advanced Settings: compatibilidad y certificados

Opción visible	Acción y riesgo
Unencrypted payloads in IKEv1 Main Mode	Acepta ID/HASH sin cifrar de implementaciones antiguas. Exposición susceptible de análisis y ataques a PSK: mantener desactivado.
Enable Cisco Extensions	Activa Unity Plugin: Split-Include, Split-Exclude y Split-DNS en clientes IKEv1 Xauth compatibles.
Strict CRL Checking	Exige CRL disponible y vigente para autenticación con certificados; puede denegar túneles si CA/CRL falla.
Make before Break	Nueva IKE_SA/CHILD_SA antes de eliminar antigua durante reautenticación IKEv2; requiere soportar SAs solapadas.
FQDN Endpoints Resolve Interval	Periodicidad en segundos de resolución del par remoto FQDN; no cambiar sin considerar DNS y cambios de gateway.

El valor predeterminado de Make before Break es desactivado según Netgate, con una breve interrupción al reautenticar; al activar puede reducirla a costa de posibles incompatibilidades de solapamiento. Estricto CRL mejora exigencia de validación, pero exige disponibilidad real del servicio de revocación y plan de contingencia.

56.20. Advanced Settings: puertos, exclusiones y cifrado

Control visible	Comportamiento
Custom ports — IKE	Puerto local UDP de escucha. Predeterminado 500; un cambio afecta a todas las VPN del firewall.
Custom ports — NAT-T	Puerto local UDP de NAT Traversal. Predeterminado 4500; coordinar con redes y pares.
Auto-exclude LAN address	Crea bypass para tráfico entre subred LAN e IP LAN del firewall ante políticas IPsec.
Additional IPsec bypass	Habilita reglas adicionales para excluir tráfico específico de políticas IPsec.

Control visible	Comportamiento
IPsec Bypass Rules (documentado)	Pares Source Address / Destination Address con máscara, utilizados conjuntamente para determinar bypass.

El bypass puede impedir que tráfico local legítimo sea capturado por una P2 muy amplia, pero una exclusión excesiva puede enviar tráfico sensible fuera de su túnel previsto. Registrar origen, destino, razón de excepción y prueba de tráfico en ambos sentidos. Los puertos personalizados se deben dejar vacíos para usar los estándares salvo interoperabilidad estrictamente demostrada.

56.21. Escenario empresarial: varias sedes y enlaces de respaldo

Un concentrador central puede conectar dos delegaciones por túneles IKEv2 independientes. Se inventarían las rutas, cada P1 representa un par y cada P2 define selectores o VTI. En conectividad Multi-WAN se verifica que el extremo remoto reconozca el cambio de IP, que el DNS/FQDN o gateway group sea apropiado y que las reglas de retorno no fuercen una WAN incorrecta.

Si se usa VTI, las rutas de las redes remotas no deben quedar duplicadas con políticas de un túnel clásico. Debe probarse caída del enlace primario, restablecimiento y reconvergencia; un estado de SA conectado no garantiza que el tráfico regrese por el enlace seleccionado.

56.22. Escenario empresarial: acceso remoto por grupos

La arquitectura móvil emplea IKEv2 con certificados y, según el entorno, EAP-TLS o EAP-RADIUS con MFA proporcionado por el servidor RADIUS. Un perfil de administración accede sólo a servicios de gestión; un perfil general accede a aplicaciones de usuario. Los pools deben ser distintos y los controles de firewall imponer el principio de mínimo privilegio.

01 Configurar fuente de identidad y certificados; verificar confianza y fecha/hora de los clientes.

02 Habilitar Mobile Clients y el método de autenticación previsto en P1; crear sus P2 móviles.

03 Definir pool general sin solape; si existe segregación por grupo, activar Group Authentication y añadir Mobile Group Pools.

04 Configurar DNS y Network List; validar expresamente split/full tunnel en cada sistema operativo.

05 Permitir únicamente los destinos necesarios desde el pool; probar usuario permitido y usuario excluido.

06 Consultar Status → IPsec → Leases y logs; validar desconexiones, renovación de credenciales y RADIUS offline.

56.23. Escenario empresarial: migración desde IKEv1 heredado

Primero se documenta el perfil IKEv1 y sus dependencias de cliente. Se diseña un perfil IKEv2 paralelo con algoritmos actuales, CA y certificados cuando proceda; se prueba con un conjunto piloto y se migran grupos. Las opciones heredadas de Main/Aggressive, Xauth, Unity y hashes antiguos no deben habilitarse globalmente sólo para acomodar una minoría de dispositivos sin análisis de riesgo.

Se conserva rollback temporal, se supervisa adopción y se elimina el modo antiguo y los secretos asociados una vez validada la transición. Si los clientes no aceptan certificados, se revisan las capacidades de autenticación antes de elegir alternativas más débiles.

56.24. Verificación: estados, SAs y registros

Status → IPsec muestra túneles habilitados y conexiones activas. La vista Overview incluye IKE y CHILD SAs; Leases muestra direcciones de clientes móviles; SAD representa asociaciones instaladas; SPD recoge políticas de tráfico. Status → System Logs → IPsec permite revisar charon y los resultados de negociación.

Evidencia	Interpretación
IKE_SA ... established	Autenticación e intercambio IKE concluidos; no acredita por sí solo CHILD_SA.
CHILD_SA ... established	Parámetros y selectores de P2 negociados.

Evidencia	Interpretación
NO_PROPOSAL_CHOSEN	Propuestas incompatibles: revisar cifrado, integridad, PRF, DH/PFS.
AUTHENTICATION_FAILED	Identidades, certificados, PSK, usuario o método no coincidentes.
INVALID_ID_INFORMATION	Posible desajuste de redes/traffic selectors en P2 IKEv1.
SA activa sin datos	Revisar firewall, rutas, NAT, interfaz de filtro y retorno del host de destino.

56.25. Diagnóstico práctico y secuencia de aislamiento



Figura 56.4. Cadena ordenada de comprobaciones antes de intervenir en seguridad o rutas.

01 Confirmar que IPsec está en marcha y que hay al menos una configuración activa.

02 Revisar la interfaz de entrada: UDP 500/4500 y ESP cuando corresponda; correlacionar con logs de firewall.

03 Revisar en IPsec Logs cuál es el último intercambio correcto (IKE_SA frente a CHILD_SA) y registrar hora.

04 Comparar ambos extremos: ID, certificados, método, cifrado, hash/PRF, DH/PFS y temporizadores.

05 Si CHILD_SA se establece, verificar selectores, interfaz enc0/VTI, rutas, NAT/BINAT y reglas IPsec.

06 Realizar captura de paquetes puntual en WAN y en el destino, comprobando si hay solicitud y respuesta.

07 Provocar rekey en ventana controlada para detectar problemas de lifetimes/PFS no visibles en primera conexión.

08 Restaurar niveles de logging y cerrar la incidencia con causa raíz, cambio y resultado.

56.26. Incidencias frecuentes y su corrección

Síntoma	Hipótesis principal	Prueba y acción
No inicia IKE	Firewall/NAT/peer inaccesible	Verificar puertos UDP, endpoint, rutas WAN y estado daemon.
P1 no autentica	Identificador, PSK o certificado	Contrastar identidades exactas, cadena CA, vencimiento y logs.
IKE sí, CHILD no	Algoritmo, selectores o PFS	Comparar propuestas de P2 y subredes inversas.
Todo conectado, no hay tráfico	Regla, route-back o NAT	Revisar IPsec/enc0 o VTI asignada y firewall remoto.
Desconecta al renovar	Life Time, PFS o colisiones	Revisar rekey, Rand Time y duplicidades de SA.

Síntoma	Hipótesis principal	Prueba y acción
Cliente sin IP	Pool solapado o RADIUS sin atributo	Consultar Leases y prioridad de asignación.
DNS no funciona en full tunnel	DNS no entregado/ruta errónea	Verificar DNS Servers, reglas y split DNS.
Cae al activar filtrado VTI	Tunnel mode bloqueado	Revertir IPsec Filter Mode desde acceso de gestión alternativo.

56.27. Plan de cambios y medidas de seguridad esenciales

- Usar autenticación robusta y preferir IKEv2 cuando sea interoperable; retirar IKEv1 inseguro de forma planificada.
- Conservar inventario actualizado de pares, claves/certificados, CA, vigencias, P1/P2, rutas, reglas y responsables.
- Configurar privilegios y grupos mínimos, segregar pools y auditar sesiones; MFA cuando la solución de autenticación elegida lo permita.
- Proteger secrets, copias de pfSense y RADIUS; rotar/revocar credenciales tras bajas o incidencias.
- No cambiar simultáneamente algoritmos, selectores y reglas. Hacer una modificación medible por vez.
- Probar rekey, cortes WAN, reinicio, failover y resolución DNS con evidencias y rutas de rollback.
- No habilitar logs Raw/Highest permanentemente; limitar acceso a registros y depurar datos sensibles.
- No utilizar IPsec Filter Mode VTI en presencia de túneles policy-based o Mobile IPsec.

56.28. Lista de validación antes y después de aplicar

Antes de guardar	Después de aplicar
Acceso alternativo al firewall probado	GUI y consola de recuperación accesibles
Back-up de configuración	IKE_SA y CHILD_SA correctas
Par remoto y canales de coordinación	Pérdida/latencia de aplicaciones medida
P1, P2, grupos y pools sin solape	Reglas, DNS y rutas en ambos sentidos
Algoritmos/tiempos acordados	Prueba de rekey y desconexión
Plan para revertir	Logs restaurados y cambios documentados

56.29. Glosario esencial de IPsec

Término	Definición operativa
IKE / IKE_SA	Negociación/autenticación que protege el plano de control.
CHILD_SA	Asociación de seguridad para proteger tráfico del plano de datos.
ESP / AH	Cifrado y autenticación de tráfico / autenticación sin cifrado.
NAT-T	Encapsulación para atravesar NAT normalmente por UDP/4500.
P1 / P2	Perfiles lógicos GUI de IKE y protección/selección del tráfico.
SPD / SAD	Bases de datos de políticas IPsec y asociaciones de seguridad.
PFS	Renovación de claves con material DH independiente.
VTI / enc0	Interfaz virtual enrutada / interfaz lógica de filtrado IPsec tradicional.

Término	Definición operativa
Xauth / EAP / RADIUS	Extensión de autenticación de usuarios / métodos extensibles / servidor AAA.
CRL / PKCS#11	Lista de revocación de certificados / interfaz para dispositivos criptográficos.

56.30. Fuentes oficiales y comprobación de versión

Documentación oficial de Netgate consultada para opciones visibles y formularios adicionales. Algunos campos copiados de la interfaz, en especial IKEv2 Retransmission Parameters y FQDN Endpoints Resolve Interval, pueden variar con el firmware y no tienen aquí valores supuestos. En la implantación real deben contrastarse los formularios desplegados y la versión exacta de pfSense Plus.

01. IPsec Configuration | 02. IPsec Tunnels Tab

03. Phase 1 Settings | 04. Phase 2 Settings

05. IPsec Mobile Clients Tab | 06. IPsec Pre-Shared Keys Tab

07. IPsec Mobile Group Pools (Plus Only) | 08. Advanced IPsec Settings

09. IPsec Status | 10. Troubleshooting IPsec Connections

11. Troubleshooting IPsec Traffic | 12. Troubleshooting IPsec Logs

57 VPN → IPsec Export: Apple Profile

Perfiles de configuración Apple · IKEv2 · certificados · identidad del servidor · instalación segura

La exportación para dispositivos Apple transforma una configuración de acceso remoto IPsec ya existente en un perfil de conexión que puede instalarse en iPhone, iPad o Mac. No crea por sí misma la Phase 1, la Phase 2 ni las reglas de firewall: su misión es preparar el cliente para negociar con los parámetros del servidor.



Figura 57.1. Dependencias técnicas de la exportación IPsec. Esquema original con datos neutros.

57.1. Propósito, alcance y ubicación en pfSense Plus

Ruta exacta de la pantalla: VPN → IPsec → IPsec Export: Apple Profile. También se accede desde la entrada de VPN denominada «IPsec Export: Apple Profile». La herramienta pertenece al paquete ipsec-profile-wizard/IPsec Export, disponible para pfSense Plus cuando está instalado; no forma parte de la edición CE.

En la cabecera aparecen dos pestañas: Apple Profile, que genera el perfil de configuración, y Windows PowerShell, orientada a un script para Windows. La segunda se estudia en el siguiente capítulo por ser una herramienta distinta. Los iconos superiores dependen de la interfaz y la versión; no es correcto atribuirles funciones concretas sin examinar su ayuda contextual.

ALCANCE DE LA VERSIÓN El paquete puede denominar este menú VPN → IPsec Export: Apple o Apple Profile. Comprobar la denominación, los requisitos y los formatos compatibles en la versión del exportador y del cliente Apple.

57.2. Fundamentos: qué contiene un perfil y qué no contiene

Un archivo de configuración de Apple (.mobileconfig) describe cargas útiles o payloads de ajustes gestionados. Un payload VPN puede definir nombre visible, servidor, tipo de VPN, identificadores, autenticación, propuestas criptográficas y otros parámetros compatibles. La composición exacta depende del método de autenticación, de las opciones negociadas y de la versión del exportador.

Elemento	Función técnica	No debe confundirse con
Perfil .mobileconfig	Instala parámetros de VPN en el dispositivo Apple.	La creación del túnel en pfSense.
IKE_SA / Phase 1	Negocia identidades, algoritmos y autenticación de IKE.	La etiqueta mostrada en Ajustes.
CHILD_SA / Phase 2	Protege el tráfico de datos y establece selectores.	Un permiso automático para cualquier red.
Certificado servidor	Vincula la identidad del extremo VPN con una clave.	Una garantía de que DNS/rutas sean correctos.
Credencial de usuario	Autentica a la persona o al certificado cliente según el modo.	La clave secreta del servidor o la de la CA.

Netgate indica que el exportador busca entradas móviles de Phase 1 y Phase 2 compatibles y emplea la primera propuesta que pueda utilizar. Por ello el orden de propuestas puede cambiar los algoritmos

generados. Revisar «View» no es opcional desde el punto de vista de seguridad; permite identificar selecciones inesperadas.

57.3. Interpretación del error: «There is no Mobile Phase 1»

Si la pantalla informa de que falta una Phase 1 móvil, se debe crear o revisar ese objeto IKE de acceso remoto: el exportador lo utiliza como origen. El mensaje no implica por sí solo un fallo de certificados Apple ni del navegador. Una propuesta incompatible con el cliente también puede impedir la exportación.

Síntoma	Interpretación	Acción de comprobación
No Mobile Phase 1	No existe una entrada móvil adecuada.	VPN → IPsec → Mobile Clients y Tunnels; crear/verificar P1 móvil.
No hay cliente seleccionable	No coincide el método de autenticación con usuarios/certificados aptos.	Comprobar EAP, CA de pares, credenciales y filtros del exportador.
Server Address vacío	No se ofrecen SAN del certificado o falta configuración base.	Revisar certificado presentado y entradas SAN.
El perfil se descarga pero no conecta	La exportación es válida como archivo, pero no se ha validado la sesión.	Status → IPsec, registros IKE, puerto UDP/500 y UDP/4500.

PRECAUCIÓN DE PRODUCCIÓN Crear o cambiar una Mobile Phase 1 puede alterar compatibilidad, autenticación y conexiones existentes. Debe trabajarse con respaldo de configuración, ventana de cambio y una vía alternativa de administración. No modificar una configuración activa solamente para eliminar el aviso.

57.4. Requisitos previos en el firewall

01 Confirmar que pfSense Plus dispone del paquete de exportación y que la pestaña Apple Profile se abre correctamente.

02 Preparar un certificado de servidor cuyo Subject Alternative Name (SAN) contenga el nombre DNS público que utilizarán los dispositivos; comprobar validez, cadena y CA de confianza.

03 En VPN → IPsec → Mobile Clients, habilitar soporte móvil y decidir autenticación compatible (por ejemplo IKEv2 con EAP y certificados de servidor, o EAP-TLS cuando proceda).

04 Crear la Mobile Phase 1 e incorporar Phase 2 apropiadas; confirmar cifrados, grupos, tiempos y selectores antes de publicar el perfil.

05 Definir un pool virtual exclusivo para clientes, DNS internos y rutas de acceso, y verificar que no solapen redes usadas por los dispositivos o por el firewall.

06 Revisar reglas de IPsec/firewall, NAT, encaminamiento y permisos de servicios internos; limitar el acceso según mínimos privilegios.

07 Validar el DNS público del servidor y la llegada a UDP/500 y UDP/4500 desde un origen externo autorizado.

57.5. Inventario exhaustivo de la pantalla Apple Profile

Control visible	Comportamiento y consideración práctica
VPN Name	Texto mostrado en la lista de redes VPN del cliente; también interviene en el nombre del fichero exportado. El valor propuesto puede incorporar datos del hostname del firewall: debe revisarse antes de distribuir.
Server Address	Lista de direcciones derivada de las entradas SAN del certificado. Elegir un nombre DNS realmente resoluble, asociado a ese certificado y accesible desde el cliente.
Custom Hostname	Se utiliza al seleccionar la modalidad «Custom Hostname» en Server Address. Debe ser un FQDN válido y estar incluido en el SAN; introducir otro nombre no corrige un certificado incorrecto.

Control visible	Comportamiento y consideración práctica
VPN Client	Selecciona el cliente/identidad que se exporta según las opciones de autenticación de la Mobile Phase 1: usuario externo o certificado TLS apto, si corresponde.
External Auth Username	En autenticación externa especifica el nombre de cuenta que incluirá el perfil. El texto de ejemplo «ChangeMe» es un marcador y debe sustituirse por la cuenta autorizada; no equivale a una contraseña.
Download	Descarga el perfil generado, después de superar las validaciones. No implica que se haya instalado ni que la VPN funcione.
View	Muestra el contenido del perfil para revisión previa. Evitar publicar o pegar XML que contenga material sensible.
Apple Profile	Pestaña activa; perfiles de configuración para sistemas Apple.
Windows PowerShell	Pestaña separada de exportación Windows; no produce el mismo artefacto ni sigue el mismo proceso de instalación.
Aviso de error	Mensaje de validación: en el estado observado no hay Mobile Phase 1. Corregir la configuración de origen antes de reintentar.

57.6. VPN Name: nombre visible, archivo y control documental

«VPN Name» es una etiqueta de presentación para que la persona usuaria reconozca la conexión. Puede emplearse «VPN corporativa» o «Acceso remoto seguro»; no debe copiarse automáticamente un nombre que revele empresa, sede, ubicación interna o topología. El hecho de elegir una etiqueta no afecta a la autenticación de la identidad IKE del servidor ni modifica registros DNS.

Recomendación operativa: emplear una nomenclatura pública breve, estable y sin información clasificada, incluir la versión documental del perfil en la distribución (fuera del nombre de VPN si no procede) y retirar versiones antiguas tras los cambios de servidor.

57.7. Server Address y Custom Hostname: DNS y SAN

El cliente debe conectarse a una dirección resoluble. Para la validación de la identidad del servidor, Netgate exige que el nombre utilizado figure entre los SAN del certificado correspondiente. Un FQDN de ejemplo para documentación sería vpn.example.com. Si el certificado únicamente identifica otro FQDN, la autenticación puede fallar aunque la dirección alcance el cortafuegos.



Figura 57.2. La etiqueta no autentica; la coherencia entre DNS, nombre del extremo y SAN sí es crítica.

Comprobación	Ejemplo de documentación	Resultado esperado
Resolución DNS	vpn.example.com	Resuelve a la IP pública que conduce al servicio VPN.
SAN del certificado	DNS:vpn.example.com	Incluye el nombre exacto elegido.

Comprobación	Ejemplo de documentación	Resultado esperado
Certificado válido	Emisor de confianza y vigencia actual	Cadena verificable y certificado apto para autenticación prevista.
NAT / WAN	UDP 500 y 4500 hacia el extremo autorizado	Llegan mensajes IKE/NAT-T sin bloqueo de terceros.

NO ES UN ATAJO «Custom Hostname» no debe emplearse para eludir una discrepancia de SAN. Primero se corrigen certificado, DNS y alcance del servidor; después se genera un perfil coherente.

57.8. VPN Client y External Auth Username

VPN Client determina qué credencial de usuario se representa en el perfil. Con certificados, el exportador presenta los certificados de cliente firmados por la CA seleccionada como autoridad de pares en la Mobile Phase 1. Con autenticación externa puede mostrar External Auth y un campo específico de usuario.

Para EAP-RADIUS se utiliza una cuenta válida de RADIUS; para EAP-MSCHAPv2 con base local se necesita una identidad con la configuración de credenciales correspondiente. El nombre de usuario del perfil no concede acceso por sí mismo: el servicio de autenticación debe validar la cuenta y sus permisos. El paquete señala que Apple requiere disponer de nombre de usuario en el perfil en ciertos modos, mientras que Windows puede solicitarlo posteriormente.

GESTIÓN DE CREDENCIALES No incorporar contraseñas reutilizadas ni claves administrativas en perfiles distribuidos. Si el perfil contiene certificados personales o material criptográfico, tratarlo como un archivo sensible y entregarlo individualmente por un canal controlado.

57.9. Procedimiento de exportación paso a paso

01 Acceder a VPN → IPsec y confirmar la presencia de la Mobile Phase 1, de las fases 2 y de los clientes previstos. Resolver cualquier error de validación.

02 Abrir VPN → IPsec Export: Apple Profile y seleccionar Apple Profile.

03 Cambiar VPN Name por una denominación neutra apta para mostrarse al personal y para formar el nombre de archivo.

04 Elegir Server Address según las entradas SAN ofrecidas. Solo seleccionar Custom Hostname si el FQDN existe en DNS y en el certificado.

05 Seleccionar VPN Client. Si aparece External Auth, establecer un External Auth Username específico y correcto para la persona destinataria.

06 Pulsar View; revisar tipo de VPN, destino, identificadores, opciones de autenticación, certificados, redes y propuestas. No confundir el XML visible con una autorización para difundirlo.

07 Si la revisión resulta satisfactoria, pulsar Download y guardar el archivo en ubicación administrativa protegida.

08 Distribuir el perfil a la persona o dispositivo autorizado y registrar la entrega, versión, responsable y posible revocación.

09 Instalar en un dispositivo piloto, conectar desde una red externa real y comprobar Status → IPsec, DNS, rutas, reglas y acceso únicamente a servicios aprobados.

57.10. Revisión del archivo .mobileconfig antes de distribuir

La opción View permite inspeccionar el perfil en formato estructurado. Según la autenticación elegida, pueden aparecer claves de payload, nombres de servidores, identificadores, parámetros IKE, referencias a certificados u otros elementos. La estructura puede cambiar con el exportador y la plataforma Apple; no se deben suponer campos XML no observados.

Revisar	Motivo	Criterio de aceptación
Servidor e identificador remoto	Evitar conexiones a destinos erróneos o identidades distintas.	Coincide con DNS y SAN del certificado.
Propuestas IKE y CHILD_SA	Evitar negociar suites inesperadas o incompatibles.	Son compatibles con la política aprobada.

Revisar	Motivo	Criterio de aceptación
Método de autenticación	Prevenir perfiles con mecanismos distintos a los planificados.	Coincide con EAP / certificados configurados.
Certificados y claves	Pueden incorporar datos privados o material de autenticación.	Solo material necesario, distribución protegida.
Redes y DNS	Determinan acceso y resolución interna.	Sin fugas inesperadas ni redes no autorizadas.
Identificadores del perfil	Permiten gestionar versiones y sustituciones.	Consistentes, sin revelar la infraestructura real.

57.11. Instalación en iPhone y iPad

01 Descargar el perfil desde un canal controlado en el dispositivo autorizado. Verificar remitente, nombre y contenido antes de abrirlo.

02 Abrir Ajustes. En versiones actuales se muestra «Perfil descargado» cuando hay uno pendiente de instalación.

03 Pulsar «Perfil descargado», revisar los detalles del perfil y seleccionar Instalar. El sistema puede solicitar código o aprobación según políticas del equipo.

04 Comprobar en Ajustes → General → VPN y gestión de dispositivos la presencia del perfil y de la conexión VPN.

05 Conectar desde una red externa (no la LAN de destino), autenticar al usuario o certificado cuando sea solicitado y confirmar que se accede solamente a las redes permitidas.

06 Anotar en inventario el estado de la prueba. Retirar perfiles obsoletos a través de la gestión autorizada; en dispositivos administrados puede intervenir MDM.

Apple advierte que, al descargar un perfil manualmente, puede ser necesario instalarlo desde Ajustes y que los perfiles pendientes no permanecen indefinidamente. La ruta exacta puede variar entre versiones de iOS/iPadOS y políticas de administración.

57.12. Instalación en macOS y despliegue corporativo

01 Recibir el perfil mediante un mecanismo corporativo autenticado y comprobar su procedencia.

02 Abrir Ajustes del Sistema → General → Gestión de dispositivos (la denominación puede variar), localizar el perfil descargado y revisarlo.

03 Autorizar la instalación únicamente tras examinar los ajustes que incorpora, especialmente la VPN y los certificados.

04 Comprobar que aparece la conexión en los ajustes de red/VPN, probar autenticación y resolución de nombres.

05 En equipos gestionados, preferir una distribución centralizada con MDM, trazabilidad de asignación y proceso de retirada.

Un perfil gestionado puede tener restricciones de eliminación. El procedimiento de baja del dispositivo deberá contemplar retirar credenciales, perfiles y autorizaciones según la política de la organización.

57.13. Escenario empresarial A: acceso remoto individual con usuario y contraseña

Una organización desea que un grupo autorizado de usuarios Apple acceda a un portal interno y a una aplicación de gestión. Se configura IKEv2/EAP con certificado servidor correcto y un pool de clientes distinto a las LAN y a las redes domésticas habituales. Cada perfil contiene un nombre de cuenta específico, mientras la autorización se mantiene en el origen de autenticación. Se habilitan únicamente el portal y la aplicación mediante reglas IPsec.

Validación: el perfil se instala, aparece la entrada VPN, se establece IKE_SA, se establece CHILD_SA, el DNS interno responde y únicamente los destinos autorizados son accesibles. La exportación, por sí sola, no valida ninguno de estos pasos.

57.14. Escenario empresarial B: EAP-TLS y certificados personales

Para un grupo reducido de administradores se propone autenticación mediante certificado de cliente, con control de emisión, caducidad y revocación. El exportador selecciona la identidad TLS conforme a la CA asociada con la Mobile Phase 1. Cada perfil se entrega individualmente y se revoca el certificado cuando cambia el dispositivo o termina la autorización.

Es importante separar el certificado de servidor de los certificados de los clientes. El servidor prueba su identidad y el cliente acredita la suya. La pérdida de un dispositivo exige revisar el perfil, la credencial y cualquier copia del material exportado.

57.15. Escenario empresarial C: DNS corporativo y acceso limitado a subredes

Un equipo de trabajo necesita resolver nombres de una zona privada y llegar a dos servicios internos, sin convertir el firewall en salida universal a Internet. El administrador define las redes permitidas, el comportamiento DNS correspondiente y las reglas adecuadas. El perfil debe reflejar una configuración compatible con la política de split tunnel, evitando que la conectividad dependa de rutas inexistentes.

Pruebas: consulta DNS corporativa, conexión a los servicios aprobados, no acceso a redes ajenas a la política y recuperación correcta tras cambios de Wi-Fi a red móvil. La configuración efectiva depende de las capacidades de IPsec, el perfil Apple y la red del dispositivo.

57.16. Validación y supervisión después de la instalación



Figura 57.3. Árbol de comprobación por etapas: el éxito de la generación no garantiza acceso de aplicación.

Dónde verificar	Qué buscar	Interpretación
Status → IPsec	IKE SA establecida, CHILD SA creada y contadores.	Negociación y actividad de la VPN.
Status → System Logs → IPsec	Certificados, EAP, propuestas, identidad y errores de negociación.	Causa precisa de rechazo o incompatibilidad.
Status → System Logs → Firewall	Bloqueos en puertos IKE o tráfico tras descifrado.	Reglas o acceso de datos.
Cliente Apple	Conexión, nombre DNS, acceso a servicio autorizado.	Experiencia final desde una red externa.
Infraestructura DNS	Registro, resolución, certificado, tiempos.	Coherencia del extremo y nombres internos.

Los mensajes «IKE_SA ... established» y «CHILD_SA ... established» permiten distinguir la negociación de control de la asociación de datos; la presencia de ambas no sustituye la comprobación de firewall, rutas y servicios.

57.17. Incidencias habituales y resolución segura

Problema	Causas probables	Respuesta recomendada
Error «No Mobile Phase 1»	No hay Phase 1 móvil adecuada.	Crear/activar P1 móvil conforme al diseño y revisar P2.

Problema	Causas probables	Respuesta recomendada
Perfil sin servidor	SAN ausente o falta certificado correcto.	Revisar identidad del certificado; no inventar un hostname.
Advertencia de certificado	SAN/CA/cadena/fecha incorrectos.	Corregir certificado; nunca desactivar verificación sin análisis.
Autenticación EAP fallida	Usuario inválido, RADIUS indisponible, método distinto.	Validar logs IPsec y servidor de identidades.
No hay conexión IKE	UDP 500/4500 filtrados, WAN o NAT incorrectos.	Capturar tráfico de llegada y revisar reglas/enrutamiento.
Conecta pero no accede	Phase 2, firewall IPsec, rutas o DNS.	Contrastar CHILD_SA, logs y reglas de acceso.
Falla al renovar	Propuestas, PFS, caducidades o movilidad.	Revisar negociación/rekey y propuestas del par.
Perfil antiguo	Certificado, gateway o propuesta cambiados.	Regenerar perfil, redistribuir y retirar anterior.

57.18. Seguridad y ciclo de vida del perfil

El archivo de configuración no debe considerarse inocuo: puede transportar direcciones, nombres de red, parámetros de autenticación, certificados o configuraciones que el sistema aceptará como gestionadas. Su protección debe adaptarse al contenido real inspeccionado con View. Se recomienda clasificar el perfil como material interno de configuración, limitar el acceso a cada identidad y evitar repositorios públicos o adjuntos reenviables.

01 Diseñar el túnel y sus permisos antes de exportar; no adaptar el firewall a conveniencia de un cliente no autorizado.

02 Usar IKEv2 y criptografía moderna compatible; evitar suites obsoletas salvo excepciones justificadas.

03 Validar la identidad del servidor mediante DNS y SAN, con certificados renovados y revocación controlada.

04 Emplear credenciales personales y, cuando el diseño lo permita, autenticación fuerte gestionada centralmente.

05 Generar un perfil por identidad cuando contenga material individual, conservar un inventario de versiones y entrega.

06 Eliminar archivos temporales, limitar copias e implantar procedimiento de revocación y baja de dispositivos.

07 Probar tras cambios de hostname, certificado, algoritmo, P1/P2, rutas o DNS: un perfil previamente válido puede quedar inutilizado.

57.19. Lista de comprobación previa a la puesta en servicio

Verificación	Resultado a registrar
Paquete IPsec Export presente y accesible.	Instalado / versión comprobada
Existe Mobile Phase 1 y Phase 2 compatibles.	Parámetros revisados
Nombre DNS de servidor coincide con SAN del certificado.	DNS y SAN validados
Cuenta o certificado del cliente está autorizado.	Identidad comprobada
VPN Name no contiene nombres privados innecesarios.	Etiqueta neutra
View revisado antes de Download.	Validación documental
Perfil instalado en un equipo piloto.	Instalación confirmada
IKE_SA / CHILD_SA y reglas verificadas.	Conectividad y alcance correctos
Distribución, revocación y versión documentadas.	Trazabilidad aprobada

57.20. Glosario técnico esencial

Término	Definición contextual
SAN	Subject Alternative Name: identidades que valida el certificado del servidor.
FQDN	Nombre de dominio completamente cualificado del extremo VPN.
IKE_SA	Asociación de seguridad de la negociación IKE.
CHILD_SA	Asociación que protege el tráfico de datos bajo IPsec.
EAP	Marco de autenticación ampliable utilizado en varios modos de acceso móvil.
EAP-TLS	Autenticación EAP basada en certificados TLS.
EAP-RADIUS	Autenticación EAP respaldada por un servidor RADIUS según el método configurado.
MDM	Gestión de dispositivos móviles para despliegue y retirada administrada de perfiles.
NAT-T	Encapsulación de ESP en UDP/4500 en escenarios con NAT.
Payload	Bloque de configuración contenido en un perfil Apple.

57.21. Documentación oficial y referencias

Fuentes consultadas para verificar la funcionalidad y las prácticas de instalación. La interfaz descrita corresponde a la pantalla examinada; las recomendaciones de diseño y diagnóstico se fundamentan en las guías oficiales indicadas a continuación.

Netgate — IPsec Export Package — https://docs.netgate.com/pfsense/en/latest/packages/ipsec-export.html

Netgate — Mobile Clients — https://docs.netgate.com/pfsense/en/latest/vpn/ipsec/mobile-clients.html

Netgate — IPsec remoto con IKEv2 y EAP-MSCHAPv2 — https://docs.netgate.com/pfsense/en/latest/recipes/ipsec-mobile-ikev2-eap-mschapv2.html

Netgate — Clientes IKEv2 en iOS — https://docs.netgate.com/pfsense/en/latest/recipes/ipsec-mobile-ikev2-client-ios.html

Netgate — Clientes IKEv2 en macOS — https://docs.netgate.com/pfsense/en/latest/recipes/ipsec-mobile-ikev2-client-macos.html

Netgate — Troubleshooting IPsec Connections — https://docs.netgate.com/pfsense/en/latest/troubleshooting/ipsec-connections.html

Netgate — Troubleshooting IPsec Logs — https://docs.netgate.com/pfsense/en/latest/troubleshooting/ipsec-logs.html

Netgate — IPsec Status — https://docs.netgate.com/pfsense/en/latest/monitoring/status/ipsec.html

Apple — Instalar perfil en iPhone y iPad — https://support.apple.com/es-es/102400

Apple — Instalar perfiles en macOS — https://support.apple.com/guide/mac-help/configuration-profiles-standardize-settings-mh35561/mac

Apple — Configuración IKEv2 para dispositivos gestionados — https://support.apple.com/guide/deployment/ikev2-vpn-declarative-configuration-depdeca2fabe/web

Nota técnica editorial: los ejemplos de identidad (vpn.example.com), nombres de red y etiquetas son completamente ficticios. Ningún dato de una infraestructura concreta se utiliza en diagramas, tablas o metadatos.

58 VPN → IPsec Export: Windows PowerShell

IKEv2 · generación de ZIP y scripts · certificados · rutas · validación y despliegue seguro

Este capítulo explica cómo trasladar a un equipo Windows una configuración de acceso remoto IPsec ya preparada en pfSense Plus. El asistente genera un script PowerShell y los certificados necesarios, pero el despliegue solo es correcto cuando coinciden identidad del servidor, propuestas IKE/ESP, autenticación, rutas y reglas de acceso. El objetivo es entender cada decisión, no ejecutar un ZIP sin revisarlo.



Figura 58.1. Secuencia de dependencias técnicas entre la configuración móvil IPsec, el exportador y Windows. Diseño original con ejemplos neutros.

58.1. Objeto, alcance, ubicación y compatibilidad

Ruta de administración: VPN → IPsec → IPsec Export: Windows PowerShell. El mismo módulo se presenta desde la entrada VPN → IPsec Export: Windows. La pantalla integra dos pestañas: «Apple Profile» y «Windows PowerShell», con esta última seleccionada. Es una utilidad de exportación de clientes, no un nuevo servidor VPN ni una alternativa a la configuración IPsec del firewall.

Netgate documenta el paquete «IPsec Export» / «ipsec-profile-wizard» como una capacidad de pfSense Plus; si no está instalado se agrega desde Package Manager. La disponibilidad de la página depende de que el paquete esté presente y sea compatible. Las funciones y los parámetros exactos pueden variar según la versión instalada y las opciones de autenticación definidas.

ALCANCE DE VERSIÓN Las opciones de este módulo pueden variar entre versiones y configuraciones. Algunos controles, como TLS User Certificate, solo se muestran cuando corresponde a la autenticación seleccionada.

58.2. Qué produce el exportador y qué no garantiza

La aplicación detecta propuestas compatibles entre las entradas Mobile Phase 1 y Mobile Phase 2, compone una configuración de cliente Windows y prepara un archivo ZIP. El ZIP incluye un script PowerShell y los certificados que requiera el mecanismo de autenticación; la composición concreta depende de la configuración del servidor. «View» permite inspeccionar el script antes de descargarlo.

Componente	Responsabilidad	Límite importante
Configuración del firewall	Define endpoint, Phase 1/2, certificados, pool, reglas y alcance de red.	El exportador no sustituye su preparación.
Script PowerShell	Crea y ajusta parámetros de la VPN nativa de Windows.	No debe ejecutarse sin revisión.
Certificados exportados	Aportan material de confianza y, si procede, credencial de cliente.	La presencia de certificados privados exige custodia estricta.
Conexión Windows	Negocia IKEv2 y crea rutas y estado de sesión según lo configurado.	Instalar el perfil no prueba que el túnel conecte.

58.3. Inventario del formulario y sus controles

Control o elemento visible	Función y comportamiento
Mensaje de error	«There is no Mobile Phase 1 in the IPsec configuration»: falta una Phase 1 móvil detectable por el exportador.
Apple Profile / Windows PowerShell	Pestañas del exportador. La segunda produce la configuración Windows.

Control o elemento visible	Función y comportamiento
Bloque IKEv2 Export Settings	Agrupa opciones de nombre y extremo remoto.
VPN Name	Nombre que mostrará Windows; también forma parte del nombre del archivo ZIP.
Server Address	Selector construido a partir de entradas SAN del certificado de servidor.
Custom Hostname	FQDN alternativo cuando Server Address toma la opción Custom Hostname.
Download	Descarga el ZIP con script y certificados, siempre sujeto a que la exportación sea válida.
View	Muestra el contenido del script para comprobarlo antes del despliegue.
Panel de información inferior	Describe importación, políticas PowerShell, privilegios, split tunneling y selección de parámetros.

58.4. Error: «There is no Mobile Phase 1 in the IPsec configuration»

El aviso rojo indica que la utilidad no encuentra una Phase 1 de tipo móvil adecuada. No es una prueba de fallo de la instalación Windows, de la cuenta de usuario o del certificado CA. Por tanto, los botones de exportación no deben usarse como vía para eludir la condición. La solución exige comprobar primero el servicio IPsec móvil, sus entradas Phase 1 y Phase 2 y la compatibilidad del modo de autenticación.

Comprobación	Ruta	Criterio de aceptación
Soporte móvil	VPN → IPsec → Mobile Clients	El soporte está habilitado conforme al diseño.
Phase 1 móvil	VPN → IPsec → Tunnels → Add P1 / Edit	Existe una entrada móvil habilitada y compatible con Windows.
Phase 2 móvil	Tunnels → Phase 2 asociadas	Selectores, pool, cifrado y redes son apropiados.
Estado del servicio	Status → Services / Status → IPsec	IPsec disponible para negociar las SAs.
Exportación	VPN → IPsec Export: Windows	Desaparece el error; «View» genera un script revisable.

PROTECCIÓN DE PRODUCCIÓN No habilitar o reconfigurar Phase 1/Phase 2 únicamente para que desaparezca el aviso. Cada cambio puede afectar a los usuarios conectados, al cifrado aceptado y a la exposición de servicios. Respaldar, revisar y aplicar en una ventana autorizada.

58.5. Requisitos previos de una VPN IKEv2 para Windows

01 Usar una edición de pfSense Plus compatible y confirmar que el paquete IPsec Export está instalado y actualizado mediante la administración de paquetes.

02 Configurar IPsec Mobile Clients, una Phase 1 móvil IKEv2 y las Phase 2 correspondientes; confirmar autenticación EAP compatible o EAP-TLS, según la política del entorno.

03 Disponer de un certificado de servidor válido, con nombre de acceso en SAN y una cadena de confianza verificable por Windows; revisar vigencia y revocación.

04 Publicar un FQDN resoluble a la dirección de servicio autorizada; comprobar acceso a UDP/500 y UDP/4500 y el escenario con NAT-T.

05 Definir pool de direcciones sin solapamientos, redes accesibles, reglas IPsec/firewall, servicios DNS internos y retorno del tráfico.

06 Preparar un dispositivo Windows de prueba con privilegios justificados, inventario de certificados de confianza y plan de retirada del perfil.

07 Comprobar propuestas IKE y CHILD SA admitidas por Windows y por el servidor; Netgate utiliza la primera combinación exportable encontrada.

58.6. Fundamento de la identidad: DNS, SAN y certificado

El campo «Server Address» se alimenta del Subject Alternative Name (SAN) del certificado del servidor. El nombre utilizado por Windows debe resolver y figurar en el SAN; además, la cadena de confianza debe

validarse. El CN tradicional no reemplaza al SAN cuando el cliente exige validar por SAN. Una IP literal solo resulta válida si las condiciones de la implementación y el certificado permiten verificarla correctamente.

Para enseñar la relación se utiliza únicamente el dominio de documentación «vpn.example.com». Su función es ilustrar que un nombre DNS publicado, el identificador al que conecta el cliente y el SAN de la identidad presentada por el servidor deben ser coherentes. No se emplean dominios, IP, usuarios ni hostnames de instalaciones reales.

Punto a revisar	Ejemplo neutro	Qué debe ocurrir
Nombre solicitado	vpn.example.com	Coincide con uno de los SAN admitidos.
DNS público	vpn.example.com → IP del servicio	Resuelve desde una red externa autorizada.
Certificado de servidor	SAN DNS:vpn.example.com	Válido, no expirado y emitido por CA confiable.
CA en Windows	Almacén de raíces/intermedias correspondiente	La cadena verifica sin importar raíces desconocidas.
Endpoint NAT/WAN	Publicación aprobada	Los paquetes IKE/NAT-T llegan al firewall.

NO USAR CUSTOM HOSTNAME COMO ATAJO Cambiar el nombre de destino no soluciona una falta de SAN o un certificado inválido. La identidad criptográfica debe seguir siendo verificable.

58.7. VPN Name: nombre del perfil y trazabilidad

Es la etiqueta con la que se identificará la conexión en la lista de VPN de Windows y sirve para crear el nombre del archivo exportado. Conviene un nombre corto y estable, por ejemplo «Acceso remoto corporativo»; no es una credencial y no constituye una comprobación de identidad. Puede ayudar a documentar la versión del despliegue, pero no debe divulgar información interna que el usuario no necesite conocer.

Si ya existe un perfil Windows con el mismo nombre, hay que revisar el script para determinar si intenta modificarlo, recrearlo o produce error. No se deben presuponer comportamientos de reemplazo sin leer las operaciones efectivamente generadas.

58.8. Server Address: selección del servidor

Muestra las direcciones seleccionables procedentes de SAN del certificado elegido para el servidor. Esta dependencia evita introducir inadvertidamente un extremo que Windows no pueda autenticar. La selección requiere coherencia con DNS, rutas WAN, certificados y configuración Phase 1; un servidor que solo resuelve internamente no sirve para usuarios externos si no hay una resolución accesible al cliente.

58.9. Custom Hostname: cuándo procede

Se utiliza al elegir «Custom Hostname» en «Server Address». Permite indicar el FQDN al que se conectará Windows en lugar de una de las opciones mostradas. Esta libertad resulta útil cuando existe un alias publicado o se necesita una denominación estable, pero no exime de que el nombre conste en SAN y resuelva correctamente.

Después de cambios de DNS, IP pública, certificado o balanceo de acceso, hay que regenerar y verificar el material de exportación si depende de dichos valores. En Multi-WAN, un alias de conexión sin control de retorno y asociación de certificados puede producir cortes intermitentes.

58.10. Campo condicional TLS User Certificate

Netgate documenta que, cuando la Mobile Phase 1 exige un certificado de usuario (por ejemplo EAP-TLS), aparece el selector «TLS User Certificate». Se trata de un campo condicional, no visible en todas las configuraciones. Permite elegir el certificado de usuario que se incorporará cuando proceda; su disponibilidad depende de la autenticación configurada, certificados existentes y de la versión de la utilidad.

TRATAMIENTO DE MATERIAL PERSONAL Si un ZIP incluye una clave privada de cliente o material exportable, debe distribuirse cifrado, solo al destinatario autorizado, con medidas de inventario y revocación. La presencia y el formato deben comprobarse en el archivo real; no se suponen.

58.11. View y Download: secuencia correcta de exportación

El botón «View» permite examinar el script generado y detectar operaciones no autorizadas antes de descargarlo. «Download» obtiene un ZIP que contiene el script y archivos de certificado requeridos. La estructura y los nombres internos del ZIP no están fijados por la captura y pueden variar; deben inventariarse tras extraerlo en un entorno de confianza.



Figura 58.2. Separación entre script, certificados y perfil instalado en Windows. Los archivos concretos dependen del escenario de autenticación.

01 Corregir el error de ausencia de Mobile Phase 1 sin cambios improvisados en producción.

02 Escribir un nombre VPN genérico y seleccionar el servidor cuyo SAN y DNS son correctos.

03 Usar «Custom Hostname» solo cuando el nombre personalizado esté validado criptográficamente.

04 Si aparece «TLS User Certificate», elegir la identidad autorizada de la persona destinataria.

05 Pulsar «View», leer el script completo y revisar cmdlets, nombres de perfil, destinos y almacenes de certificados.

06 Una vez aprobado el contenido, pulsar «Download» y registrar la procedencia del ZIP y su integridad.

07 Descargar por un canal seguro y llevarlo a un equipo Windows de pruebas antes de desplegar masivamente.

58.12. Qué revisar dentro del script PowerShell

El script es código operativo: puede crear una conexión, importar autoridades certificadoras, establecer autenticación, introducir parámetros IPsec, habilitar split tunneling y crear rutas. No debe describirse como un documento pasivo. Microsoft expone estas operaciones mediante el módulo VpnClient, con cmdlets como Add-VpnConnection, Set-VpnConnectionIPsecConfiguration, Set-VpnConnection y Add-VpnConnectionRoute.

Bloque funcional	Preguntas de revisión	Riesgo a evitar
Perfil VPN	¿Nombre, servidor y tipo de túnel son los aprobados?	Sobrescritura o conexión al endpoint equivocado.
Autenticación	¿EAP y certificados corresponden al usuario previsto?	Identidad mal vinculada o material privado distribuido.
Algoritmos IKEv2/ESP	¿DH, integridad, cifrado y PFS coinciden con Phase 1/2?	NO_PROPOSAL_CHOSEN; fallos tras renovación.
Importación de CA	¿Qué certificado se instala y en qué almacén?	Ampliación indebida de confianza.
Rutas y split tunnel	¿Cuáles son los prefijos concretos?	Desvío de tráfico o acceso no deseado.
Privilegios y cambios	¿Necesita permisos administrativos? ¿Es reversible?	Cambio en todos los usuarios o política local.

58.13. Cómo ejecutar de forma segura en Windows

Extraer el ZIP en una carpeta controlada, leer todos los comandos y confirmar el origen de cada certificado. Trabajar primero sobre un equipo de laboratorio o piloto, guardar el estado anterior y emplear los mínimos

privilegios posibles; ciertas importaciones de CA requieren elevación. Ejecutar únicamente el script aprobado por la organización.

01 Revisar la integridad del ZIP y el inventario de ficheros. Documentar el hash SHA-256 obtenido localmente y el origen de distribución.

02 Visualizar el script en un editor de texto y cotejarlo con «View». Revisar si incluye parámetros o secretos destinados a otro usuario.

03 Comprobar políticas efectivas PowerShell y restricciones de GPO antes de intentar ejecutarlo; evitar relajar las restricciones del equipo de forma global.

04 Identificar operaciones de importación de certificados: verificar huellas digitales, propósito y almacén de destino; aprobar solo CA reconocidas.

05 Ejecutar en una consola del nivel de permisos estrictamente necesario y registrar la salida, sin guardar contraseñas ni tokens en logs.

06 Comprobar el perfil VPN, el almacén de certificados y las rutas agregadas; finalmente conectar desde una red externa de pruebas.

POLÍTICAS POWERSHELL Las directivas de ejecución no son una barrera de seguridad completa ni un certificado de confianza del script. Microsoft distingue ámbitos Process, CurrentUser y LocalMachine y precedencia de GPO; no se recomienda un cambio permanente a Bypass.

58.14. Comprobaciones reproducibles en PowerShell

Los siguientes comandos son de lectura o diagnóstico y emplean nombres ficticios. La sintaxis debe adaptarse al sistema concreto. Los comandos que alteren certificados, perfiles o rutas deben aprobarse aparte, tras revisar el script exportado.

```
Get-ExecutionPolicy -List
```

```
Get-VpnConnection -Name "Acceso remoto corporativo"
```

```
Get-VpnConnectionRoute -ConnectionName "Acceso remoto corporativo"
```

```
Resolve-DnsName vpn.example.com
```

```
Get-ChildItem Cert:\LocalMachine\Root | Select-Object Subject, Thumbprint, NotAfter
```

Para verificar políticas IKEv2 y parámetros certificados puede consultarse la ayuda de Get-VpnConnection y la referencia Set-VpnConnectionIPsecConfiguration; la capacidad de introspección depende del sistema. Evitar pruebas UDP con Test-NetConnection -Port 500, que comprueba TCP y no verifica el intercambio IKE. Para UDP 500/4500, usar captura de paquetes, eventos y estado IPsec.

58.15. Split tunneling, Network List y rutas móviles

La información de ayuda del módulo advierte de un comportamiento concreto: si en VPN → IPsec → Mobile Clients se activa «Network List», el script puede configurar split tunneling y añadir rutas para las redes declaradas en las entradas móviles de Phase 2. Sin esta condición, el comportamiento del cliente debe verificarse expresamente y no se debe asumir que todas las subredes son accesibles.

Decisión	Consecuencia	Validación
Split tunnel activado	Solo prefijos específicos se envían a la VPN; el resto puede usar salida local.	Get-VpnConnectionRoute y tabla de rutas; pruebas por red.
Full tunnel configurado	El tráfico definido por el perfil viaja por la VPN, condicionado por reglas/NAT y diseño.	Ruta por defecto, DNS, salida a Internet y protección de fuga.
Phase 2 sin red correcta	El cliente puede conectar sin acceso al destino previsto.	Selectores Phase 2, rutas Windows y reglas IPsec.
Red solapada con LAN doméstica	Puede elegirse ruta local y no alcanzar servicios remotos.	Comparar prefijos local/remoto y métricas.

LÍMITE DE SPLIT TUNNELING La opción de rutas no constituye un control de autorización. Aunque Windows conozca una ruta, la red de destino debe quedar protegida por reglas, autenticación y segmentación del firewall.

58.16. Algoritmos y elección de la primera propuesta compatible

Netgate especifica que la utilidad examina las configuraciones Mobile Phase 1 y Mobile Phase 2, selecciona la primera combinación compatible y la traduce a parámetros admitidos por Windows. Si el orden de propuestas no refleja la política criptográfica aprobada, el script debe revisarse y ajustarse o bien corregirse la configuración de origen mediante procedimiento autorizado.

Entre los parámetros configurables del cliente Windows mediante Set-VpnConnectionIPsecConfiguration figuran algoritmos de cifrado e integridad, grupo Diffie–Hellman y PFS. Los valores aceptados dependen de la versión de Windows y del módulo; no es recomendable copiar combinaciones antiguas de una guía sin comprobar la interoperabilidad y la política criptográfica vigente.

58.17. Certificados: confianza del servidor y certificado de usuario

Importar el certificado de una CA implica confiar en los certificados que esa autoridad emita conforme a las políticas y restricciones. En EAP-TLS, además, puede requerirse un certificado personal de cliente con clave privada, normalmente almacenada con controles de acceso y sujeto a revocación. La pertenencia a una CA no demuestra por sí sola que una identidad individual esté autorizada: siguen aplicando validación EAP, grupos y restricciones del servidor.

Elemento	Uso típico	Control recomendado
CA raíz/intermedia	Validación del certificado del servidor.	Confirmar emisor, huella, vigencia y ámbito de confianza.
Certificado de servidor	Identifica al servidor IPsec y su nombre DNS.	Revisar SAN, EKU/política según la autenticación, cadena y revocación.
Certificado personal cliente	Autenticación EAP-TLS, si se utiliza.	Custodia individual, protección de clave privada y revocación.
Contraseña de EAP	Autenticación según EAP/RADIUS, si aplica.	Evitar contraseñas en claro y reutilización; MFA según arquitectura.

58.18. Arquitectura de implantación empresarial: tres escenarios

Escenario A — portátil corporativo con identidad EAP/RADIUS. Una persona autorizada recibe un paquete revisado con la CA aprobada, instala el perfil VPN nativo y autentica sus credenciales conforme a la política. La conectividad se limita a servicios internos autorizados; el administrador audita asignación de direcciones, acceso a DNS y registro de conexión.

Escenario B — equipos gestionados con EAP-TLS. Se emiten certificados personales para identidades únicas, se controla la exportabilidad de claves privadas y se incorpora el certificado autorizado a cada equipo. El paquete se distribuye por un medio de gestión corporativa y se establece revocación para bajas y pérdida de dispositivos.

Escenario C — personal remoto con subredes seleccionadas. Se habilita Network List y se exporta un script con rutas a redes declaradas en Mobile Phase 2; se validan prefijos con Get-VpnConnectionRoute y se limita el acceso mediante reglas IPsec por origen/destino. Si el hogar y la red de empresa solapan prefijos, no se considera resuelto por el mero hecho de ver el estado «Connected».

58.19. Prueba de aceptación funcional por capas

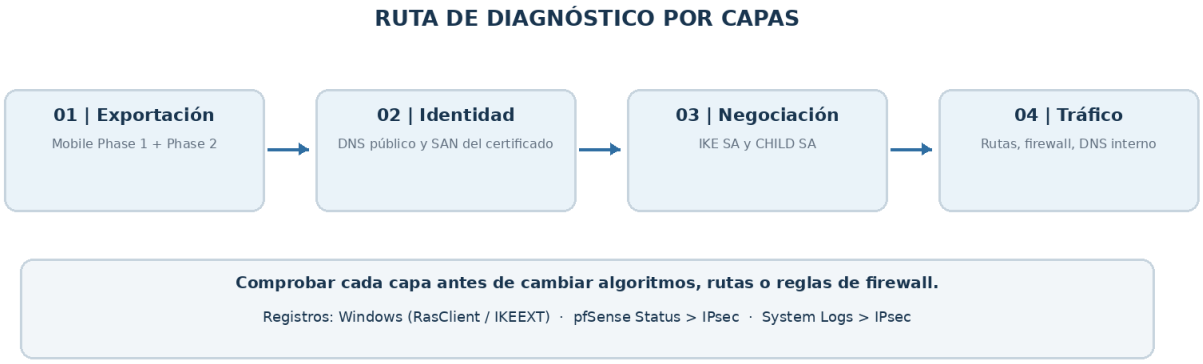


Figura 58.3. Método de diagnóstico desde la exportación hasta el tráfico real. Elaboración original.

01 Exportación: confirmar que no aparece el aviso Mobile Phase 1 y que «View» ofrece un script sin errores.

02 Identidad: resolver el FQDN desde una conexión externa, verificar SAN, fechas, cadena de CA y respuesta correcta del extremo.

03 Instalación: registrar el perfil VPN y certificados en sus almacenes esperados; confirmar que no hay materiales de otro usuario.

04 Negociación: observar «IKE_SA … established» y «CHILD_SA … established» en los registros del firewall si la sesión se completa.

05 Tráfico: desde Windows, revisar rutas, DNS y acceso a un recurso de prueba explícitamente permitido.

06 Revocación y retirada: ensayar suspensión del usuario/certificado, retirada del perfil y limpieza de material temporal conforme a política.

58.20. Estado y registros de pfSense y Windows

En pfSense el panel Status → IPsec permite revisar túneles y asociaciones de seguridad, mientras que Status → System Logs → IPsec muestra mensajes de strongSwan. La presencia de una IKE SA prueba el intercambio de fase IKE; una CHILD SA establecida confirma la negociación de la asociación de tráfico, no la autorización de todas las aplicaciones. Las reglas IPsec, rutas y DNS deben validarse aparte.

En Windows se puede examinar el registro de eventos relacionado con VPN/RasClient e IKEEXT, las propiedades del perfil y el estado de la interfaz VPN. En problemas intermitentes deben registrarse fecha, origen de la prueba, código de error y correlación con los eventos del firewall; no enviar registros sin retirar previamente información de usuarios, direcciones y certificados.

58.21. Tabla de diagnóstico de incidencias

Síntoma	Causa probable	Respuesta técnica
No existe Mobile Phase 1	No hay entrada móvil disponible o habilitada.	Ver Mobile Clients y Tunnels; comprobar IKEv2 y Phase 2.
Server Address vacío	No hay SAN utilizable o no hay certificado válido seleccionado.	Revisar certificado de servidor, SAN y selección Phase 1.
ZIP no genera perfil	No existe propuesta exportable o falta configuración requerida.	Leer el aviso del exportador; comprobar propuestas y autenticación.
PowerShell deniega script	Política de ejecución o GPO.	Ver Get-ExecutionPolicy -List; consultar al administrador; no desactivar GPO.
Importación CA fallida	Falta elevación, formato incompatible o almacén incorrecto.	Examinar certificado y permisos; evitar importar en raíces por ensayo-error.
Nombre no coincide	FQDN no presente en SAN o DNS incorrecto.	Corregir DNS y certificado; volver a exportar.

Síntoma	Causa probable	Respuesta técnica
IKE no inicia	Filtrado UDP/500 o 4500, NAT-T, endpoint inaccesible.	Capturar tráfico, revisar reglas y ruta de retorno.
NO_PROPOSAL_CHOSEN	Transformaciones IKE/ESP no compatibles.	Comparar proposals del cliente con Phase 1/2 y logs.
IKE SA sin CHILD SA	Fase 2/selectores, PFS o autenticación de tráfico.	Revisar logs CHILD SA y parámetros Phase 2.
Conecta sin acceder	Rutas, DNS interno, reglas IPsec o retorno.	Inspeccionar rutas Windows, filtrado, NAT y servicios.
Falla al renovar	Diferencia PFS/rekey o interrupciones de red.	Comparar configuración de renovación y registros en ambas partes.

58.22. Seguridad operativa y distribución del paquete

El ZIP debe tratarse como un artefacto sensible: puede describir infraestructura, CA internas y, bajo determinadas configuraciones, incluir credenciales de certificado cliente. Conviene generar los paquetes de manera individual cuando contengan identidades personales, aplicar control de acceso, minimizar almacenamiento, usar un canal cifrado de entrega y contar con procedimiento de baja y revocación.

No incluir contraseñas, claves privadas ni nombres identificativos en tickets, correos de soporte sin protección, repositorios o ejemplos públicos. Revisar certificados antes de modificar almacenes raíz de confianza. Conservar solo las evidencias necesarias y documentar qué perfil y qué certificados fueron instalados, por quién y con qué aprobación.

ADVERTENCIA DE ADMINISTRACIÓN La ejecución del script puede modificar el perfil de VPN y los certificados del equipo. Si el script solicita elevación, comprender primero la operación privilegiada; no convertir la ejecución como administrador en un procedimiento automático.

58.23. Mantenimiento, renovación y retirada

Al sustituir un certificado de servidor, modificar el FQDN o cambiar las propuestas Phase 1/2, la configuración exportada puede quedar obsoleta. Planificar nuevas exportaciones, pruebas piloto y distribución controlada. Comprobar expiración de los certificados de usuario y fechas de renovación de perfiles; preparar una retirada para dispositivos perdidos o empleados que dejan de necesitar acceso.

Las rutas creadas por el script pueden persistir como parte del perfil VPN. Antes de desinstalar o recrear una VPN, conservar un inventario de sus rutas, su nombre y cualquier raíz CA instalada exclusivamente para ese servicio. La eliminación de una CA raíz podría afectar a otros usos de la estación; no ejecutar una limpieza indiscriminada.

58.24. Lista de comprobación antes de autorizar el despliegue

Control final	Evidencia que se debe conservar
Mobile Phase 1 y Phase 2 compatibles	Captura o registro redactado del diseño aprobado.
FQDN y SAN del certificado verificados	Resultado de DNS, vigencia y validación de cadena.
Propuestas IKEv2/ESP revisadas	Selección esperada y resultado de la vista previa.
Script, ZIP y certificados inspeccionados	Inventario de archivos, hash y aprobación.
Políticas PowerShell y permisos validados	Resultado Get-ExecutionPolicy y nivel de acceso autorizado.
Rutas y split tunneling justificados	Subredes permitidas y pruebas de aplicación.
Conexión y tráfico verificados	Registros IKE/CHILD SA y prueba a recurso autorizado.
Retirada y revocación preparadas	Responsable, vigencia y procedimiento de retirada.

58.25. Glosario esencial

Término	Definición operativa
IKEv2	Protocolo de negociación de identidad, claves y asociaciones IPsec.
IKE SA	Asociación de seguridad que protege la negociación IKE.
CHILD SA	Asociación que protege el tráfico de datos IPsec.
EAP	Familia de métodos de autenticación extensible; admite varios mecanismos.
EAP-TLS	Autenticación EAP basada en certificados de cliente y servidor.
SAN	Subject Alternative Name; nombres identificativos certificados del servidor.
PFS	Perfect Forward Secrecy, intercambio de clave adicional según propuesta.
Split tunneling	Enrutamiento selectivo de destinos a través de la VPN.
CA	Autoridad certificadora utilizada como raíz de confianza de una cadena.
NAT-T	Encapsulación IPsec sobre UDP/4500 para atravesar NAT cuando procede.
Execution Policy	Política de PowerShell que determina condiciones de carga de scripts, no un control de confianza integral.

58.26. Plan de pruebas piloto y criterios de reversión

Antes de distribuir el paquete a un conjunto amplio de equipos conviene ejecutar un piloto controlado y documentar qué cambios produce el script en el estado de la estación. La aceptación no debe limitarse a comprobar que aparece un perfil VPN: debe verificarse la negociación, el tráfico autorizado, el comportamiento al desconectar y la ausencia de impactos sobre la conectividad habitual del equipo.

Prueba del piloto	Resultado esperado	Actuación si falla
Instalación de perfil y certificados	Se crea solo el perfil previsto; la confianza añadida está autorizada.	Retirar el cambio efectuado y revisar la instrucción responsable.
Conexión desde red exterior	Negociación IKE y CHILD SA completadas sin alterar otros túneles.	Contrastar eventos Windows y registros pfSense.
Acceso a servicio permitido	Se llega únicamente a los recursos y puertos autorizados.	Comprobar firewall, rutas y resolución DNS.
Rutas en desconexión	Las rutas persistentes se limitan a las asociadas al perfil.	Revisar rutas VPN exportadas y reglas de la plataforma.
Cambio de usuario en Windows	No se comparte indebidamente una credencial o certificado personal.	Revisar alcance CurrentUser/LocalMachine y material de EAP-TLS.
Retirada planificada	Es posible desinstalar el perfil y revocar el certificado sin afectar otros servicios.	Separar CA compartidas del material exclusivo de la VPN.

La reversión requiere un inventario del perfil anterior, sus rutas y certificados afectados. Si el script agrega una autoridad certificadora que también se emplea para otros servicios, retirarla indiscriminadamente puede interrumpir aplicaciones ajenas a la VPN. Las credenciales personales se revocan en la infraestructura de identidad y no se consideran anuladas simplemente por borrar archivos del ZIP en el puesto.

Para el despliegue corporativo, los responsables de operación deben registrar el paquete aprobado, la fecha de aplicación, los equipos objetivo, los resultados del piloto y los mecanismos de soporte. Esta trazabilidad permite comprobar qué versión de la política IPsec ha instalado cada equipo sin almacenar contraseñas ni copias innecesarias de claves privadas.

58.27. Documentación oficial y referencias contrastables

Las fuentes siguientes permiten verificar los comportamientos del paquete, las operaciones de Windows y los criterios de diagnóstico. Los formularios concretos pueden variar con las versiones de pfSense Plus, Windows y el paquete instalado.

Netgate — IPsec Export Package
Netgate — IPsec Mobile Clients Tab
Netgate — IKEv2 clients on Windows
Netgate — IPsec Status
Netgate — Troubleshooting IPsec Logs
Netgate — Troubleshooting IPsec Connections
Netgate — Troubleshooting IPsec Traffic
Microsoft — VpnClient PowerShell module
Microsoft — Add-VpnConnection
Microsoft — Set-VpnConnectionIPsecConfiguration
Microsoft — PowerShell Execution Policies

59 VPN → L2TP

Configuración · usuarios · direccionamiento · autenticación · firewall · interoperabilidad y seguridad

L2TP (Layer 2 Tunneling Protocol) permite transportar tráfico de nivel 2 mediante un túnel entre un cliente y un servidor. En pfSense Plus puede actuar como servicio de acceso remoto, con usuarios locales o RADIUS, direccionamiento específico y reglas de filtrado propias. Esta utilidad debe valorarse críticamente: el túnel L2TP, sin otra capa, no cifra el contenido de la comunicación.

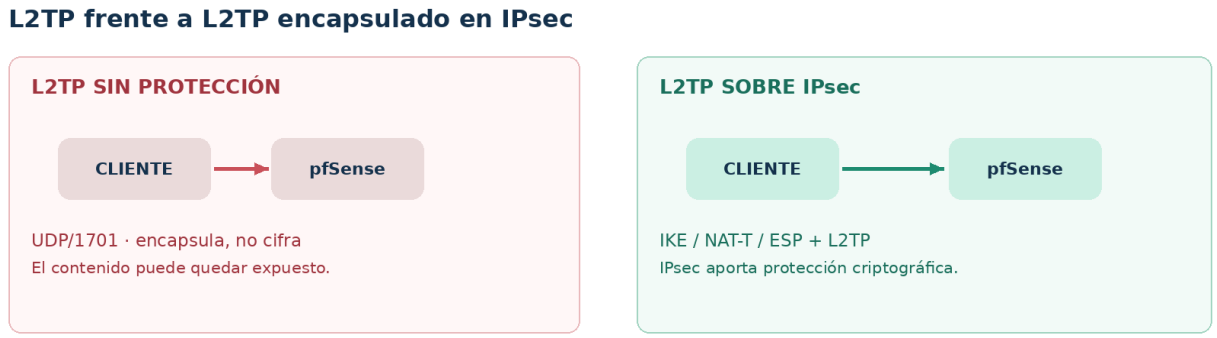


Figura 59.1. Diferencia conceptual entre el transporte L2TP sin cifrado y una sesión protegida mediante IPsec. Esquema original.

59.1. Objeto, alcance y ruta de administración

Ruta: VPN → L2TP. Configuration permite habilitar y parametrizar el servicio; Users mantiene las cuentas locales. Si el servidor está deshabilitado, la configuración puede limitarse inicialmente a Enable L2TP server. Users presenta el listado y Add para crear cuentas.

CONTROLES CONDICIONALES Habilitar el servicio muestra las opciones de configuración. Comprobarlas en un entorno de pruebas antes de aplicar cambios, especialmente cuando se trata de clientes o mecanismos de autenticación heredados.

59.2. Fundamentos del protocolo y su funcionamiento

L2TP encapsula tramas PPP dentro de paquetes UDP, normalmente mediante el puerto de destino 1701. PPP proporciona la negociación y autenticación de la sesión; L2TP organiza el túnel y la comunicación. El cliente obtiene una dirección para su extremo remoto y el firewall decide qué tráfico puede transitar hacia los recursos protegidos.

La existencia de un túnel no implica confidencialidad, integridad ni autenticación criptográfica del servidor. L2TP/IPsec añade protección mediante IPsec, pero no elimina todas las incompatibilidades existentes entre implementaciones y clientes. Una conexión establecida tampoco equivale a autorización para acceder a servidores internos: intervienen las reglas de firewall, las rutas y los servicios de nombres.

59.3. Ventajas, usos admisibles y principales limitaciones

Ventaja o aplicación	Límite y criterio profesional
Soporte de clientes heredados	Puede resolver una necesidad concreta de compatibilidad, tras prueba en entorno controlado.
Administración central de credenciales	Permite usuarios propios de L2TP o RADIUS; no equivale al User Manager general.
Direcciones para clientes	Facilita un pool y asignaciones fijas; exige no solapar redes.
Encapsulación PPP	No cifra; jamás debe confundirse con una VPN segura por sí sola.
L2TP/IPsec	Posible técnicamente, pero Netgate advierte de problemas significativos con clientes Windows detrás de NAT.

ADVERTENCIA DE SEGURIDAD La documentación vigente de Netgate aconseja evitar L2TP/IPsec salvo necesidad estricta y considerar IKEv2, OpenVPN o WireGuard para nuevas VPN de acceso remoto.

59.4. Inventario exacto de controles visibles: Configuration

Elemento visible	Efecto o interpretación
Ruta VPN / L2TP / Configuration	Confirma la sección y la pestaña activa.
Pestañas Configuration / Users	Alternan los ajustes de servicio y el mantenimiento de usuarios.
Enable L2TP server (casilla sin marcar)	En el estado mostrado, el servidor no está habilitado; marcarla permite configurar y activar el servicio cuando se guarda.
Save	Almacena los cambios. Con configuración válida y servidor habilitado, Netgate indica que se inicia el servicio.
Aviso «Don’t forget to add a firewall rule…»	Recuerda crear reglas para permitir tráfico originado por clientes L2TP, independientemente de habilitar el servicio.
Icono de ayuda e información	Acceso a ayuda/contexto. Su contenido puede variar con la versión.

59.5. Inventario exacto de controles visibles: Users

Elemento visible	Función
Pestaña Users	Inventario de cuentas definidas específicamente para L2TP.
Username	Identificador del usuario configurado.
IP address	Dirección fija asociada, cuando está definida.
Actions	Columna para acciones sobre entradas existentes; no hay filas en la imagen.
Add	Abre el formulario de creación de usuario.
Tabla vacía	No hay usuarios locales L2TP listados en la pantalla mostrada; no demuestra nada sobre RADIUS ni sobre sesiones remotas.
Iconos superiores de ayuda/controles	Elementos generales de la GUI; no se les atribuye una acción concreta sin contraste de versión.

59.6. Configuración ampliada al habilitar el servidor

Al activar Enable L2TP server se habilitan las opciones que Netgate agrupa en interfaz, direccionamiento, DNS y autenticación. Los rótulos concretos pueden variar ligeramente entre revisiones de la interfaz. No se ha supuesto un valor predeterminado para ningún campo que no aparezca documentado como tal.

59.6.1. Interface: punto de escucha

Selecciona dónde se enlaza el demonio L2TP para recibir conexiones. Habitualmente se escoge la WAN por la que entrarán los clientes. No confundir la interfaz de escucha con las redes internas a las que se permitirá acceder tras la autenticación. En despliegues con Multi-WAN, la interfaz elegida y la ruta de retorno pueden no coincidir.

59.6.2. Server Address y Remote Address Range

Server Address es la dirección que utilizará el extremo servidor del túnel; Netgate exige que esté libre y fuera del conjunto de direcciones asignadas a clientes. Remote Address Range determina el conjunto de direcciones disponibles para los clientes conectados. El rango debe ser coherente con la máscara de red, no solaparse con LAN, VLAN, VPN o redes de usuarios externos y no incluir una dirección utilizada por otro servicio.

El ejemplo gráfico emplea etiquetas abstractas y direcciones de documentación cuando se mencionan IP; son referencias pedagógicas que no pueden desplegarse en una red real. En producción se debe reservar un prefijo privado propio, revisado frente al plan corporativo y a los rangos de los usuarios.

59.6.3. Number of L2TP users y servidores DNS

Number of L2TP users determina el número máximo de conexiones simultáneas previsto para el servicio, no simplemente el número de cuentas existentes. El dimensionamiento debe contemplar usuarios concurrentes, disponibilidad de direcciones, recursos del firewall y demanda de tráfico. Los campos Primary L2TP DNS server y Secondary L2TP DNS server permiten proporcionar servidores DNS a los clientes; deben ser alcanzables a través del túnel y estar autorizados a responder las consultas correspondientes.

Campo documentado	Propósito	Validación recomendada
Interface	Interfaz local donde escucha L2TP.	Comprobar llegada y ruta de respuesta.
Server Address	Dirección del extremo servidor.	IP libre, no incluida en el rango de clientes.
Remote Address Range / máscara	Direcciones que se asignarán a clientes.	Capacidad suficiente y sin solapamientos.
Number of L2TP users	Conexiones simultáneas permitidas.	Coherencia con pool, recursos y concurrencia.
Primary / Secondary L2TP DNS server	Servidores DNS anunciados a clientes.	Conectividad, reglas y resolución de nombres.

59.7. Autenticación: métodos y consecuencias

Netgate documenta Authentication Type con las alternativas PAP, CHAP y MS-CHAPv2. La compatibilidad depende del sistema cliente y de la integración de RADIUS. PAP transporta material de autenticación especialmente sensible cuando no existe un canal cifrado exterior; CHAP y MS-CHAPv2 evitan ciertos problemas de PAP, pero no sustituyen una capa criptográfica robusta. MS-CHAPv2 tiene limitaciones conocidas y no debe presentarse como garantía moderna de protección.

Opción	Cómo funciona a grandes rasgos	Precaución
PAP	Comprobación de usuario y contraseña.	Solo contemplar bajo un transporte seguro compatible y con criterio de excepción.
CHAP	Intercambio reto/respuesta basado en un secreto compartido.	No cifra tráfico de usuario; revisar compatibilidad cliente/servidor.
MS-CHAPv2	Variante reto/respuesta ampliamente ligada a entornos históricos.	Hereda debilidades criptográficas; evitar suponer que protege el túnel.
Secret / Confirm Secret	Secreto requerido por determinadas implementaciones L2TP.	Netgate aconseja dejarlo vacío salvo necesidad del cliente; no equivale a cifrado IPsec.
Use a RADIUS server for authentication	Delega la autenticación de usuarios a RADIUS.	Validar servidor, secreto compartido, políticas y registros.

59.8. RADIUS: integración, seguridad y disponibilidad

La casilla Use a RADIUS server for authentication cambia la fuente utilizada para autenticar usuarios: deben configurarse las direcciones y secretos correspondientes al servidor RADIUS, según los controles disponibles en esa versión. Puede permitir integrar políticas centralizadas y servicios como NPS, pero no convierte L2TP en un protocolo cifrado. Con RADIUS, la pestaña Users no es la base de cuentas que necesariamente se consulta para validar un acceso.

Recomendaciones: definir permisos mínimos entre firewall y servidor RADIUS, comprobar estabilidad de red y de DNS, restringir orígenes autorizados, proteger el shared secret y registrar los eventos de autenticación. Una caída de RADIUS puede impedir nuevas conexiones aunque el servicio L2TP siga habilitado. Los nombres, puertos RADIUS secundarios y controles opcionales concretos dependen de la implementación; no se fijan valores sin verificación.

59.9. Alta y mantenimiento de cuentas locales

Ruta: VPN → L2TP → Users → Add. El formulario solicita Username, Password y Confirm Password, y permite asignar una IP estática. Comprobar los requisitos de la versión y utilizar credenciales exclusivas para esta función.

01 Confirmar que el servidor utilizará la base local de L2TP y no exclusivamente autenticación RADIUS.

02 Pulsar Add, crear un Username no ambiguo y establecer una contraseña única y suficientemente robusta.

03 Repetir la contraseña en Confirm Password. No reutilizar cuentas administrativas ni secretos de otros servicios.

04 Usar IP estática solo cuando exista una necesidad operativa, confirmando ausencia de colisiones.

05 Guardar. Verificar que el usuario aparece en la lista y ensayar acceso con un cliente de pruebas autorizado.

06 Para editar una cuenta, emplear el icono de lápiz; para eliminarla, el de papelera. Comprobar implicaciones sobre sesiones y documentación de accesos.

SEPARACIÓN DE REPOSITORIOS Los usuarios locales L2TP se administran en esta pestaña. No se debe presuponer que coincidan automáticamente con System → User Manager.

59.10. Direccionamiento: planificación y errores frecuentes

Antes de fijar las direcciones del servidor y de los clientes, elaborar un inventario de prefijos LAN/VLAN, otras VPN, redes internas de terceros y subredes domésticas previsibles. Los solapamientos provocan decisiones de enrutamiento contradictorias: el cliente puede enviar el tráfico a su red local en lugar de enviarlo por el túnel, aunque la autenticación sea correcta.

Decisión de diseño	Riesgo si se ignora	Medida de control
Elegir subred exclusiva para VPN	Colisión de rutas, inaccesibilidad.	Inventario y validación de no solapamiento.
Reservar IP del extremo servidor	Conflictos de dirección.	Separarla del pool de clientes.
Calcular sesiones concurrentes	Agotamiento de direcciones o rechazo.	Dimensionar pool y número de usuarios.
Asignar IP fija a un usuario	Duplicidad o error de trazabilidad.	Registro de reservas y prueba de conexión.
Entregar DNS interno	Conecta por IP, falla por nombre.	Permitir y probar DNS desde rango VPN.

59.11. Reglas de firewall: dos niveles obligatorios

Se aplican dos filtros independientes: llegada de UDP/1701 por la interfaz de entrada y acceso a redes interiores desde Firewall → Rules → L2TP VPN. Activar el servidor no crea automáticamente la regla de entrada; una sesión autenticada tampoco garantiza acceso a los recursos.

Con L2TP/IPsec, UDP/1701 debe permitirse donde se recibe el tráfico descifrado, habitualmente en la pestaña IPsec; no se recomienda exponer L2TP sin cifrar a Internet. IPsec requiere además la negociación IKE/NAT-T y las reglas propias de su configuración.



Figura 59.2. Recorrido lógico del establecimiento y del tráfico permitido por las reglas. Las flechas indican controles consecutivos, no una topología de producción.

59.12. Política de mínimo privilegio y segmentación

Una regla «permitir cualquier origen hacia cualquier destino» facilita una comprobación inicial, pero no constituye una política aceptable como estado final. Segmentar por grupos, recursos y puertos necesarios reduce el impacto de una credencial comprometida. Registrar accesos autorizados y bloqueados donde sea operativo ayuda a distinguir problemas de VPN de problemas de aplicación o DNS.

59.13. L2TP con IPsec: alcance real y límites

En un esquema L2TP/IPsec, IPsec protege el transporte mientras L2TP establece la sesión PPP. Netgate publica una receta de compatibilidad histórica con IPsec Mobile Clients, Phase 1, Phase 2 en modo Transport, PSK y reglas adecuadas. Las propuestas criptográficas antiguas mostradas en algunas recetas son referencias de interoperabilidad, no configuraciones recomendadas para nuevas implantaciones.

Debe evitarse confundir el secreto propio de L2TP con la clave de IPsec. Son parámetros distintos y con funciones diferentes. Un cliente Windows detrás de NAT puede completar la negociación IPsec y no lograr que L2TP funcione; la documentación oficial atribuye este síntoma a incompatibilidades entre el cliente de Windows y strongSwan. En tales escenarios se recomienda migrar a IKEv2 en lugar de abrir puertos o debilitar algoritmos de forma indiscriminada.

COMPATIBILIDAD WINDOWS + NAT Netgate advierte expresamente que una gran proporción de clientes Windows L2TP/IPsec detrás de NAT no funcionarán correctamente. No debe planificarse una implantación empresarial masiva sobre la hipótesis de compatibilidad universal.

59.14. Multi-WAN: interfaz de escucha y retorno asimétrico

L2TP usa UDP 1701 y depende de la selección de ruta para responder. Netgate documenta problemas con conexiones recibidas por una WAN distinta de la predeterminada: la respuesta puede salir por el gateway por defecto en lugar de regresar por la interfaz de entrada. Verificar rutas, captura de paquetes y correspondencia de origen y destino antes de cambiar políticas globales. No asumir que una política de encaminamiento de LAN corrige el tráfico originado por el propio firewall.

59.15. DNS Resolver y resolución de nombres

Los clientes pueden recibir los servidores DNS indicados en la configuración, pero eso no garantiza que la consulta sea aceptada. Cuando se utiliza Unbound, puede ser preciso incorporar el prefijo de clientes L2TP a las Access Lists de Services → DNS Resolver; además, las reglas del túnel deben permitir acceso a los puertos DNS y a las redes donde residen los resolutores. Comprobar tanto consultas A/AAAA como acceso a recursos por FQDN.

59.16. Procedimiento profesional: preparar un laboratorio L2TP aislado

01 Seleccionar un contexto aislado, nunca la WAN productiva, y justificar por qué se requiere L2TP frente a IKEv2/OpenVPN/WireGuard.

02 Inventariar subredes y decidir Server Address, Remote Address Range, número de sesiones y DNS. Documentar que las direcciones del manual son ilustrativas.

03 Abrir VPN → L2TP → Configuration, activar Enable L2TP server y escoger la interfaz de recepción.

04 Completar los campos documentados de direccionamiento y el método de autenticación compatible con el cliente.

05 Si se usa la base local, crear un usuario de prueba en Users; si se usa RADIUS, verificar su disponibilidad antes de guardar.

06 Guardar y comprobar el inicio del servicio, evitando anunciarlo en Internet sin una capa cifrada y reglas restrictivas.

07 Aplicar solo las reglas necesarias en la interfaz de llegada y en L2TP VPN; comprobar también DNS y rutas.

08 Conectar un cliente de laboratorio, comprobar IP, rutas, DNS y comunicación con el destino de pruebas, y registrar resultados.

59.17. Procedimiento: migración de un acceso L2TP heredado

01 Inventariar sistemas que usan L2TP y sus limitaciones; distinguir L2TP directo de L2TP protegido por IPsec.

02 Elegir destino soportado (preferentemente IKEv2, OpenVPN o WireGuard) y preparar cliente piloto con autenticación robusta.

03 Definir nuevas reglas y perfiles sin desconectar el acceso de administración actual.

04 Probar desde distintas redes y NAT, con DNS interno, segmentación y auditoría.

05 Planificar transición por grupos, revocar credenciales anteriores, cerrar UDP 1701 donde deje de ser necesario y eliminar reglas obsoletas.

59.18. Procedimiento: baja o sustitución de usuarios

Al cesar una autorización, editar o eliminar la cuenta en VPN → L2TP → Users si es local; si está centralizada, actuar en RADIUS. Comprobar sesiones activas, revisar registros y retirar asignaciones IP fijas innecesarias. Una simple eliminación de la entrada no sustituye las acciones de revocación que correspondan en la plataforma de autenticación o en las credenciales IPsec asociadas.

59.19. Comprobaciones reproducibles tras el alta

Prueba	Resultado esperado	Dónde revisar
Llegada UDP/1701	Tráfico visible en la interfaz prevista.	Diagnostics → Packet Capture / registros firewall.
Autenticación	Sesión aceptada para cuenta válida; rechazo para cuenta inválida.	Status → System Logs → VPN → L2TP Logins.
Asignación IP	IP dentro del rango previsto, sin duplicidad.	Cliente y registro de conexión.
Acceso a recurso autorizado	Comunicación únicamente a destinos permitidos.	L2TP VPN reglas, registros y servidor destino.
DNS interno	Resolución de nombres esperada sin fugas no deseadas.	Cliente, Unbound y reglas.
Reconexión y cierre	Sesiones auditables; no persistencia indeseada.	L2TP Logins y L2TP Raw.

59.20. Registros, trazabilidad y comprobación de sesiones

La documentación oficial sitúa el historial de entrada y salida en Status → System Logs → VPN → L2TP Logins. Cada evento puede registrar fecha, usuario y dirección asignada; la pestaña L2TP Raw expone mayor detalle del subsistema. En diagnósticos, correlacionar estos registros con bloqueos de Firewall y capturas de paquetes, sin guardar contraseñas ni material de autenticación.

59.21. Diagnóstico por capas y causas raíz

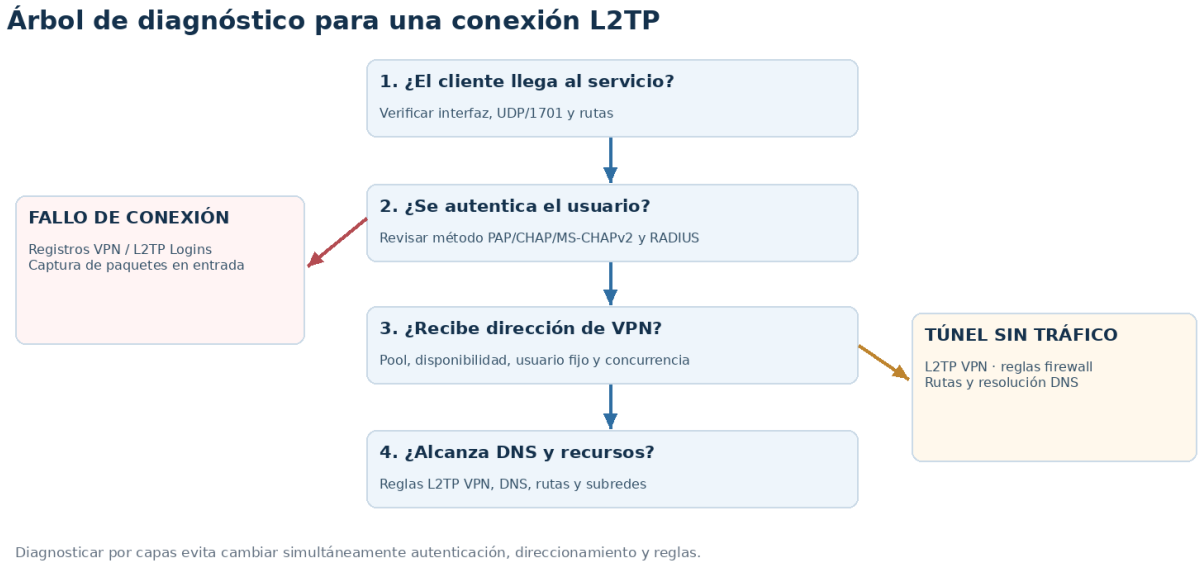


Figura 59.3. Guía de localización de incidencias por etapas: llegada, autenticación, direccionamiento y acceso. Esquema propio.

Síntoma	Causas probables	Prueba y acción
No llega a conectar	Servicio apagado, interfaz incorrecta o UDP 1701 bloqueado.	Comprobar escucha, capturas y reglas de entrada.
Fallo de usuario	Contraseña, tipo PAP/CHAP, cuenta local o RADIUS.	Consultar L2TP Logins / L2TP Raw y estado RADIUS.
Autentica sin dirección	Pool agotado o mal definido; IP estática duplicada.	Revisar direccionamiento y concurrencia.
Conecta pero no llega a servidores	Falta regla L2TP VPN, rutas o subnet solapada.	Inspeccionar reglas, tabla de rutas y captura.
Accede por IP, no por nombre	DNS suministrado inaccesible o sin ACL.	Prueba de consultas y Access Lists de Unbound.
Funciona por WAN principal y no secundaria	Asimetría de ruta / default gateway.	Capturar ida y vuelta por ambas interfaces.
IPsec establece, L2TP no funciona con Windows	Incompatibilidad conocida en cliente tras NAT.	Evitar cambios inseguros; valorar IKEv2.
Tráfico TCP bloqueado de salida en L2TP/IPsec	Condiciones de estado específicas documentadas por Netgate.	Antes de introducir una floating rule avanzada, verificar el patrón exacto en logs y revisar el impacto.

59.22. Tratamiento excepcional de estados y reglas flotantes

Netgate documenta para una incidencia concreta de L2TP/IPsec bloqueado en salida una regla Floating de dirección Out sobre la interfaz L2TP VPN, con Quick y ajuste Sloppy State. Es una solución de diagnóstico para un patrón observable en los logs, no una regla general que deba añadirse a todas las implantaciones. Antes de usarla conviene comprobar que no amplía el acceso a destinos no autorizados ni interfiere con el seguimiento normal de conexiones.

59.23. Escenarios empresariales: aplicabilidad y decisión

Escenario	Evaluación razonada	Decisión
Aplicación industrial heredada que solo admite L2TP	Aislar red y autenticación, fijar plazo de retirada y evitar exposición abierta.	Solo como excepción documentada.

Escenario	Evaluación razonada	Decisión
Teletrabajo Windows en redes domésticas con NAT	Alta probabilidad de incompatibilidad L2TP/IPsec y mayor carga de soporte.	Preferir IKEv2 u otra VPN moderna.
Conexiones de proveedores externos	Necesitan trazabilidad, revocación, segmentación y acceso limitado.	Preferir tecnología moderna con identidad individual.
Firewall con dos conexiones WAN	El retorno puede seguir gateway por defecto y romper la sesión.	No prometer alta disponibilidad automática de L2TP.

59.24. Seguridad, rendimiento, operación y continuidad

Evitar L2TP sin cifrar para datos privados. No publicar UDP 1701 indiscriminadamente. Mantener credenciales individuales y revocables, RADIUS disponible cuando se use, reglas restrictivas, registro de accesos y un plan de migración. Los recursos del firewall y el rendimiento deben evaluarse con pruebas reales; la capacidad no se deduce solo del número de usuarios que permite el formulario.

Antes de modificar un túnel en producción, guardar una copia de la configuración según la política de la organización, contar con acceso administrativo alternativo y registrar hora, responsable, alcance, validaciones y plan de reversión. La activación/desactivación o cambio de autenticación puede cortar sesiones existentes. Una modificación errónea de firewall, rutas o DNS puede dejar conexiones «establecidas» sin servicios útiles.

59.25. Glosario técnico esencial

Término	Significado
L2TP	Layer 2 Tunneling Protocol; encapsulación de tráfico PPP, sin cifrado inherente.
PPP	Protocolo punto a punto para transportar tráfico y negociar sesión/autenticación.
IPsec	Conjunto de mecanismos criptográficos para proteger comunicaciones IP.
PAP / CHAP / MS-CHAPv2	Métodos históricos de autenticación ligados a PPP.
RADIUS	Servicio externo de AAA usado para validar usuarios, según integración.
Pool de clientes	Conjunto de direcciones asignables a sesiones remotas.
WAN asimétrica	Situación en la que entrada y salida siguen interfaces diferentes.
ACL DNS	Regla que determina qué redes pueden consultar un resolver.

59.26. Checklist de revisión antes de dar el servicio por válido

- **01** Necesidad de compatibilidad justificada y alternativa moderna evaluada.
- **02** Servicio y puerto de escucha identificados; exposición de entrada limitada.
- **03** Direcciones sin solapamientos; pool, máscara y concurrencia revisados.
- **04** Autenticación local o RADIUS probada; usuarios y secretos protegidos.
- **05** Reglas de acceso a servicio y reglas L2TP VPN independientes y mínimas.
- **06** DNS, rutas, recursos internos y conectividad de vuelta verificados.
- **07** Cliente de referencia probado desde las condiciones reales de NAT/WAN.
- **08** Registros y plan de bajas, restauración y migración documentados.

59.27. Referencias oficiales y límites de versión

Las fuentes siguientes describen el comportamiento y los requisitos de L2TP en pfSense. Contrastar las opciones del servidor y de los clientes con sus versiones instaladas. No se debe presuponer que los sistemas actuales conserven las interfaces o el soporte de mecanismos L2TP heredados.

01 L2TP VPN · **02** Configuración · **03** Firewall · **04** Multi-WAN

05 L2TP/IPsec · **06** Diagnóstico · **07** Registros · **08** Autenticación

60 VPN → OpenVPN

Servidores · clientes · excepciones por identidad · asistente · criptografía · enrutamiento · operación

OpenVPN ofrece una arquitectura de túneles cifrados aplicable al acceso remoto y a la interconexión de redes. En pfSense Plus combina autenticación TLS, políticas de acceso, direccionamiento virtual, rutas y mecanismos de supervisión. Su correcta implantación exige distinguir el estado de la conexión del transporte efectivo de tráfico y conocer cómo interactúan certificados, cifrados, reglas de firewall y gateways.

ALCANCE Este capítulo examina las cuatro pestañas mostradas en VPN → OpenVPN y desarrolla de manera especialmente detallada el formulario de edición de Clients. Las pantallas de alta, los formularios del servidor y el asistente se amplían utilizando documentación oficial de Netgate. Las opciones disponibles pueden depender de versión, modo y paquete.



Figura 60.1. Dos arquitecturas funcionales: acceso remoto y túnel entre sedes. Esquema original sin datos de instalaciones reales.

60.1. Objeto y estructura de la sección

Ruta: VPN → OpenVPN. En la interfaz mostrada se presentan cuatro pestañas: Servers, Clients, Client Specific Overrides y Wizards. La primera mantiene instancias que aceptan conexiones, la segunda conexiones iniciadas por el cortafuegos, la tercera excepciones por identidad en servidores SSL/TLS, y la última conduce un procedimiento de configuración de un servidor de acceso remoto. La pantalla de Clients enseña una instancia existente; por confidencialidad, en esta obra se trata exclusivamente como ejemplo estructural de la tabla, sin reproducir ninguno de sus datos.

Pestaña	Función técnica	Acción visible en la captura
Servers	Define terminación de túneles y perfiles de acceso.	Listado y Add.
Clients	Inicia conexiones OpenVPN hacia un servidor remoto.	Listado, editar, duplicar, borrar y Add.
Client Specific Overrides	Ajustes individuales asociados a una identidad o Common Name.	Listado y Add.
Wizards	Asistente para alta de servidor de acceso remoto.	Type of Server y Next.

60.2. Fundamentos: control TLS, canal de datos y direcciones

OpenVPN encapsula paquetes IP mediante TUN (capa 3) o tramas Ethernet mediante TAP (capa 2). Sobre UDP o TCP establece un canal de control basado en TLS que valida identidades y negocia parámetros de sesión. El canal de datos transporta los paquetes cifrados. Que el proceso indique «Connected» confirma el establecimiento del túnel, pero no valida por sí mismo el permiso en firewall, la existencia de rutas de ida y vuelta ni la resolución DNS.

Normalmente se prefiere UDP para evitar interacciones de control de congestión entre TCP externo e interno. TCP puede ser necesario por restricciones de red o proxy, pero puede producir degradación bajo

pérdida de paquetes. La elección debe considerar MTU, saturación WAN, calidad del enlace y características del cliente. Un túnel de nivel 3 no transporta difusión Ethernet arbitraria; para ello se requiere TAP/bridge, menos habitual y sujeto a limitaciones importantes.

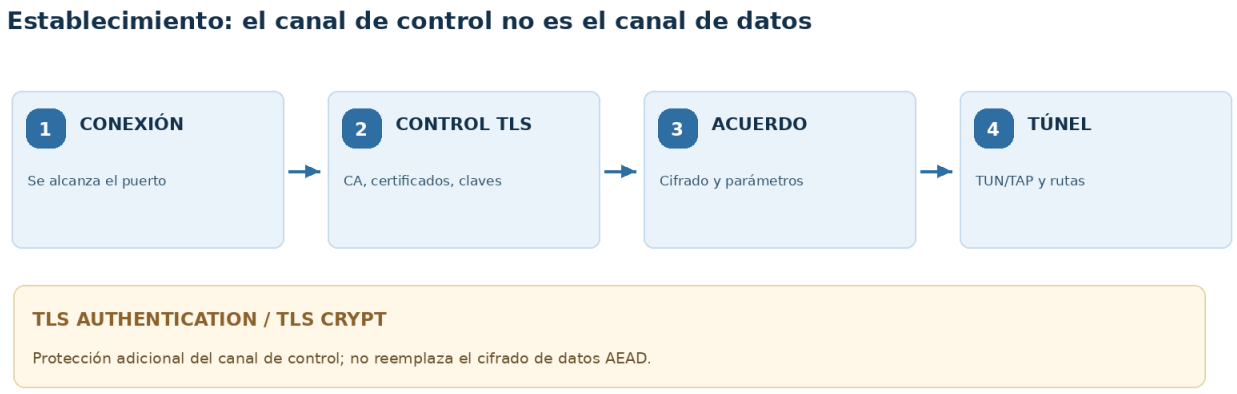


Figura 60.2. Separación entre negociación TLS, protección adicional del control y transporte cifrado de datos.

60.3. Elección del diseño antes de configurar

Necesidad	Diseño y criterio	Riesgo principal
Teletrabajo con identidad individual	Remote Access con usuarios, certificados o ambos.	Revocación de identidad y DNS insuficientes.
Dos sedes, subredes conocidas	Peer to Peer SSL/TLS y rutas de ambas redes.	Solapamiento de prefijos; ruta de retorno.
Varias sedes sobre un mismo servidor	SSL/TLS y Client Specific Overrides para cada sede.	Falta iroute / limitación DCO.
Banda ancha con CPU exigida	Evaluar DCO de pfSense Plus y cifrados AEAD.	Activar DCO con opciones incompatibles.
Compatibilidad con clientes antiguos	Proyecto temporal de migración, no modo Shared Key nuevo.	Algoritmos débiles, compresión, obsolescencia.

SEGURIDAD OpenVPN Shared Key está obsoleto y Netgate aconseja migrar a SSL/TLS. La compresión del tráfico cifrado también está desaconsejada por riesgos de filtración de secretos. No habilitar ninguna de estas opciones solo para «hacer funcionar» una conexión.

60.4. Servers: listado principal y controles visibles

Columna o control	Qué representa	Implicación administrativa
Interface	Interfaz donde escucha el servidor OpenVPN.	La elección condiciona llegada del tráfico.
Protocol / Port	Familia IPv4/IPv6, transporte y puerto de escucha.	Debe coincidir con WAN y clientes.
Tunnel Network	Red virtual destinada al transporte del túnel.	No debe solaparse con redes existentes.
Mode / Crypto	Modo del servidor y cifrado publicado.	No demuestra por sí mismo la seguridad integral.
Description	Nombre administrativo de la instancia.	Evitar incluir secretos o datos sensibles.
Actions	Controles de administración de instancias existentes.	Editar, duplicar o eliminar según iconos disponibles.
Add	Inicia alta de servidor.	No altera la red hasta guardar/aplicar la configuración.
Tabla vacía	No hay servidores listados en esta pantalla.	No implica que falten clientes salientes.

60.5. Servers: parámetros de creación y elección de modo

Add/Edit Servers se organiza en General Information, Mode Configuration, Backend for authentication, Endpoint Configuration, Cryptographic Settings, Tunnel Settings, Client Settings, Ping Settings, Advanced Client Settings y Advanced Options. La disponibilidad de cada bloque depende del modo elegido y de la versión.

60.5.1. General Information, Disabled y Description

Description permite identificar la finalidad del servidor y su rol en la arquitectura. Disabled deshabilita la instancia sin eliminar su definición; una operación de este tipo interrumpe nuevas conexiones y puede terminar sesiones. El identificador interno del servidor es generado por pfSense y sirve para diferenciar procesos, interfaces y registros; no debe emplearse como sustituto de una descripción clara.

60.5.2. Server Mode, autenticación y certificados

Modo documentado	Aplicación	Aspecto a vigilar
Remote Access (SSL/TLS)	Clientes certificados; validación de identidad mediante certificados.	Emisión y revocación de certificados individuales.
Remote Access (User Auth)	Autenticación con usuarios; backend local o externo.	Fortaleza de identidades, gestión y política MFA cuando proceda.
Remote Access (SSL/TLS + User Auth)	Combina certificado y autenticación del usuario.	Comprobar que ambas capas están realmente exigidas.
Peer to Peer (SSL/TLS)	VPN entre firewalls y enlaces LAN a LAN.	CA, certificados y rutas internas coherentes.
Peer to Peer (Shared Key)	Modo heredado de clave estática.	Obsoleto; no crear nuevas implantaciones.

Para autenticación por cuentas, el servidor puede usar Local Database, LDAP o RADIUS según modo y backends configurados. LDAP/RADIUS no crean automáticamente certificados individuales; el administrador debe habilitar el modo que exija la identidad adecuada. El control Username as Common Name modifica también el modo en el que se seleccionan los overrides.

60.5.3. DCO y Device mode en el servidor

DCO (Data Channel Offload) traslada procesamiento del canal de datos al kernel y puede mejorar mucho el rendimiento. En pfSense Plus requiere una versión que lo soporte y un túnel TLS compatible; no existe en pfSense CE según Netgate. Sus principales limitaciones documentadas incluyen UDP, suites AEAD admitidas, ausencia de compresión, incompatibilidad con opciones de inactividad, exit-notify y ciertos escenarios con enrutamiento interno iroute. En topologías TUN con /30 o prefijos menores no debe activarse.

TUN encapsula paquetes de nivel 3 y suele ser la opción adecuada. TAP trabaja en capa 2 y hace posible el puenteo, pero aumenta la complejidad de broadcast, filtrado y rendimiento. No es una elección intercambiable sin revisar ambos extremos del túnel.

60.6. Servers: endpoint, criptografía y redes

Campo de servidor documentado	Comportamiento	Verificación operativa
Protocol	UDP/TCP y familia IP para recepción.	Regla WAN concordante; no confundir UDP4 con UDP6.
Interface	IP/interfaz local a la que se enlaza.	Conexión por WAN correcta en Multi-WAN.
Local port	Puerto de escucha, habitualmente 1194 como referencia.	Validar firewall y NAT anterior si existe.
TLS key / TLS-crypt	Protege adicionalmente mensajes del canal de control.	Misma clave y modo que el cliente.
Peer Certificate Authority	CA de la que se confía la firma de certificados.	No utilizar CA no autorizadas.

Campo de servidor documentado	Comportamiento	Verificación operativa
Server certificate	Certificado usado por el servidor TLS.	Vigencia, propósito, clave privada y nombre.
Data Encryption Algorithms	Lista ordenada negociable de algoritmos.	Preferir AEAD compatibles.
Fallback Encryption Algorithm	Compatibilidad de pares que no negocian algoritmos.	Evaluar necesidad; no bajar seguridad sin análisis.
Auth digest	HMAC en contextos donde corresponde.	En AEAD no sustituye la autenticación del dato.
IPv4/IPv6 Tunnel Network	Prefijo virtual dedicado al túnel.	Separarlo de LAN, otras VPN y redes de clientes.
Local Network(s)	Redes detrás del servidor que deben alcanzar los clientes.	Rutas, reglas y DNS de destinos.
Remote Network(s)	Redes detrás de clientes remotos en enlace de sedes.	Rutas sistema + overrides / iroute según diseño.

60.6.1. Client Settings y parámetros enviados a clientes

El servidor puede enviar rutas, gateway por defecto, DNS, dominio de búsqueda, servidores NTP y parámetros de resolución de nombres. Redirect Gateway convierte el servidor VPN en salida predeterminada para el tráfico permitido; exige capacidad de enlace, NAT de salida y análisis de fugas. Dynamic IP puede facilitar continuidad de clientes que cambian IP pública. Topology subnet es la topología habitual; net30 está obsoleta y se debe evitar en nuevas instalaciones.

Los ajustes DNS Default Domain, DNS Servers, Block Outside DNS, Force DNS Cache Update, NTP Servers, NetBIOS y WINS responden a necesidades diferentes y su eficacia depende del cliente. No debe presumirse que todos los sistemas operativos aplican por igual las opciones enviadas; comprobar su resultado efectivo en el dispositivo.

60.6.2. Ping, estabilidad y Advanced Options en servidor

Los intervalos de ping y reinicio permiten detectar pares que han dejado de responder; valores demasiado agresivos pueden multiplicar reconexiones en conexiones móviles o satelitales. Advanced Options contempla, según modo, verbosidad, buffers, notificación de salida y opciones personalizadas. Las directivas personalizadas no son validadas íntegramente por pfSense: una combinación inválida puede impedir el arranque del proceso.

60.7. Clients: listado principal y operaciones visibles

La pestaña Clients gestiona instancias OpenVPN que el propio pfSense inicia hacia servidores remotos. Esto no representa una lista de usuarios que se conectan al servidor local: cada fila es una configuración de conexión saliente. La existencia de una fila no garantiza que esté conectada: el estado real se valida desde Status → OpenVPN.

Elemento	Significado	Precaución
Interface	Interfaz de salida que intentará utilizar el cliente.	Rutas Multi-WAN y gateway de destino.
Protocol	UDP/TCP, familia IP, tipo TUN/TAP.	El servidor debe soportar la misma modalidad.
Server	Destino remoto y puerto configurados.	No reproducir FQDN/IP privados en la documentación.
Mode / Crypto	Modo TLS, cifrados y digest mostrados como resumen.	Verificar negociación real en logs.
Description	Etiqueta local de mantenimiento.	No identifica credenciales ni autorización.
Lápiz	Modificar instancia.	Guardar puede reiniciar y cortar túnel.

Elemento	Significado	Precaución
Copiar / duplicar	Crear otra configuración con parámetros como punto de partida.	No duplicar secretos inadvertidamente.
Papelera	Eliminar instancia después de confirmar.	Puede dejar rutas, gateways o reglas sin utilidad.
Add	Crear instancia de cliente.	Registrar previamente servidor, CA y certificados.

CONFIDENCIALIDAD Las direcciones, nombres, puertos particulares, certificados y claves visibles en material operativo no se incluyen en el texto, tablas, esquemas, propiedades, comentarios o metadatos del Word.

60.8. Clients — General Information y Mode Configuration: campo por campo

Campo visible en formulario ampliado	Explicación técnica y consecuencias
Description	Nombre para identificar la instancia en inventarios, estado y eventos. No debe contener secretos.
Disabled — Disable this client	Con la casilla activa se conserva la definición, pero se deshabilita la conexión; puede provocar pérdida de acceso a la red remota.
Unique VPN ID	Identificador de sistema, p. ej. ovpncN; útil para asociar proceso, interfaz, regla y gateway. Su valor se genera en el sistema.
Server mode	Peer to Peer (SSL/TLS) para conexión con certificados. La variante Shared Key es obsoleta y debe migrarse.
DCO — Enable Data Channel Offload	Acelera el canal de datos en pfSense Plus; exige compatibilidad con UDP, suites AEAD y demás restricciones.
Device mode: tun	Nivel 3; paquetes IPv4/IPv6; diseño normal de redes enrutadas.
Device mode: tap	Nivel 2; transporte Ethernet para puenteos especializados; menos portable y más complejo.

60.9. Clients — Endpoint Configuration: todos los controles

Campo	Significado preciso	Acción o límite
Protocol	Familia y transporte de comunicación con el servidor.	UDP4 es habitual; TCP según restricción del entorno.
Interface	Interfaz local por la que se origina el enlace.	Puede ser WAN, VIP o grupo según versión.
Local port	Puerto UDP/TCP de origen que enlaza el cliente.	Vacío o 0: puerto dinámico; preferible normalmente.
Server host or address	FQDN o IP del servidor remoto.	Usar vpn.example.com como ejemplo; revisar resolución DNS.
Server port	Puerto de escucha remoto.	1194 es referencia común, no obligatorio.
Proxy host or address	Proxy HTTP intermedio del cliente.	Solo cuando el modo de transporte permite proxy TCP.
Proxy port	Puerto del proxy configurado.	Distinguirlo del puerto real del servidor OpenVPN.
Proxy Authentication	Método de autenticación del proxy.	Según opción, requiere credenciales específicas.

La selección Interface no garantiza por sí sola la ruta correcta cuando el destino remoto se resuelve a una IP alcanzable por una WAN diferente de la predeterminada. La documentación oficial señala que en ciertos escenarios hace falta una ruta estática explícita hacia el servidor. Evitar que la ruta al propio servidor

OpenVPN quede dentro del túnel que intenta establecerse, lo que crea un bucle o dependencia de conectividad.

60.10. Clients — User Authentication Settings

Campo	Función	Riesgo de mala configuración
Username	Usuario enviado a un backend cuando el servidor lo exige. Puede quedar en blanco cuando no hay autenticación de usuario.	Usar una cuenta incorrecta puede provocar AUTH_FAILED.
Password	Contraseña asociada al usuario anterior, solo si el servidor la necesita.	Un secreto introducido debe tratarse como credencial operativa.
Authentication Retry — Do not retry connection when authentication fails	Activa salida del proceso cuando recibe rechazo de autenticación; sin la opción normalmente intenta reintentar.	Puede detener el servicio hasta intervención del operador; útil para evitar bucles de intentos.

No es recomendable reutilizar la cuenta de administrador del firewall ni compartir una identidad personal entre varias sedes. Si la autenticación se integra con RADIUS o LDAP, verificar fallos de backend, MFA y política de bloqueo; la disponibilidad del túnel puede depender de servicios externos además de la conectividad IP.

60.11. Clients — TLS Key, Usage Mode y certificados

El campo Use a TLS Key solicita una clave compartida adicional para proteger los paquetes del canal de control. Esta clave no reemplaza ni a la CA, ni al certificado del cliente, ni a la cifra del canal de datos. Cuando el servidor usa TLS Authentication, el cliente debe utilizar la misma clave y direcciones compatibles. TLS Encryption and Authentication (tls-crypt cuando corresponde) añade cifrado al canal de control y reduce exposición de metadatos.

Control	Qué significa	Comprobación
TLS Configuration / Use a TLS Key	Habilita mecanismo complementario de autenticación/cifrado de control.	Ambos extremos deben soportar mismo modo.
TLS Key	Material criptográfico compartido.	No pegarlo en manuales, tickets ni registros.
TLS Key Usage Mode	TLS Authentication o modo de cifrado/autenticación según servidor.	Misma modalidad en ambos lados.
TLS keydir direction	Dirección HMAC específica en tls-auth.	Si extremo A usa 0, extremo B usa 1; ambos pueden omitir.
Peer Certificate Authority	CA confiable de los certificados del servidor.	Importarla por System → Cert. Manager.
Peer Certificate Revocation List	CRL con certificados revocados, si existe.	Plan de revocación y distribución vigente.
Client Certificate	Certificado y clave privada local.	Vigencia, EKU, CA emisora y uso correcto.

CLAVE TLS SENSIBLE Una clave TLS real incluida en un formulario o copia de configuración debe tratarse como secreto. Si se ha compartido fuera del ámbito autorizado, planificar su rotación simultánea en ambos extremos. No usar valores inventados como «clave de ejemplo» para formar una VPN real.

60.11.1. Cómo validar la cadena de confianza sin debilitar TLS

La conexión necesita una cadena verificable hasta una CA reconocida, certificados no vencidos, coincidencia con el uso previsto y ausencia de revocaciones relevantes. Server Certificate Key Usage Validation comprueba el uso del certificado presentado por el extremo remoto como servidor TLS, evitando que se acepte sin más un certificado de cliente. Para fallos de confianza, corregir la PKI o el certificado y no desactivar la validación de forma permanente.

60.12. Clients — Data Encryption Algorithms, fallback y digest

La lista «Available Data Encryption Algorithms» reúne opciones que la compilación ofrece, incluso algoritmos antiguos o poco convenientes para nuevos enlaces. «Allowed Data Encryption Algorithms» determina cuáles se anuncian y en qué orden; su selección no implica que todos se vayan a usar, pues la negociación acuerda una cifra común. AES-256-GCM, AES-128-GCM y ChaCha20-Poly1305 son familias AEAD de uso habitual; la compatibilidad concreta con DCO depende de la revisión de pfSense Plus/OpenVPN.

Control / familia	Función	Criterio actual
AES-256-GCM / AES-128-GCM	Cifrados AEAD autenticados.	Opciones preferentes si el hardware y el par lo soportan.
CHACHA20-POLY1305	AEAD basado en cifrado de flujo.	Alternativa eficiente según plataforma.
AES-CBC	Cifrado en bloque heredado que requiere integridad separada.	Restringir a compatibilidad justificada.
AES-CFB / OFB y CAMELLIA	Modos históricos disponibles en ciertos builds.	No asumir recomendación por figurar en el selector.
3DES / DES-EDE, None	Algoritmos antiguos o sin cifrado.	No recomendables para nuevas implantaciones.
Allowed Data Encryption Algorithms	Lista ordenada que negocia con el servidor.	Preferir subconjunto moderno compatible.
Fallback Data Encryption Algorithm	Cifra para pares incapaces de negociar.	Evitar habilitar legacy sin necesidad; documentar impacto.
Auth digest algorithm	HMAC donde procede; con AEAD queda aplicado al control según modo.	SHA256 para compatibilidad verificada; no confundir con cifra.
Server Certificate Key Usage Validation	Exige uso de certificado de servidor.	Activar cuando la PKI sea compatible.

COMPATIBILIDAD DCO La documentación de Netgate enumera AES-256-GCM, AES-128-GCM y ChaCha20-Poly1305 entre las cifras compatibles con DCO, pero algunas páginas de ajustes están referidas a revisiones con selección más limitada. Comprobar la versión instalada y la ayuda contextual antes de fijar opciones; no extrapolar valores a todas las versiones.

60.13. Clients — Tunnel Settings: direcciones IPv4 e IPv6

Campo	Propósito y comportamiento
IPv4 Tunnel Network	Subred virtual del túnel; en SSL/TLS normalmente debe quedar en blanco en el cliente si el servidor asigna la dirección. Una red /30 o menor fuerza un comportamiento especial P2P con limitaciones.
IPv6 Tunnel Network	Prefijo virtual IPv6; normalmente proporcionado desde el servidor; con ajuste estático del cliente aplica asignación local según documentación.
IPv4 Remote network(s)	Prefijos detrás del servidor que deben encaminarse por el túnel. Separa con comas; evitar superponer redes locales.
IPv6 Remote network(s)	Equivalente IPv6 para destinos de la red remota. Exige políticas y retorno IPv6 coherentes.
Limit outgoing bandwidth	Límite de envío en bytes/s, no bits/s; 100–100.000.000, campo vacío sin límite. Incompatible con UDP Fast I/O.

En un cliente site-to-site, Remote Networks normalmente se refiere a redes alcanzables en el otro extremo. El prefijo virtual del propio túnel no debe confundirse con los prefijos LAN conectados. Para ilustraciones se emplean exclusivamente nombres reservados y el prefijo IPv6 2001:db8::/32; todos los diagramas son lógicos, no una receta de direccionamiento desplegable.

60.14. Clients — Compression y Topology

Allow Compression activa la posibilidad de comprimir paquetes del túnel; la compresión previa al cifrado presenta riesgos conocidos de recuperación de información (por ejemplo VORACLE). En redes modernas es preferible deshabilitarla y corregir la configuración heredada. El selector Compression puede presentar Adaptive LZO Legacy y otros modos asociados a compatibilidad antigua: no deben interpretarse como opciones seguras por defecto.

Topology subnet configura una única subred lógica en TUN. El comportamiento de direccionamiento debe concordar en servidor y cliente; net30 está obsoleto en instalaciones nuevas. Un error de topología puede hacer que el túnel negocie pero que la interfaz virtual no obtenga una dirección válida o que los paquetes no encuentren su siguiente salto.

60.15. Clients — Rutas automáticas, DNS y opciones de tráfico

Control	Marcado / comportamiento	Desmarcado / precaución
Type-of-Service	Copia el TOS del paquete interior a la cabecera exterior.	Puede revelar clases de tráfico y no garantizar QoS fin a fin.
Don’t pull routes	El cliente no acepta rutas anunciadas por el servidor.	Desmarcado: puede recibir rutas, incluida la predeterminada.
Don’t add/remove routes	OpenVPN no instala ni retira rutas mediante comandos del SO.	Se requiere gestión externa del routing; no elimina reglas.
Pull DNS	pfSense puede utilizar los DNS entregados por servidor remoto para servicios propios.	Puede alterar cómo resuelve nombres el firewall.
Gateway creation	Both / IPv4 only / IPv6 only para gateways al asignar interfaz.	La selección de familia afecta gateway monitoring y PBR.

60.15.1. Interacción con DNS Resolver/Forwarder

Cuando se habilita Pull DNS en un cliente del firewall, los DNS remotos pueden influir en consultas realizadas por el propio pfSense y, según su integración, en DNS Resolver/Forwarder. No basta con que la VPN tenga conectividad a una IP: verificar puertos 53/UDP y 53/TCP, acceso a resolutores autorizados y ausencia de rutas que envíen la consulta fuera del túnel cuando no se desea.

60.16. Clients — Ping Settings y salida por inactividad

Parámetro	Acción	Advertencia
Inactive	Termina proceso tras N segundos sin tráfico útil en TUN/TAP; 0 desactiva.	No incluye pings ni control TLS como actividad. Puede no reiniciarse automáticamente.
Ping method	Selecciona la forma de definir keepalive y ping-restart.	Alinear con capacidades del par y condiciones WAN.
Interval	Cadencia de paquetes de supervisión configurados por método.	Intervalos cortos producen tráfico y ruido en enlaces malos.
Timeout	Tiempo de detección de pérdida antes de reiniciar sesión.	Demasiado corto genera flapping; demasiado largo oculta fallos.

El par de valores ilustrativos 10/60 es habitual en ciertas configuraciones, pero no universal. En enlaces con elevada latencia o pérdidas intermitentes debe comprobarse el comportamiento real antes de reducir tiempos. DCO no es compatible con el timeout por inactividad descrito en su documentación y puede ignorar o deshabilitar ciertos parámetros.

60.17. Clients — Advanced Configuration: detalles técnicos

Campo	Qué hace	Riesgo o compatibilidad
Custom options	Inserta directivas de OpenVPN separadas por punto y coma.	Pueden anular GUI y provocar error de inicio.

Campo	Qué hace	Riesgo o compatibilidad
UDP Fast I/O	Optimiza operaciones de escritura de paquetes UDP.	Experimental; incompatible con límite de ancho de banda y DCO.
Exit Notify	Notifica cierre a servidor/pares mediante UDP.	No compatible con algunos modos P2P / DCO.
Send/Receive Buffer	Ajusta buffers de red del proceso.	Requiere pruebas; 512 KiB es punto inicial de evaluación, no valor global.
Gateway creation	Limita gateways IPv4/IPv6 creados cuando se asigna interfaz.	Cambiarlo puede alterar rutas/policy routing.
Verbosity level	Controla detalle de registros; nivel 3 suele ser útil para diagnóstico.	Niveles elevados generan volumen y pueden exponer metadatos.

60.18. Clients — procedimiento detallado para nueva conexión SSL/TLS

01 Inventariar propósito de enlace, responsable, ventana de cambio, rutas locales/remotas y dirección de salida. Verificar acceso de gestión alternativo.

02 Obtener de forma segura CA, certificado de cliente, clave privada y, si procede, material tls-auth o tls-crypt. Importar desde System → Cert. Manager.

03 Abrir VPN → OpenVPN → Clients → Add. Introducir Description neutra y elegir Peer to Peer (SSL/TLS).

04 Seleccionar Device mode tun, protocolo UDP de la familia correcta, interfaz WAN y FQDN autorizado como vpn.example.com; usar puerto confirmado por el servidor.

05 No establecer local port salvo requisito; configurar proxy solo en escenarios TCP compatibles. Añadir Username/Password exclusivamente si el servidor usa autenticación de usuario.

06 Ajustar TLS Key Usage Mode, CA, certificado y dirección tls-auth para que coincidan con el extremo remoto, sin exponer materiales de clave en informes.

07 Establecer lista de AEAD negociables y fallback solo si existe requerimiento heredado; comprobar DCO y sus incompatibilidades antes de activarlo.

08 Definir IPv4/IPv6 Remote Networks según arquitectura; dejar Tunnel Network al servidor si este asigna dirección dinámica. Revisar topología y ausencia de solapamientos.

09 Mantener compresión deshabilitada, revisar rutas automáticas y DNS. Guardar la instancia.

10 Crear o comprobar las reglas que permitan el tráfico útil del túnel, tanto de origen como de retorno; revisar NAT solo si la arquitectura lo exige.

11 Abrir Status → OpenVPN, consultar OpenVPN logs y realizar pruebas desde firewall y hosts internos; documentar latencia, pérdida, ruta y DNS.

12 Aplicar ajustes de rendimiento uno a uno, especialmente DCO, buffers, MTU y pings; disponer de procedimiento de reversión.

60.19. Client Specific Overrides: listado principal

Esta pestaña presenta la tabla CSC Overrides con columnas Disabled, Common Name, Description y Actions, además de Add. Las entradas permiten aplicar parámetros específicos a una identidad de cliente de servidor OpenVPN. La captura no contiene entradas. La función está pensada para conexiones que llegan a una instancia de servidor; no para modificar indiscriminadamente un cliente saliente configurado en Clients.

Columna / control visible	Significado
Disabled	Indica si una excepción está desactivada.
Common Name	Identificador con el que se compara el cliente autenticado.
Description	Finalidad de la excepción.
Actions	Editar, copiar o eliminar una excepción existente según versión.

Columna / control visible	Significado
Add	Crear entrada de Client Specific Override.

60.20. Overrides: formulario Add/Edit documentado

Campo oficial	Efecto operativo y condición
Description / Disable	Etiqueta de la excepción y desactivación no destructiva.
Common Name	Coincide con CN de certificado o usuario según Username as Common Name.
Connection Blocking	Rechazo temporal de conexiones coincidentes; no reemplaza revocar certificado/cuenta.
Server List	Servidores a los que se aplica la excepción; sin selección puede aplicarse a todos.
IPv4/IPv6 Tunnel Network	Preferencia de dirección virtual cliente; no es reserva absoluta.
IPv4/IPv6 Local Network(s)	Rutas adicionales que se envían a este cliente; se suman a las globales.
IPv4/IPv6 Remote Network(s)	Prefijos accesibles a través de cliente; se generan rutas internas OpenVPN (iroute).
Redirect Gateway	Empuja una ruta por defecto al cliente seleccionado.
Server Definitions	Permite suprimir opciones de servidor enviadas al cliente.
Remove Server Routes	Evita rutas globales del servidor para cliente, dejando otras opciones.
DNS Default Domain / DNS Servers	Sobrescribe o complementa DNS publicado para un cliente particular.
NTP Servers / NetBIOS Options	Ajustes por cliente para tiempo y parámetros heredados de nombres.
Advanced	Directivas personalizadas separadas por punto y coma.

60.20.1. Common Name, Username as Common Name y entrada DEFAULT

Si se usa autenticación por certificado únicamente, Common Name coincide con el CN del certificado. Con usuario+certificado depende de la opción Username as Common Name del servidor; si está activada, se utiliza el usuario. La entrada especial DEFAULT es una regla de excepción aplicable cuando no coincide ninguna otra; puede servir para bloquear por defecto, pero debe ensayarse cuidadosamente para evitar denegar el acceso legítimo.

60.20.2. Ruta del sistema frente a iroute interno

En entornos con varias sedes conectadas a un solo servidor OpenVPN, la red detrás de un cliente necesita dos informaciones: una ruta del sistema operativo del servidor para enviar tráfico al proceso OpenVPN, y una ruta interna (iroute) para que el proceso identifique cuál de sus clientes debe recibirlo. Los Remote Networks del servidor establecen la ruta del cortafuegos y los Remote Networks del override identifican el cliente. Su ausencia produce túnel conectado pero inaccesibilidad de la red de ese cliente.



Figura 60.3. Diferencia fundamental entre rutas del cortafuegos y rutas internas del servicio OpenVPN.

LIMITACIÓN DCO DCO no usa actualmente iroute en el patrón de múltiples sedes conectadas a un único servidor que dependen de Client Specific Overrides. Evitar activar DCO en esa arquitectura sin un diseño alternativo explícitamente probado.

60.21. Wizards: primera pantalla y tipos de autenticación

Ruta VPN → OpenVPN → Wizards. La primera pantalla mostrada presenta «OpenVPN Remote Access Server Setup» y la selección «Type of Server», inicialmente «Local User Access», seguida de Next. El aviso de la propia pantalla indica que el asistente puede abandonarse en cualquier momento mediante el elemento de cabecera previsto en esa interfaz. La documentación oficial incorpora las modalidades Local User Access, LDAP y RADIUS.

Type of Server	Efecto en asistente	Consideración
Local User Access	Autenticación gestionada en el firewall; modo SSL/TLS + User Auth y certificados de usuario.	Adecuado para menor complejidad y usuarios individuales.
LDAP	Integra una fuente LDAP configurada o creada en el proceso.	Usar canal TLS verificado y estructura DN correcta.
RADIUS	Integra un backend RADIUS gestionado en pfSense.	Verificar disponibilidad, secretos y políticas MFA.

60.22. Wizards: recorrido verificado de los pasos siguientes

01 Elegir backend de autenticación. Para Local User Access se evitan pasos específicos LDAP/RADIUS; para los demás se selecciona o registra un servidor de autenticación.

02 Seleccionar una CA existente o generar una de uso controlado. Gestionar autoridad, vigencia, custodia y exportación del material criptográfico.

03 Seleccionar o crear un certificado de servidor con uso correcto, nombre y validez apropiados; comprobar que corresponde al servidor que recibirá conexiones.

04 Configurar servidor OpenVPN: interfaz, protocolo, puerto, cifrados, TLS, Tunnel Network, redes locales, DNS, topología y demás campos presentados por la versión.

05 Revisar la configuración de reglas de firewall ofrecida por el wizard: regla de entrada WAN y regla de tránsito por OpenVPN. Ajustar después a mínimo privilegio.

06 Finalizar, comprobar estado, crear usuarios/certificados si procede, distribuir perfiles mediante procedimiento seguro y ejecutar pruebas de aceptación.

Netgate indica que DCO no forma parte del asistente en la documentación consultada: si se pretende usar, completar el wizard y después editar el servidor para habilitarlo tras comprobar compatibilidad.

60.23. Reglas WAN, reglas del túnel y NAT: capas distintas

La creación de servidor OpenVPN no introduce por sí sola una regla WAN de acceso, salvo la que pueda generar opcionalmente el asistente. La regla WAN permite llegar al puerto del demonio; después de autenticar, el tráfico interior pasa por Firewall → Rules → OpenVPN o por la pestaña de interfaz asignada. Son dos filtros distintos. Un cliente saliente debe poder abrir la conexión hacia el servidor y también disponer de permisos internos para acceder a redes detrás del túnel.

Si el tráfico sale a Internet a través de la VPN, evaluar NAT de salida en el destino; si se conectan dos LAN, lo normal es preservar direccionamiento y enrutar sin NAT, salvo solapamientos que demanden una solución explícita. Evitar crear NAT para ocultar errores de retorno: antes comprobar la ruta y el firewall de destino.

60.24. Asignación de interfaces OpenVPN: capacidades y peligros

Interfaces → Assignments permite asignar una interfaz ovpns/ovpnc. Esto habilita reglas por interfaz, NAT, gateways y policy routing granular. Netgate advierte que debe configurarse correctamente el gateway predeterminado antes de asignar una interfaz VPN; si permanece Automatic, el sistema podría tomar la VPN como gateway por defecto de forma inesperada.

Tras la asignación puede ser necesario guardar de nuevo la instancia OpenVPN para regenerar el proceso y recuperar el túnel. Las reglas genéricas de la pestaña OpenVPN se evalúan antes que las reglas de las pestañas de interfaces asignadas: una regla permisiva global puede impedir que una regla más específica controle el tráfico. Cualquier cambio de reglas o gateways debe tener plan de reversión y vía alternativa de acceso al cortafuegos.

60.25. Multi-WAN, failover, rutas y alta disponibilidad

La interfaz del cliente fija su origen preferido, pero la ruta real hacia IP de servidor, la resolución de su FQDN y el gateway predeterminado pueden conducir a otra WAN. En escenarios de enlaces alternativos, documentar rutas host al servidor, comportamiento de gateway groups y condiciones de failover; no asumir que cambiar una selección garantiza recuperación inmediata. Si se usan VIP CARP, la instancia cliente puede quedar detenida cuando el nodo es BACKUP, para evitar rutas incoherentes.

Para alta disponibilidad hay que revisar persistencia de estado, certificados en ambos nodos, regla de salida y comportamiento de restablecimiento. Un failover interrumpe sesiones TCP establecidas dentro de túneles cuando cambian las identidades o direcciones del extremo, incluso si el VPN vuelve a aparecer conectado.

60.26. IPv6 y Dual-Stack: reglas específicas

Un cliente UDP4/TCP4 usa IPv4 para el transporte, pero un túnel TUN puede transportar IPv6 en el interior si ambos extremos lo habilitan. Diferenciar familia del socket OpenVPN, prefijo del túnel y redes accesibles. Las reglas de IPv4 no autorizan automáticamente IPv6. Revisar además resolución AAAA, NDP si hay puenteo TAP y acceso a servidores DNS con IPv6. El prefijo 2001:db8::/32 se emplea solo como ejemplo documental.

60.27. Rendimiento: DCO, MTU, cifrado y ancho de banda

DCO reduce cambios de contexto y aumenta la eficiencia del canal de datos, pero sus restricciones tienen prioridad sobre expectativas teóricas de velocidad. En pruebas representativas comparar throughput, latencia, CPU, pérdidas y estabilidad con y sin DCO, usando cifras AEAD compatibles. Un enlace WAN saturado o un sistema de almacenamiento lento puede limitar el rendimiento antes que la CPU criptográfica.

Un desajuste MTU/PMTUD suele manifestarse como conexiones pequeñas exitosas y transferencias grandes bloqueadas. Diagnosticar con capturas y pruebas de paquetes de tamaños progresivos; evitar ajustar fragmentación/MSS sin evidencia y revisar firewalls que bloquean ICMP necesario. Los límites de salida del formulario están en bytes/s; por ejemplo 1 000 000 bytes/s equivale aproximadamente a 8 Mbit/s de carga útil antes de overhead, sin confundir unidades.

60.28. Seguridad operativa y ciclo de vida de certificados

Mantener una CA controlada, emitir identidades diferentes para máquinas/usuarios, registrar vencimientos y revocar certificados comprometidos mediante CRL. Restringir rutas anunciadas, habilitar reglas de mínimo privilegio, proteger material TLS, no guardar contraseñas en documentación y evaluar MFA con el método de autenticación realmente soportado. Cambiar un certificado, una CA, una clave tls-auth o un modo tls-crypt exige coordinación de ambos extremos.

Aumentar Verbosity temporalmente para diagnóstico y volver a un nivel operativo. Evitar adjuntar logs no depurados a sistemas externos: pueden revelar endpoints, Common Names, IPs, rutas, estructuras internas o datos de sesión. El backup de pfSense puede incluir material sensible; debe cifrarse, restringirse y someterse a control de acceso.

60.29. Procedimiento empresarial A: acceso remoto con identidad individual

01 Definir grupo autorizado, subred de túnel exclusiva, recursos y aplicaciones publicados; documentar DNS y política split/full tunnel.

02 Elegir una CA y certificado de servidor de confianza. Configurar el backend de usuarios y su política de credenciales.

03 Ejecutar Wizards o crear el servidor manualmente; preferir TLS moderno, UDP y AEAD, sin compresión ni Shared Key.

04 Configurar red virtual de clientes, DNS interno, reglas WAN y reglas de la VPN restringidas a recursos permitidos.

05 Emitir certificados personales si el modo los requiere; exportar perfiles solo por un canal seguro y comprobar nombre del servidor y CA.

06 Verificar desde una red externa no administrada: autenticación válida e inválida, DNS, rutas, aplicaciones autorizadas y rechazos esperados.

07 Auditar sesiones y definir procedimiento de baja con revocación y retirada de privilegios, no solo bloqueo temporal mediante override.

60.30. Procedimiento empresarial B: interconectar dos sedes

01 Asegurar que ninguna red LAN, VLAN o VPN colisiona entre ambas sedes; registrar rutas de retorno y disponibilidad WAN.

02 Crear CA, certificado servidor y certificado cliente, con extensiones válidas y copias seguras para cada extremo.

03 Crear servidor Peer to Peer SSL/TLS con TUN y red de túnel exclusiva. Establecer Local/Remote Network coherentes con el diseño.

04 En la otra sede, abrir Clients → Add, elegir interfaz WAN, destino vpn.example.com, puerto acordado, CA, certificado y modo TLS.

05 Mantener compresión desactivada; alinear parámetros de cifrado; comprobar compatibilidad de DCO antes de activarlo.

06 Permitir tráfico de negocio seleccionado en ambas sedes sin regla «allow any» perpetua; verificar retorno desde los equipos finales.

07 Observar OpenVPN status, logs, rutas, DNS y capturas desde origen y destino. Ensayar reconexión y fallo WAN supervisado.

60.31. Procedimiento empresarial C: varias sedes con overrides

01 Definir una identidad separada por sede mediante certificado o usuario inequívoco según configuración Common Name.

02 Crear rutas del sistema operativo hacia las redes de cada sede en el servidor OpenVPN, usando Remote Network(s) del servidor.

03 Crear un Client Specific Override por sede y vincularlo al servidor correspondiente; especificar Remote Network(s) de ese cliente para generar iroute.

04 No activar DCO en arquitectura que dependa del iroute interno no soportado; estudiar alternativas antes de migrar.

05 Comprobar desde una sede hacia su red propia, desde el servidor y desde otra sede autorizada. Revisar el orden de reglas y rutas de retorno.

60.32. Checklist de validación reproducible

Verificación	Resultado de aceptación	Fuente de evidencia
Resolución FQDN del servidor	Resuelve la dirección planificada por la WAN prevista.	DNS Resolver / Diagnostics → DNS Lookup.
Transporte y firewall	El flujo UDP/TCP entra/sale por interfaz correcta.	Packet Capture / Firewall Logs.
TLS / CA / certificado	El par se valida sin advertencias ni errores de uso.	OpenVPN logs.
Negotiación cifrada	Existe cifra común y las políticas coinciden.	OpenVPN logs / estado.
Interfaz túnel	Dirección/prefijo correcto y proceso activo.	Status → OpenVPN / Interfaces.
Rutas	Rutas a prefijos remotos y de retorno presentes.	System → Routing / Diagnostics.
DNS interno	Resuelve FQDN autorizado y alcanza el servidor DNS.	nslookup/dig con orígenes controlados.
Política de acceso	Permite recurso necesario y bloquea recurso prohibido.	Firewall Rules / estado y capturas.
Resiliencia	Recupera conexión después de corte acotado.	OpenVPN status y cronología de logs.
Privacidad y copias	Sin claves ni topología sensible en documentación.	Auditoría editorial y control de backups.

60.33. Diagnóstico estructurado: identificar la etapa que falla



Figura 60.4. Secuencia de diagnóstico por capas desde la conectividad externa hasta los recursos internos.

Comenzar por Status → OpenVPN y Status → System Logs → OpenVPN. Si falta el intento de conexión, comprobar FQDN, rutas, protocolo, puerto y reglas WAN; si aparece TLS error, examinar CA, hora, certificados, EKU y TLS Key; si se establece el túnel sin tráfico, comprobar rutas, reglas, gateway y DNS. Usar Diagnostics → Packet Capture en WAN, túnel y LAN para confirmar entrada, tránsito y salida del paquete, sin volcar tráfico sensible innecesariamente.

60.34. Matriz de incidencias frecuentes

Síntoma	Causa probable	Comprobación / corrección segura
AUTH_FAILED	Usuario/contraseña o backend rechazado.	Revisar origen de autenticación y logs, sin registrar credenciales.
TLS Error / verify failed	CA, fecha, certificado o clave de control no coinciden.	Validar cadena, EKU, revocación y reloj en ambos extremos.
TLS key mismatch	tls-auth vs tls-crypt, dirección o material distinto.	Alinear modo y claves con intercambio seguro.
Conexión no sale por WAN prevista	Ruta al servidor y gateway incorrectos.	Capturar flujo saliente; establecer ruta adecuada.
Sin negociado de cifrado	No hay algoritmo común; fallback inapropiado.	Alinear AEAD compatibles y modo DCO.
Conectado, sin ping LAN	Faltan rutas/firewall/retorno o ICMP bloqueado.	Comprobar con TCP a servicio real y capturas.
Una sede no llega a su red	Falta override iroute o ruta en servidor.	Validar las dos tablas de enrutamiento.
Solo falla por nombre	DNS no anunciado, inaccesible o bloqueado.	Consultar resolutor autorizado desde origen real.
Conexiones largas se cortan	Ping timeout, inestabilidad WAN, NAT, flapping.	Correlación de logs y cambios de IP del enlace.
DCO activado, sin tráfico	Opción incompatible, compresión o /30.	Revisar limitaciones DCO y probar sin DCO.
Fichero grande se bloquea	MTU/PMTUD y fragmentación.	Captura y pruebas de tamaños con ICMP.
Tras asignación interfaz pierde conectividad	Gateway automático o reinicio de proceso pendiente.	Revisar default gateway y re-guardar instancia.
Servidor permite conexión, pero reglas no se aplican	Regla global OpenVPN precede a interfaz asignada.	Reordenar reglas según política de mínimo privilegio.

60.35. Alertas especiales: cambios que pueden interrumpir el servicio

OPERACIÓN CRÍTICA Cambiar modo de autenticación, CA, certificados, cifrados, puerto, red virtual, topología, reglas o rutas interrumpe o invalida conexiones. Antes de aplicar, preservar acceso alternativo al firewall, copia de configuración, ventana acordada y procedimiento de reversión.

Cambios en Pull DNS pueden modificar la resolución del propio cortafuegos y afectar otros servicios; Disable en un cliente puede retirar rutas de una sede completa; la asignación de interfaz puede introducir gateways inesperados y afectar policy routing. Habilitar rutas por defecto al cliente cambia el camino de Internet, obliga a validar NAT y puede afectar cumplimiento normativo y fugas DNS.

60.36. Control de calidad y seguimiento de explotación

Registrar responsables de cada instancia, razón de negocio, red de origen/destino, backend de autenticación, CA y fechas de caducidad (sin claves), puertos de llegada, reglas asociadas, gateway de salida, supervisión y plan de recuperación. Mantener un registro de configuraciones deshabilitadas, rutas obsoletas y certificados revocados. Después de cada actualización de pfSense Plus, revisar changelog de OpenVPN, DCO y compatibilidad con clientes remotos antes de actualizar en producción.

60.37. Glosario técnico

Término	Definición breve
OpenVPN	Software y protocolo de VPN que usa TLS y un canal de datos cifrado.
TUN / TAP	Dispositivo virtual capa 3 / dispositivo virtual capa 2.

Término	Definición breve
DCO	Data Channel Offload: aceleración de datos en kernel.
CA / CRL / EKU	Autoridad de certificación / lista de revocación / uso extendido de clave.
TLS-auth / TLS-crypt	Autenticación adicional / cifrado y autenticación del canal de control.
AEAD / GCM	Cifrado autenticado / modo autenticado basado en Galois/Counter.
CN / CSC	Common Name; Client Specific Override.
iroute / route	Ruta interna de OpenVPN a cliente / ruta del sistema operativo.
Split tunnel / full tunnel	Solo redes seleccionadas por VPN / túnel como ruta de salida general.
NAT / PBR / CARP	Traducción de direcciones / policy based routing / redundancia con VIP.
PMTUD / MTU	Descubrimiento de MTU extremo a extremo / unidad máxima transmisible.

60.38. Referencias oficiales y documentación técnica

Las siguientes referencias enlazan la documentación original. Las funcionalidades y opciones pueden cambiar con la versión instalada. El administrador debe contrastar la ayuda contextual del formulario antes de aplicar parámetros avanzados.

01. Netgate — OpenVPN Configuration Options
02. Netgate — Server Configuration Options
03. Netgate — Client Configuration Options
04. Netgate — Client Specific Overrides
05. Netgate — DCO
06. Netgate — Server Mode
07. Netgate — Server Tunnel Settings
08. Netgate — Server Cryptographic Settings
09. Netgate — Server Client Settings
10. Netgate — Advanced Client Settings
11. Netgate — Advanced Options
12. Netgate — Remote Access Wizard
13. Netgate — Site to Site SSL/TLS
14. Netgate — Site to Site with DCO
15. Netgate — Assigning OpenVPN Interfaces
16. Netgate — Troubleshooting OpenVPN
17. Netgate — OpenVPN Status
18. Netgate — VPNs and Firewall Rules
19. Netgate — OpenVPN Logs
20. Netgate — Custom Configuration Options

61 VPN → WireGuard

Tunnels · Peers · Settings · Status · criptografía · rutas · seguridad · diagnóstico

WireGuard es una VPN de capa 3 con configuración criptográfica sencilla y muy buen rendimiento. En pfSense Plus se administra mediante un paquete y cuatro vistas principales. Su aparente simplicidad puede ocultar decisiones críticas de rutas, prefijos Allowed IPs, reglas, interfaces asignadas y dirección de salida en Multi-WAN.

DISPONIBILIDAD DE LAS OPCIONES Las cuatro pestañas y los formularios Add Tunnel y Add Peer se explican junto con las referencias oficiales de Netgate. La disponibilidad de los controles debe contrastarse con la versión instalada de pfSense Plus y del paquete. La versión del paquete indicada en Status no identifica por sí sola la versión de pfSense Plus. Las topologías y direcciones de ejemplo son ficticias.

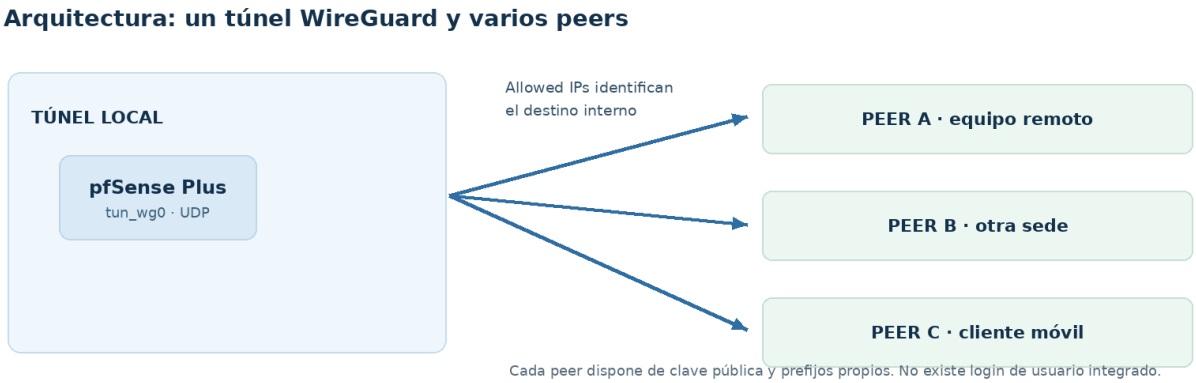


Figura 61.1. Relación funcional entre túnel y peers. Arquitectura conceptual sin información de ninguna instalación.

61.1. Objeto, alcance y ubicación de la funcionalidad

Ruta de administración: VPN → WireGuard. Pestañas: Tunnels, Peers, Settings y Status (esta última abre la vista Status → WireGuard). WireGuard se instala como paquete mediante System → Package Manager, cuando no está presente. Su disponibilidad y funciones específicas dependen de la versión compatible del paquete, del sistema y de FreeBSD.

Pestaña / ruta	Qué controla	Visto directamente
Tunnels	Instancias locales: puerto UDP, par de claves y direcciones.	Listado, columnas de túnel, aviso de vacío y Add Tunnel.
Peers	Contrapartes autorizadas de cada túnel.	Listado, Allowed IPs, Endpoint: Port y Add Peer.
Settings	Servicio, persistencia del paquete, resolución DNS y presentación de secretos.	Todos los controles generales de la captura.
Status	Actividad del túnel, tráfico y versión del paquete.	Columnas de estado y tabla Package Versions.

61.2. Qué es WireGuard y cómo funciona técnicamente

Un túnel WireGuard es una interfaz virtual IP. Cada extremo posee una clave privada local y una clave pública que se distribuye al otro lado. Los peers se reconocen criptográficamente mediante las claves públicas configuradas; WireGuard no incorpora formularios de usuario, contraseñas ni autorización por grupos como las soluciones que integran LDAP/RADIUS. La identidad operativa de un peer es su clave, no un nombre personal.

El protocolo intercambia mensajes de handshake para derivar material de cifrado de sesiones y encapsula los paquetes IP en datagramas UDP. Emplea un conjunto criptográfico deliberadamente reducido, que incluye Curve25519 para intercambio de claves y ChaCha20-Poly1305 para cifrado autenticado. La negociación no funciona como la elección libre de múltiples suites de IPsec u OpenVPN. Una clave precompartida adicional es opcional y complementa el intercambio asimétrico.

WireGuard no establece “sesiones de usuario” administrativas. Un peer puede estar definido y sin tráfico reciente; la presencia del túnel en la configuración o el estado no acredita por sí misma el acceso extremo a extremo. IPv4 e IPv6 son posibles en el interior del túnel, con configuración explícita de direcciones y rutas.

61.3. Diseños habituales y selección del esquema

Topología	Cómo se organiza	Ventajas / precauciones
Acceso remoto	Una instancia local y múltiples peers con endpoint dinámico.	Múltiples equipos; asignación estática individual de direcciones.
Sede a sede	Normalmente una instancia en cada sede con un peer remoto.	Facilita rutas estáticas y control por interfaz.
Hub and spoke	Una central con varios peers y sedes con uno.	Requiere Allowed IPs únicos y rutas de retorno.
VPN de salida	pfSense actúa como peer que inicia hacia un endpoint conocido.	Revisar política de rutas, gateway y NAT.
Enrutamiento dinámico	Una única contraparte por túnel y FRR cuando proceda.	Mayor flexibilidad; OSPF requiere vecino configurado.

CRITERIO DE DISEÑO WireGuard no dispone de un concepto rígido de cliente/servidor. Se habla de «cliente» cuando un peer inicia hacia un firewall con endpoint conocido, y de «servidor» por comodidad. Los pares son técnicamente peers.

61.4. Tunnels: lectura del listado y sus controles

Columna / elemento	Significado	Uso y cautela
Name	Identificador local de la interfaz/túnel.	Relacionar con tun_wgN; no equiparar a nombres DNS.
Description	Etiqueta administrativa.	Usar función, no secretos ni datos sensibles.
Public Key	Clave pública local anunciable a peers.	Puede compartirse; nunca divulgar la privada.
Address / Assignment	Direcciones del túnel o interfaz asignada.	Su configuración cambia al asignar la interfaz.
Listen Port	Puerto local UDP del túnel.	Diferenciar del puerto remoto del peer.
Peers	Peers asociados a esa instancia.	Un túnel puede transportar varios peers.
Actions	Acciones por fila cuando existe una instancia.	Editar/eliminar según iconos disponibles.
Add Tunnel	Abre el formulario de alta.	Requiere guardar y crear reglas/rutas necesarias.
Sin túneles	El listado muestra el mensaje de ausencia de túneles.	No existe conectividad WireGuard configurada en esa vista.

61.5. Tunnels: formulario Add / Edit Tunnel

Los siguientes controles se describen a partir de las opciones documentadas por Netgate. No aparecen abiertos en el listado de la captura; su disponibilidad debe verificarse en la versión del paquete instalada.

Control de alta	Comportamiento técnico	Operación segura
Enable	Activa o desactiva la instancia local.	Un túnel asignado a una interfaz no puede deshabilitarse mientras siga asignado.
Description	Nombre administrativo de la instancia.	Asociar a función y ámbito del túnel.

Control de alta	Comportamiento técnico	Operación segura
Listen Port	Puerto UDP local; referencia 51820 para el primero.	Cada túnel local debe disponer de su puerto; revisar WAN y NAT previo.
Interface Keys · Private Key	Secreto criptográfico local de la instancia.	Generar y guardar en el cortafuegos; proteger backups.
Public Key	Derivada de la clave privada; la GUI la presenta.	Copiar al peer remoto, verificar sin confundir sentidos.
Generate	Genera un nuevo par de claves.	Rotar obliga a actualizar todos los peers relacionados.
Copy	Copia la clave pública desde el formulario.	No confundir con secretos ni PSK.
Interface Addresses	IPv4/IPv6 del túnel cuando no está asignado.	Si se asigna, configurar dirección en la interfaz asignada.

El primer túnel propone UDP 51820 de manera predeterminada, y los adicionales deben usar puertos diferentes. La dirección de túnel puede pertenecer a un prefijo interno del plan de red. Para ejemplos ilustrativos se emplean bloques reservados para documentación: tales direcciones no deben desplegarse literalmente en una red operativa.

RIESGO DE OPERACIÓN Generar nuevas claves en un túnel activo invalida la confianza anterior hasta que cada contraparte reciba la clave pública actualizada. Planificar ventana y procedimiento de reversión.

61.6. Peers: explicación del listado principal

Columna / control	Qué representa	Interpretación
Description	Texto identificativo del peer.	Debe describir dispositivo o función.
Public key	Clave pública del peer remoto.	La clave privada correspondiente nunca sale de ese peer.
Tunnel	Instancia local que alojará al peer.	Una instancia puede compartir puerto entre varios peers.
Allowed IPs	Prefijos asociados al peer para enrutamiento criptográfico.	No crea rutas del SO; prevenir duplicidades.
Endpoint: Port	Destino IP/FQDN y puerto remoto, cuando se conoce.	No es el mismo concepto que Listen Port local.
Actions	Operaciones administrativas del registro.	Editar/deshabilitar/eliminar según contexto.
Add Peer	Abre alta de peer.	Seleccionar túnel, clave y Allowed IPs.

61.7. Peers: formulario Add / Edit Peer

Campo documentado	Qué ocurre	Comprobación
Enable	Activa el peer sin eliminarlo.	Deshabilitar impide intercambiar tráfico con ese peer.
Tunnel	Instancia WireGuard a la que se asocia.	Puede quedar Unassigned mientras se prepara.
Description	Etiqueta administrativa del extremo.	Registrar propietario técnico sin datos sensibles en ejemplos.
Dynamic Endpoint	Considera que la dirección remota puede variar.	Adecuado cuando un usuario viaja o usa LTE/5G.
Endpoint	IP o hostname de destino fijo.	Si no se conoce, dejar vacío; el remoto debe iniciar.
Endpoint Port	Puerto UDP remoto; por defecto 51820 si no se indica.	Se ignora si Endpoint está vacío.

Campo documentado	Qué ocurre	Comprobación
Keep Alive	Intervalo en segundos para conservar estados NAT.	Desactivado por defecto; usar solo si se justifica.
Public Key	Clave pública de la contraparte.	Debe emparejarse con su clave privada.
Pre-Shared Key	Secreto adicional opcional idéntico en los dos extremos.	Distribuir por canal seguro; no sustituye la clave pública.
Allowed IPs	Prefijos alcanzables mediante ese peer.	Excluir solapamientos y crear rutas aparte.

61.8. Claves, autenticación y protección de secretos

La clave privada es un secreto de alta sensibilidad: permite suplantar al peer correspondiente. La clave pública sirve para reconocerlo y puede intercambiarse. La pre-shared key, si se utiliza, añade un secreto simétrico que debe coincidir exactamente en ambos extremos. La protección adicional no evita que la mala gestión del archivo de configuración, del equipo o de sus respaldos comprometa las credenciales.

Cada cliente remoto debe contar con su par de claves independiente; reutilizar pares entre dispositivos dificulta atribución, revocación y enrutamiento. La baja de un dispositivo consiste en retirar o deshabilitar su entrada de peer y revocar operacionalmente su clave pública; tras robo o exposición, conviene rotar la identidad del peer afectado y cualquier secreto compartido que corresponda.

BACKUPS La opción Hide Secrets solamente oculta la visualización en la GUI. Netgate advierte que no cifra esos secretos dentro de config.xml; restringir acceso a copias de seguridad y almacenamiento fuera del equipo.

61.9. Allowed IPs: el concepto decisivo del protocolo

Allowed IPs cumple dos funciones relacionadas: identifica direcciones de origen aceptables para el peer y determina a qué clave pública se dirige un paquete cuando ya entra por una interfaz WireGuard. En una instancia multipar, un prefijo no puede pertenecer simultáneamente a peers distintos; los solapamientos pueden producir un peer operativo y otro sin correspondencia correcta. Las rutas de pfSense deben llevar primero el paquete hacia el túnel.

Caso	Allowed IPs local para ese peer	Consecuencia
Acceso remoto individual	192.0.2.10/32 (ejemplo documental).	Asociación a una dirección de peer.
Sede remota	192.0.2.10/32, 198.51.100.0/24 (solo ilustración).	Incluye host de túnel y prefijo de LAN remota.
Túnel de salida único	0.0.0.0/0 o ::/0.	Abarca todas las redes de esa familia: requiere política de rutas explícita.
Varios peers con 0.0.0.0/0	Configuración incompatible para asignación inequívoca.	Solo el último peer coincidente puede quedar correctamente asociado.
Prefijos de dos sedes iguales	Conflicto de redes superpuestas.	Diseñar traducción, segmentación o prefijos diferentes.

IMPORTANTE Los ejemplos con 192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24 y 2001:db8::/32 son direcciones reservadas para documentación y no son un plan operativo de direccionamiento. Sustituirlas por prefijos válidos y aprobados de la empresa.

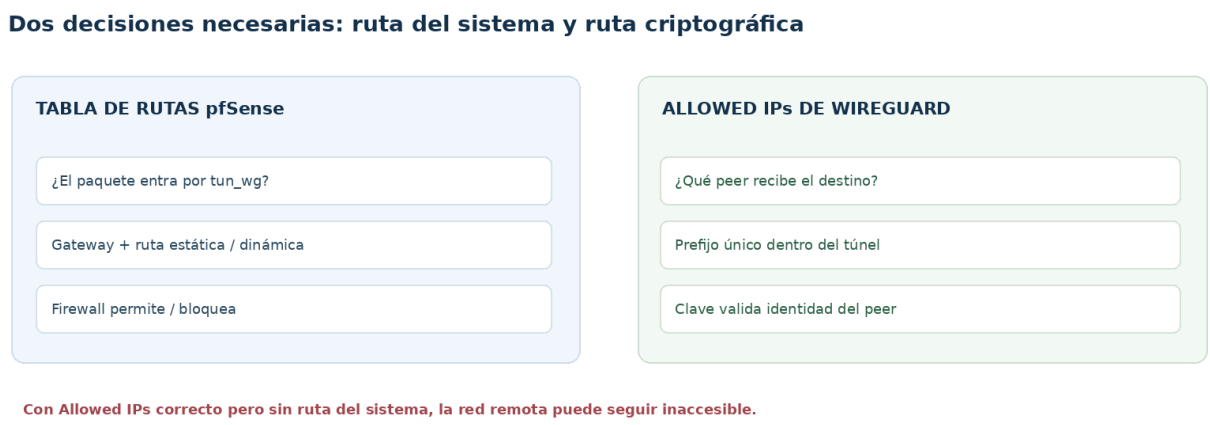


Figura 61.2. La tabla de rutas del cortafuegos y Allowed IPs resuelven problemas diferentes.

61.10. Settings: controles de General Settings visibles

Control	Valor visible / predeterminado indicado	Efecto y cautela
Enable WireGuard	En la imagen, desmarcado.	Activa el servicio; no lo desactiva si existen túneles asignados a interfaces.
Keep Configuration	En la imagen, marcado; descripción: predeterminado.	Conserva túneles, peers y ajustes ante instalación/desinstalación del paquete.
Endpoint Hostname Resolve Interval	300 segundos en la captura; predeterminado 300.	Reconsulta nombres de host remotos; 0 desactiva re-resolución.
Track System Resolve Interval	En la imagen, desmarcado.	Usa la periodicidad del sistema para alias FQDN cuando está activo.
Interface Group Membership	All Tunnels seleccionado en la captura; predeterminado.	Determina inclusión en el grupo WireGuard y filtrado por reglas grupales.

La lista de miembros del grupo puede utilizarse para excluir túneles asignados y evitar que reglas grupales más generales intercepten tráfico que necesita reglas con reply-to. El desplegable puede presentar valores adicionales según versión del paquete; All Tunnels es el valor visible confirmado y el comportamiento de pertenencia está documentado por Netgate.

61.11. Settings: User Interface Settings

Control	Captura	Comportamiento
Hide Secrets	Marcado.	Oculta claves privadas y precompartidas en la GUI; no cifra config.xml.
Hide Peers	Marcado; la propia pantalla lo señala como predeterminado.	Los peers aparecen inicialmente ocultos en la página Status.
Save	Botón disponible.	Guarda la configuración; revisar efecto sobre túneles activos.

Hide Peers solo altera la presentación del estado, no deshabilita peers ni reduce los permisos para administrar el paquete. Su descripción se toma del texto visible en la captura. No debe confundirse con un mecanismo de seguridad de acceso a la configuración.

61.12. Status: lectura de la pantalla de supervisión

Columna en Status	Significado operacional	Límite interpretativo
Tunnel / Description	Identidad y finalidad de la instancia.	No equivale a una conexión activa.

Columna en Status	Significado operacional	Límite interpretativo
Peers	Conjunto o recuento de peers asociados.	La presencia del registro no garantiza handshake.
Public Key	Identificador criptográfico público local.	No revela la clave privada.
Address / Assignment	Direcciones o referencia a interfaz asignada.	Confirmar IP y máscara en la pestaña correspondiente.
MTU	Unidad máxima de transmisión del túnel.	Desajustes pueden bloquear paquetes de gran tamaño.
Listen Port	Puerto UDP local.	La WAN debe permitir entradas desde remotos que inician.
RX / TX	Contadores de recepción/transmisión de datos.	No miden por sí solos calidad ni éxito de un servicio.
Package Versions	Nombre, Version, Comment.	La captura identifica paquete pfSense-pkg-WireGuard 0.2.13_4.

La captura carece de túneles configurados y por eso no aporta handshakes ni métricas de peers. En una instalación activa, la ausencia de un handshake reciente puede ser normal para peers inactivos sin tráfico; a la inversa, un intercambio de claves reciente no confirma permisos o rutas de aplicación. Deben correlacionarse estado, contadores, captura de paquetes y pruebas de extremo a extremo.

61.13. Firewall: distinguir transporte UDP y tráfico interno

WireGuard no crea automáticamente reglas de entrada WAN. Si un peer remoto inicia conexiones hacia el cortafuegos, abrir en Firewall → Rules → WAN el puerto UDP de escucha únicamente para los orígenes necesarios, cuando estos puedan restringirse. Después se necesitan reglas de paso en Firewall → Rules → WireGuard o en la pestaña de la interfaz WireGuard asignada, según diseño. Una regla WAN permite paquetes cifrados al servicio; no autoriza por sí sola acceso a las LAN.

Las reglas de grupo WireGuard se evalúan antes que las reglas de las interfaces individuales. Si una regla del grupo coincide antes, puede impedir el comportamiento deseado de reply-to de la interfaz asignada. Netgate aconseja filtrar en pestañas de interfaz asignada cuando es fundamental el retorno por el mismo túnel. NAT entrante y saliente requiere normalmente interfaz asignada y revisión de reglas específicas.



Figura 61.3. Diferencia entre permiso del protocolo UDP en la WAN y permiso del tráfico descifrado.

61.14. Interfaces asignadas, gateways, rutas y MTU

Para utilizar una instancia como interfaz propia: 1) fijar primero un gateway predeterminado de sistema conocido bajo System → Routing; 2) abrir Interfaces → Assignments y asignar tun_wgN; 3) activar OPTx, nombrarla y fijar tipo de dirección y MTU; 4) crear gateway hacia la IP del peer cuando el diseño lo requiera; 5) agregar rutas estáticas a redes remotas y reglas de firewall y NAT compatibles con el objetivo.

Una vez asignada, la dirección del túnel se configura desde la interfaz, no en Interface Addresses del formulario WireGuard. La MTU debe contemplar la encapsulación UDP/IP y el camino real. Netgate cita como referencias habituales 1420 para IPv4+IPv6 y 1440 en ciertos enlaces solo IPv4, pero no son

universales. Validar PMTU, fragmentación y tráfico de tamaños diferentes antes de establecer una cifra de producción.

ALTO RIESGO Netgate advierte que, si el default gateway del cortafuegos permanece en Automatic, al asignar WireGuard podría elegirse la interfaz del túnel como ruta por defecto. Fijarlo expresamente antes de asignar y validar el acceso administrativo después.

61.15. Procedimiento A — Acceso remoto seguro: un túnel y varios peers

01 Planificar una red virtual exclusiva, direcciones individuales, DNS y redes autorizadas; documentar el acceso esperado por recurso.

02 Instalar el paquete compatible y activar VPN → WireGuard → Settings → Enable. Mantener ocultación de secretos y backups protegidos.

03 Crear un túnel en Tunnels → Add Tunnel; activar, describir, elegir puerto UDP y generar su par de claves.

04 Configurar dirección virtual del túnel, siempre coherente con si la interfaz está asignada o no.

05 Crear un peer distinto por dispositivo: Public Key remota, Dynamic Endpoint y Allowed IPs con la IP virtual individual /32 o /128.

06 En el dispositivo remoto, establecer clave privada propia, IP del túnel, clave pública del firewall, Endpoint del firewall y AllowedIPs de destinos deseados.

07 Crear regla WAN UDP en el puerto correcto, más reglas restringidas de entrada WireGuard y, si procede, salida/NAT para acceso a Internet.

08 Conectar desde una red externa, observar paquete, handshake, RX/TX y acceso solo a los recursos aprobados; registrar pruebas y revocación.

DISEÑO DE SEGURIDAD Un perfil de acceso remoto con AllowedIPs = 0.0.0.0/0 en el cliente solicita enrutar todo IPv4 por la VPN. En split tunnel se indican solo prefijos necesarios; IPv6 se configura separadamente, no se da por protegido por el prefijo IPv4.

61.16. Procedimiento B — Site-to-site entre dos firewalls

01 Comprobar conectividad WAN, direccionamiento sin solapamientos y disponibilidad de ventana de mantenimiento.

02 Crear un túnel en cada pfSense con puertos conocidos y pares de claves diferentes; intercambiar solo claves públicas.

03 En cada extremo, crear el peer opuesto y establecer Endpoint y Endpoint Port correctos; Allowed IPs debe incluir el peer y redes remotas.

04 Antes de asignar WireGuard, fijar la ruta por defecto en System → Routing y validar que el firewall sigue alcanzando Internet.

05 Asignar tun_wgN como OPTx y configurar direcciones virtuales, gateway de peer y MTU apropiada.

06 Crear rutas estáticas recíprocas hacia LAN remotas por el gateway del túnel; comprobar vuelta de cada prefijo.

07 Autorizar UDP externo y el tráfico interno limitado al destino, origen y servicio necesarios.

08 Validar desde hosts de ambas sedes, incluyendo DNS, MTU, rutas, logs, ida y vuelta y caída programada.

La creación de rutas estáticas no se sustituye únicamente por Allowed IPs. Los prefijos deben existir tanto en el enrutamiento del SO como en las asociaciones de peers, y las ACL deben permitir el paso de ida y la respuesta.

61.17. Procedimiento C — Hub and spoke y segregación por peer

En un concentrador con varios peers, asignar a cada delegación su dirección de túnel y los prefijos de sus redes. No replicar el mismo /0 ni la misma subred entre peers de un mismo túnel. En los spokes, Allowed IPs hacia el concentrador puede abarcar los prefijos de otras sedes si se desea interconexión; además hay que crear rutas, permitir tráfico entre peers y definir las políticas de aislamiento. Para visibilidad y retorno estricto, evaluar túneles separados o interfaces asignadas con reglas por túnel.

61.18. Procedimiento D — Salida completa y split tunnel

Decisión	Qué se configura	Qué se comprueba
Split tunnel	Cliente: AllowedIPs solamente a redes de trabajo.	Ruta de Internet original conservada y DNS adecuado.
Full tunnel IPv4	Cliente: 0.0.0.0/0 al peer, y política de salida en pfSense.	Ruta por VPN, NAT WAN y fugas DNS.
Full tunnel IPv6	Cliente: ::/0 y diseño IPv6 completo.	Firewall/routing IPv6 y ausencia de fugas.
PfSense como cliente upstream	Rutas y gateways de salida al proveedor; selección del peer único.	No sustituir por accidente default gateway de administración.

61.19. Rendimiento, MTU, DNS, NAT y keepalive

El impacto de rendimiento depende de CPU, ancho de banda, procesamiento de paquetes, MTU, colas y condiciones WAN. La elección del puerto 51820 no acelera por sí sola la conexión; lo relevante es consistencia, reglas y ausencia de bloqueos del operador. Un peer tras NAT puede necesitar Persistent Keepalive periódico; el campo Keep Alive está desactivado de manera predeterminada y debe ajustarse solo si los estados caducan antes de que exista tráfico.

Si se utiliza un endpoint FQDN, el intervalo de re-resolución determina cuándo se incorporan cambios de dirección. Resolución DNS no es lo mismo que DNS utilizado por el cliente para consultar recursos internos. La salida por NAT debe revisarse en ambas direcciones: reglas Outbound NAT en WAN para salida a Internet de peers, y NAT de interfaces asignadas solo cuando el diseño lo exija.

61.20. Multi-WAN: llegada, salida y dirección de origen

Netgate documenta que WireGuard puede recibir en diferentes direcciones WAN y responder desde la dirección a la que el remoto conectó, cuando resulta posible. Sin embargo, el tráfico que el firewall inicia hacia un endpoint suele seguir la ruta por defecto, salvo que la tabla de rutas disponga otro camino. Si se pretende salida por WAN secundaria hacia un peer estático, hay que estudiar una ruta explícita al endpoint por el gateway correcto.

En entornos con endpoints que cambian por DNS, rutas estáticas por IP pueden quedar obsoletas tras un cambio de dirección. Una arquitectura Multi-WAN profesional debe probar fallos reales de WAN, re-resolución, transición entre rutas, puertos, reglas y recuperación, sin asumir conmutación transparente de todas las sesiones.

61.21. Alta disponibilidad y CARP

La implementación puede mostrar comportamientos inesperados si cambia el propietario de una dirección virtual CARP. Una conexión activa puede seguir asociada a una dirección concreta del nodo anterior si el peer aprende un endpoint distinto durante mantenimiento; la NAT de salida tampoco garantiza transferencia automática de los estados al nodo de respaldo. En configuraciones HA es preferible diseñar quién inicia el tráfico y probar conmutación y retorno en laboratorio antes de despliegue productivo.

> **DISPONIBILIDAD** No declarar alta disponibilidad WireGuard validada únicamente porque CARP conmuta o porque una configuración ha sido sincronizada. Probar desplazamiento de VIP, fuente del tráfico, nuevos handshakes y reconvergencia real.

61.22. Rutas dinámicas: FRR, BGP y OSPF

Netgate contempla enrutamiento dinámico con WireGuard, ensayado con FRR, siempre teniendo presente que un túnel con un solo peer admite mejor el intercambio de prefijos variables. BGP puede utilizar la dirección de túnel del vecino, mientras que OSPF necesita modo Non-Broadcast y vecino definido manualmente al no disponer del descubrimiento multicast habitual. La existencia del protocolo de rutas no elimina la necesidad de políticas de filtrado y control de anuncios.

61.23. Monitorización y validación reproducible

01 Confirmar VPN → WireGuard → Settings → Enable y que el túnel y el peer figuran habilitados.

02 Revisar IP de endpoint y su resolución DNS, puerto UDP remoto y reglas de tráfico entrante de WAN.

03 Consultar Status → WireGuard: instancia, peers, direcciones, MTU, Listen Port, RX y TX; ampliar el estado del peer cuando exista.

04 Iniciar tráfico desde un extremo y comprobar si hay handshake y crecen los contadores adecuados; distinguir datos de control y útiles.

05 Verificar tabla de rutas, gateway de peer, Allowed IPs, reglas de grupo/interfaz y posibles NAT.

06 Probar acceso a un servicio concreto por IP y por nombre, luego desde el extremo inverso, registrando hora/origen/destino.

07 Probar pausa, reconexión, rotación controlada de DNS si procede y tolerancia a cambios de red del cliente.



Figura 61.4. Orden de las comprobaciones para evitar atribuir un fallo de routing a un fallo de criptografía.

61.24. Diagnóstico de incidencias frecuentes

Síntoma	Causas frecuentes	Acciones de verificación
Sin intercambio inicial	UDP WAN bloqueado; endpoint/puerto/clave incorrectos.	Captura en WAN; DNS; public keys y PSK coincidentes.
Handshake y sin tráfico	Allowed IPs mal definidos, ruta ausente o firewall.	Rutas de SO, tablas de firewall y destino real.
Solo funciona un peer	Allowed IPs superpuestos o claves reutilizadas.	Una clave y prefijos únicos por peer.
Responde una WAN inesperada	Ruta por defecto dirige el paquete iniciado.	Ruta al endpoint por gateway deseado.
Pequeños paquetes sí, grandes no	MTU/PMTU inadecuada.	Pruebas por tamaños; ajustar MTU y analizar encapsulación.
Reconecta tras cambiar IP móvil	Endpoint dinámico/roaming normal; NAT expira.	Handshake, keepalive y reglas del operador.
No resuelve nombres internos	DNS del cliente o rutas a DNS no configuradas.	IP directa; DNS alcanzable y split DNS.
No llega Internet por full tunnel	Falta NAT o permiso WAN, ruta salida o IPv6.	Estados, outbound NAT, reglas y gateway.
No permite desactivar servicio	Existe un túnel asignado a interfaz.	Retirar o desactivar asignación con plan de cambio.
HA falla al conmutar	CARP VIP y origen de respuesta inconsistentes.	Capturas en ambos nodos y pruebas postfailover.

61.25. Seguridad empresarial y política de operación

Mantener inventario de cada clave pública, ámbito de Allowed IPs y fecha de alta; proteger claves privadas y PSK; restringir lectura de config.xml y respaldos; evitar reglas any-any como configuración final; registrar

las razones por las que se habilita salida completa o roaming; eliminar peers retirados; revisar interfaces asignadas tras cambios de gateway y comprobar alcance real de las ACL. El uso del protocolo no sustituye controles de identidad del equipo, actualizaciones, protección de endpoints ni procedimientos de respuesta ante incidentes.

La rotación de claves debe tratarse como cambio coordinado. Si se rota la clave privada del túnel local, todos los peers deben recibir su nueva clave pública. Si se rota la clave de un cliente, actualizar exclusivamente la entrada correspondiente. Cuando existe sospecha de compromiso, deshabilitar el peer y revisar tanto históricos de acceso como inventario de dispositivos autorizados.

61.26. Pruebas de aceptación y plan de reversión

Prueba	Criterio de éxito	Evidencia a conservar
Handshake bajo carga ligera	Aparece actividad coherente al enviar tráfico.	Hora y estado sin publicar claves ni endpoints reales.
Tráfico entre redes	Servicios concretos responden desde orígenes autorizados.	Origen/destino ficticios o redactados en informes.
Segmentación	Los destinos prohibidos siguen bloqueados.	Reglas y resultado de denegación.
Rutas de retorno	La respuesta utiliza túnel/interfaz previstos.	Capturas anonimizadas y tabla de rutas.
WAN secundaria / failover	Conserva o recupera conectividad según objetivo acordado.	Tiempos observados y acciones realizadas.
Reversión	Se restablece configuración previa conocida.	Backup protegido, cambio documentado y validación.

61.27. Glosario de términos

Concepto	Definición operativa
Peer	Extremo remoto identificado por clave pública.
Tunnel	Instancia local WireGuard y su interfaz virtual.
Allowed IPs	Prefijos válidos para un peer y correspondencia de routing criptográfico.
Endpoint	IP/FQDN y puerto UDP de la contraparte.
Handshake	Intercambio criptográfico para establecer claves de tráfico.
Keepalive	Datagrama periódico que ayuda a mantener estados NAT.
PSK	Pre-shared key opcional, secreto adicional compartido.
MTU	Tamaño máximo de paquete transportable sin superar el límite configurado.
Cryptokey routing	Selección del peer de destino a partir de claves y prefijos permitidos.
reply-to	Comportamiento pf que favorece respuesta por la misma interfaz del flujo entrante.

61.28. Referencias oficiales verificables

01. **Netgate — WireGuard overview**	**02.** **Netgate — WireGuard Settings (package, tunnel, peer)**
03. Netgate — Design Considerations	**04.** Netgate — WireGuard Limitations
05. Netgate — Configure a WireGuard Tunnel	**06.** Netgate — Assign a WireGuard Interface
07. Netgate — WireGuard and Rules / NAT	**08.** Netgate — WireGuard Routing

01. Netgate — WireGuard overview	**02. Netgate — WireGuard Settings (package, tunnel, peer)**
09. Netgate — Remote Access VPN configuration	**10.** Netgate — Site-to-Site VPN configuration
11. Netgate — Site-to-Multisite configuration	**12.** Netgate — WireGuard VPN Client configuration
13. Netgate — Changing Credentials and Keys	**14.** Netgate — VPNs and Firewall Rules

Nota de versión: la documentación enlazada corresponde a la versión «latest» de Netgate consultada durante la preparación editorial. Los valores exactos de todas las opciones adicionales se deben comprobar contra la versión efectiva del paquete y de pfSense Plus desplegada.

Parte VI Status

62 Status → Introducción general

Supervisión · continuidad de servicio · registros · tráfico · DHCP/DNS · VPN · diagnóstico operacional

La sección Status de pfSense Plus reúne vistas de supervisión, registros, estadísticas y, en determinados apartados, acciones operativas de mantenimiento. Constituye el punto de partida para confirmar qué está ocurriendo en el cortafuegos, qué servicios responden y dónde buscar evidencias antes de cambiar una configuración.

A diferencia de los menús dedicados a configurar reglas, interfaces o túneles, Status permite analizar resultados observables. Sin embargo, no todas sus acciones son de solo lectura: algunas pueden reiniciar demonios, vaciar concesiones, modificar el papel de un nodo CARP o interrumpir sesiones. Por ello, supervisión y administración deben separarse en procedimientos controlados.

ÁMBITO DE ESTE CAPÍTULO Se presentan los 19 accesos visibles del menú Status y sus relaciones funcionales. Las pantallas específicas de cada opción se desarrollan en los capítulos de la sección. La presencia de opciones, controles y paquetes puede variar según versión y servicios instalados.

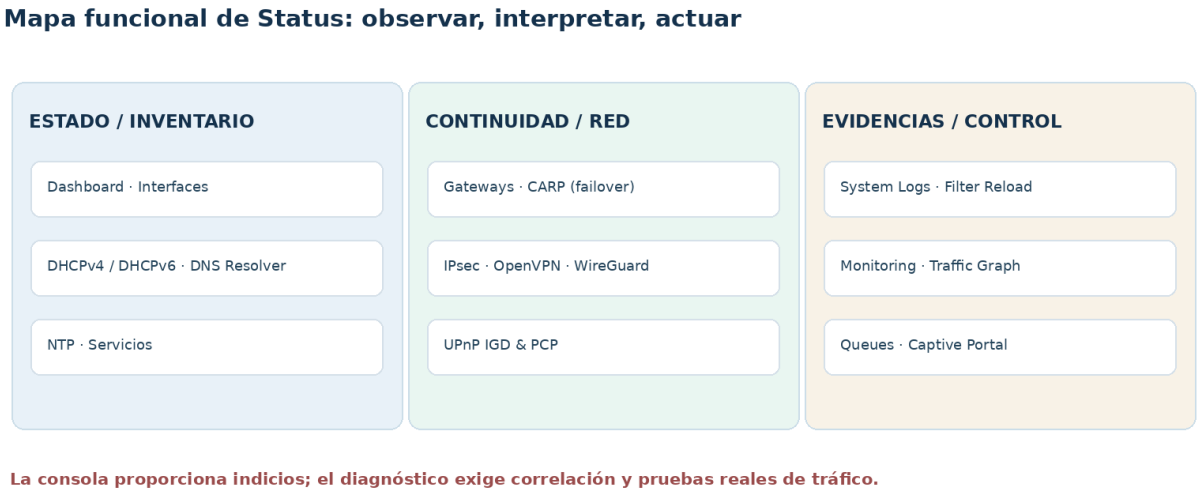


Figura 62.1. Clasificación funcional de las entradas de Status, con nombres neutros y arquitectura conceptual.

62.1. Ubicación, propósito y límites de la sección

Ruta: menú superior Status. En un entorno de administración, comenzar aquí permite separar síntomas de hipótesis: un usuario que no navega puede tener una concesión DHCP válida y un enlace físico activo, pero un problema de DNS; un túnel puede indicar estado conectado y no disponer de la ruta de retorno o del permiso de firewall necesario.

La información mostrada depende del componente: algunas vistas presentan una instantánea, otras gráficos históricos a partir de RRD y otras registros de eventos con hora. La ausencia de filas no siempre constituye un fallo: puede no existir una configuración activa o no haberse generado tráfico todavía. De igual manera, una luz verde o un proceso Running no certifica la funcionalidad completa de la aplicación empresarial que depende de él.

62.2. Mapa íntegro del menú Status

N.º	Entrada	Información principal	Naturaleza
01	Captive Portal	Sesiones de portal cautivo y vales, si se utilizan.	Estado + acciones
02	CARP (failover)	Roles de IP virtuales, mantenimiento HA y pfsync.	Estado + alto riesgo

N.º	Entrada	Información principal	Naturaleza
03	Dashboard	Widgets y visión global del cortafuegos.	Resumen
04	DHCP Leases	Concesiones IPv4 y acciones asociadas.	Estado + acciones
05	DHCPv6 Leases	Concesiones IPv6, identificadores y delegaciones.	Estado + acciones
06	DNS Resolver	Caché de infraestructura y estadísticas Unbound.	Estado
07	Filter Reload	Progreso de recarga de reglas y sincronización.	Estado + alto riesgo
08	Gateways	Estado de gateways, grupos y calidad del enlace.	Estado
09	Interfaces	Estado físico/lógico y contadores de interfaces.	Estado
10	IPsec	IKE SA, CHILD SA y túneles.	Estado + acciones
11	Monitoring	Gráficas históricas RRD de recursos y red.	Serie temporal
12	NTP	Pares y sincronización del reloj.	Estado
13	OpenVPN	Instancias, clientes y sesiones.	Estado + acciones
14	Queues	Colas ALTQ y descartes cuando corresponda.	Estado
15	Services	Demonios locales y de paquetes.	Estado + alto riesgo
16	System Logs	Eventos del sistema, firewall y subsistemas.	Evidencia
17	Traffic Graph	Caudal actual de una interfaz.	Tiempo real
18	UPnP IGD & PCP	Redirecciones dinámicas de puertos activas.	Estado
19	WireGuard	Túneles, pares y contadores del paquete.	Estado condicional

Esta clasificación es orientativa: cada pantalla puede incluir varios mecanismos y controles cuya disponibilidad depende de la versión, de los permisos de usuario y de la configuración vigente. La entrada WireGuard está asociada al paquete WireGuard, que no debe confundirse con un componente obligatorio de cualquier instalación.

62.3. El significado real de los indicadores

Indicador	Qué aporta	Qué NO demuestra por sí solo
Running / Stopped	El daemon se ejecuta o no se ejecuta.	Que la cadena completa de resolución, ruta, permisos y aplicación funcione.
Online / Offline	Resultado del criterio de monitorización configurado.	Que todos los destinos de Internet sean alcanzables.
MASTER / BACKUP	Propietario efectivo de una VIP CARP frente a su respaldo.	Que pfsync y todas las rutas de aplicaciones estén sanas.

Indicador	Qué aporta	Qué NO demuestra por sí solo
Activo / expirado (DHCP)	Situación de una concesión en la base DHCP.	Que el dispositivo esté conectado y utilice ese servicio.
VPN conectada	Se negoció o mantiene asociación/túnel.	Que tráfico interno, DNS y puertos de aplicación estén permitidos.
RX/TX en aumento	Se reciben o transmiten bytes/paquetes.	Que no existan pérdidas, errores o retransmisiones.
Gráfico sin datos	No hay puntos disponibles en ese periodo/métrica.	Que necesariamente haya fallo o ausencia de tráfico.

REGLA DE INTERPRETACIÓN Siempre diferenciar señal, hipótesis y prueba. Una alarma muestra que se ha cruzado un criterio; no identifica automáticamente la causa.

62.4. Dashboard: primera evaluación del firewall

Ruta: Status → Dashboard. Es el acceso más rápido para revisar widgets del sistema, interfaces, servicios, recursos, gateways y otros componentes habilitados. Los widgets disponibles y su disposición varían entre versiones y módulos. Conviene mantener una selección suficiente para el trabajo operativo sin convertir la pantalla de inicio en una acumulación difícil de leer.

Interpretación: verificar estado del sistema, consumo de recursos, memoria y almacenamiento, interfaces y alertas de gateways. Si aparecen valores fuera del patrón habitual, ir a la página especializada. Un uso de CPU alto durante un instante no justifica por sí solo reiniciar; es más útil correlacionarlo con throughput, logs y evolución temporal.

62.5. Estado de red y disponibilidad: Interfaces, Gateways y CARP

Status → Interfaces presenta la situación de las interfaces configuradas, la capa de enlace, direcciones y contadores según hardware y configuración. Una WAN con enlace UP puede seguir sin acceso a su gateway, y un error de negociación de velocidad/dúplex puede manifestarse como pérdida y retransmisión. Examinar flaps, errores, paquetes descartados y el estado del enlace junto con los eventos de sistema.

Status → Gateways observa monitorización de gateways individuales y grupos Multi-WAN. RTT, pérdida de paquetes y estados ONLINE/ALARM dependen del destino monitorizado y de umbrales; que el monitor remoto no conteste ICMP puede producir una alarma sin pérdida total de conectividad. Contrastarlo con rutas vigentes, DNS y pruebas hacia destinos independientes. El monitor puede ser distinto de la IP del gateway.

Status → CARP (failover) informa del papel MASTER, BACKUP o estados de inicialización de las IP virtuales de un clúster de alta disponibilidad. También permite poner el nodo en mantenimiento, habilitar/deshabilitar CARP temporalmente y, en circunstancias específicas, restablecer la democión. Operaciones de este tipo pueden producir un cambio de nodo activo y cortar sesiones si pfsync o la red de HA no funcionan correctamente.

ALTO RIESGO CARP Antes de activar un modo de mantenimiento o alterar la democión: consultar ambos nodos, confirmar conectividad de interfaces y sincronización, comunicar la intervención y establecer un método de reversión. No colocar simultáneamente ambos nodos en mantenimiento.

62.6. Estado de direccionamiento y nombres: DHCP, DHCPv6 y DNS

Status → DHCP Leases lista concesiones IPv4 del servidor local y admite diversas operaciones, incluidas asociaciones estáticas y acciones de Wake-on-LAN. El diseño exacto depende del backend DHCP, por ejemplo Kea frente a ISC. El estado «offline» basado en tablas de vecindad no prueba que el equipo esté apagado: quizá no haya intercambiado tráfico recientemente con el cortafuegos.

Status → DHCPv6 Leases utiliza DUID e IAID para identificar las concesiones, puede presentar delegaciones de prefijos y, cuando corresponde, datos de alta disponibilidad. Los dispositivos configurados exclusivamente mediante SLAAC no aparecen necesariamente en el inventario DHCPv6, por lo que un listado vacío no demuestra ausencia de clientes IPv6.

Status → DNS Resolver muestra información de caché de infraestructura de Unbound y datos sobre servidores consultados. Su interpretación varía según trabaje como resolvedor recursivo o con reenvío. Un

proceso Unbound en marcha no implica que todos los dominios se resuelvan: pueden fallar upstream, DNSSEC, zonas locales, políticas o conectividad hacia los servidores necesarios.

Síntoma	Primera pantalla	Contrastación necesaria
Cliente no recibe IPv4	DHCP Leases	VLAN, scope, asignación real y logs DHCP.
Cliente IPv6 ausente	DHCPv6 Leases	Comprobar SLAAC, RA y existencia de DHCPv6.
Nombre interno no resuelve	DNS Resolver	Consultar resolución específica, override y registros Unbound.
Pool DHCP cerca del límite	DHCP Leases	Calcular utilización de pool y concesiones expiradas.
Fallo DNS intermitente	Monitoring + System Logs	Comparar tiempo, proveedor upstream y transacciones.

62.7. Servicios, registros y recarga del filtro

Status → Services muestra procesos base y de paquetes en estado Running o Stopped, con acciones de arranque, parada y reinicio cuando corresponda. «Stopped» puede ser normal si el servicio no está habilitado o su uso es intermitente; contrastar configuración deseada y dependencias antes de intervenir. Reiniciar OpenVPN, DNS, DHCP o un servicio de HA sin plan previo podría provocar pérdida de acceso.

Status → System Logs constituye la fuente de evidencia cronológica. Existen apartados de sistema, firewall, DHCP, resolución de nombres, VPN y otros demonios. Buscar por rango horario y correlación de errores; revisar zona horaria y sincronización NTP. Los registros rotan y no son un repositorio forense permanente: para retención, auditoría y búsquedas centralizadas se recomienda syslog remoto protegido y políticas de conservación.

Status → Filter Reload refleja el progreso de recarga del filtro, que puede concluir con «Done.». Ofrece un mecanismo de recarga manual y, en clústeres configurados, sincronización forzada de configuración XMLRPC. Estas operaciones no son equivalentes a consultar el estado y pueden alterar reglas activas o propagar cambios; examinar tareas pendientes y errores antes de pulsar controles.

> **ACCIONES DE IMPACTO** Borrar toda la base de concesiones DHCP, detener un servicio, reiniciar VPN, forzar Filter Reload o disparar sincronización XMLRPC no son pruebas de diagnóstico inocuas. Exigir autorización, ventana de cambio y seguimiento posterior.

62.8. Supervisión de VPN: IPsec, OpenVPN y WireGuard

Status → IPsec presenta asociaciones de seguridad IKE y CHILD_SA, descripciones y contadores. La vista permite distinguir problema de negociación (fase de control) frente a un SA válido sin tráfico interno. Cuando un túnel parece «conectado» pero la aplicación falla, revisar selectores, tabla de rutas, reglas IPsec/VTI, NAT y las redes declaradas en ambos extremos.

Status → OpenVPN muestra estado de instancias cliente/servidor y, para servidores de acceso remoto, sesiones y datos de conexiones. Una instancia en marcha no significa que todos sus usuarios estén conectados ni que un cliente concreto tenga acceso a recursos. Relacionar el usuario/CN con los registros, las rutas empujadas, la configuración de split tunneling y la interfaz asociada.

Status → WireGuard corresponde a la supervisión del paquete WireGuard, si está instalado. Puede mostrar túneles, peers y contadores RX/TX; los estados de handshake no son equivalentes a una sesión de usuario autenticada. Un peer puede estar inactivo legítimamente hasta que existe tráfico; comprobar claves, endpoints, Allowed IPs, rutas y reglas, evitando deducir fallo solo por inactividad.

Tecnología	Señal de plano de control	Segunda prueba obligada
IPsec	IKE SA establecida / CHILD_SA presente.	Tráfico por los selectores o VTI + rutas y firewall.
OpenVPN	Instancia activa y cliente conectado.	Dirección de túnel, ruta real, DNS y recurso final.
WireGuard	Peer configurado, handshake o contadores.	Envío/recepción del prefijo permitido y ruta de retorno.

62.9. Observabilidad del tráfico: Monitoring, Traffic Graph y Queues

Status → Monitoring utiliza registros RRD y permite examinar tendencias de tráfico, recursos, calidad del enlace y, si se han configurado, datos de colas o VPN. El promedio por intervalo puede disimular picos breves; evaluar el periodo elegido antes de concluir que no hubo saturación. La comparación simultánea de tráfico, pérdidas y CPU suele ofrecer mayor valor que una métrica aislada.

Status → Traffic Graph ofrece una vista dinámica del tráfico que circula por una interfaz seleccionada, útil para apreciar variaciones en ese momento. La unidad, dirección y punto de medición deben anotarse: un incremento en RX en WAN no equivale a tráfico útil entregado por LAN. Este gráfico no sustituye el histórico de RRD ni una captura de paquetes para identificar protocolos.

Status → Queues representa el estado de las colas de tráfico ALTQ cuando existe una política de shaping compatible. Presenta utilización, paquetes/s y descartes. Los descartes pueden ser resultado esperado de priorización, por lo que es fundamental relacionarlos con congestión, latencia de aplicación y diseño del plan de QoS. No asumir que una cola vacía es una avería.

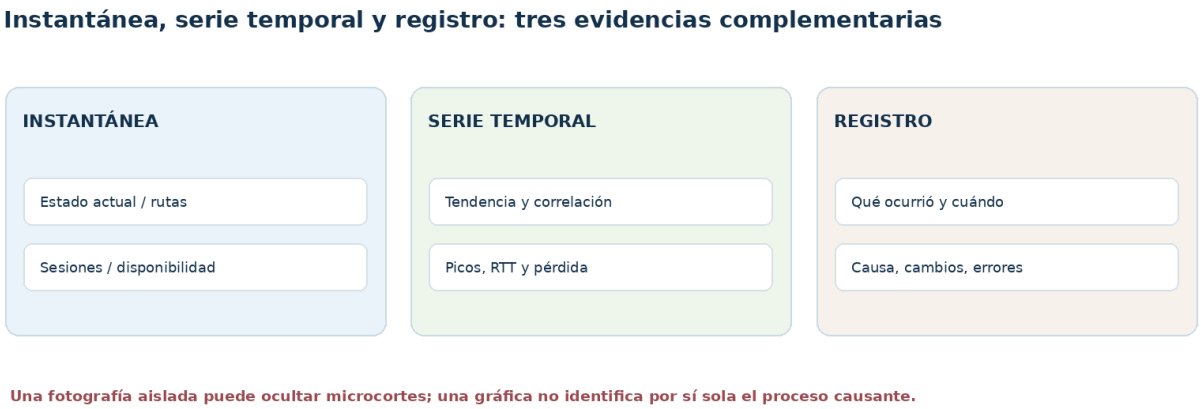


Figura 62.2. Las evidencias instantáneas, históricas y cronológicas responden preguntas diferentes.

62.10. Portal cautivo, UPnP y otras observaciones dependientes de servicios

Status → Captive Portal lista sesiones cuando existen zonas de portal cautivo habilitadas. Su vista de usuarios activos puede incluir IP, MAC, identificador, comienzo de sesión y acciones para expulsar un cliente. Estas acciones son relevantes para asistencia a invitados o depuración de vales, pero pueden cortar el acceso de una persona en mitad de una operación.

Status → UPnP IGD & PCP permite observar asignaciones dinámicas de puertos producidas por los clientes autorizados. Una regla publicada por este servicio puede exponer un dispositivo interno al tráfico entrante. La revisión periódica debe comparar solicitudes vigentes con ACL de UPnP, interfaces autorizadas y necesidad real del servicio; comprobar la redirección desde un origen externo controlado.

No todos los entornos muestran todas las entradas: algunas dependen de paquetes instalados, interfaces asignadas, hardware, permisos o versión concreta. Las rutas del menú documentan el producto, no garantizan un conjunto idéntico de controles en todas las versiones de pfSense Plus.

62.11. Clasificación por nivel de riesgo operativo

Nivel	Acciones o consultas	Procedimiento de control
Bajo	Leer estados, logs y gráficos; consultar detalles.	Registrar hora y contexto; evitar divulgar identificadores al compartir evidencias.
Medio	Cambiar periodo gráfico, aplicar filtros, visualizar concesiones.	Verificar alcance y efecto, conservar capturas anonimizadas si son necesarias.
Alto	Terminar sesión de portal, parar/reiniciar un daemon o VPN.	Autorización, evaluación de dependencias y supervisión poscambio.

Nivel	Acciones o consultas	Procedimiento de control
Crítico	Forzar failover CARP, recargar filtro en producción, sincronizar HA, vaciar DHCP.	Ventana formal, backup, acceso de emergencia y plan de reversión.

La criticidad depende del contexto. Parar un servicio poco usado en un laboratorio puede ser inocuo, mientras que reiniciar el mismo servicio en un cortafuegos central puede generar una interrupción relevante. Los permisos RBAC deben alinearse con estas diferencias.

62.12. Método universal de diagnóstico: contexto, evidencia y validación



Figura 62.3. Secuencia operativa de diagnóstico sin cambios prematuros en producción.

01 Delimitar el impacto: una sede, una VLAN, varios usuarios o toda la organización. Registrar inicio, duración y gravedad.

02 Comprobar Dashboard, Interfaces y Gateways: descartar cortes físicos, cambios de ruta y alarmas de monitorización.

03 Consultar Services y System Logs durante el periodo afectado; confirmar hora correcta y correlación del evento.

04 Seleccionar el subsistema: DHCP, DNS, VPN, CARP, colas o sesiones según el síntoma y el alcance.

05 Reproducir mediante una prueba controlada: resolución de un nombre, traceroute, ping de destino adecuado, acceso de aplicación o captura de paquetes.

06 Si es necesario modificar, documentar hipótesis, impacto, copia previa, responsable y reversión; ejecutar el menor cambio posible.

07 Confirmar recuperación con la misma prueba inicial, comparar métricas y registrar el resultado de la intervención.

62.13. Ejemplos prácticos empresariales: diagnóstico por síntomas

Incidencia	Secuencia de comprobación	Decisión guiada por evidencia
Navegación intermitente desde varias redes	Interfaces → Gateways → Monitoring → System Logs → DNS.	No cambiar NAT si hay pérdida física o alarmas de gateway reproducibles.
Una sede VPN desconectada	Gateways → IPsec/OpenVPN/WireGuard → System Logs.	Diferenciar fallo de handshake, ruta o filtrado.
Clientes sin red al arrancar	DHCP Leases → Services → DHCP logs → VLAN/Interfaces.	No vaciar todas las concesiones como primera medida.
DNS lento con WAN correcta	DNS Resolver → Monitoring → System Logs.	Revisar DNSSEC/reenvío/upstream antes de sustituir configuración.
Caída parcial tras mantenimiento HA	CARP → Interfaces → Filter Reload → System Logs.	Verificar MASTER/BACKUP, pfsync y sincronización sin forzar ambos nodos.

Incidencia	Secuencia de comprobación	Decisión guiada por evidencia
Llamadas con audio degradado	Monitoring → Queues → Traffic Graph → Interfaces.	Correlacionar congestión, descartes y priorización, no solo bitrate.

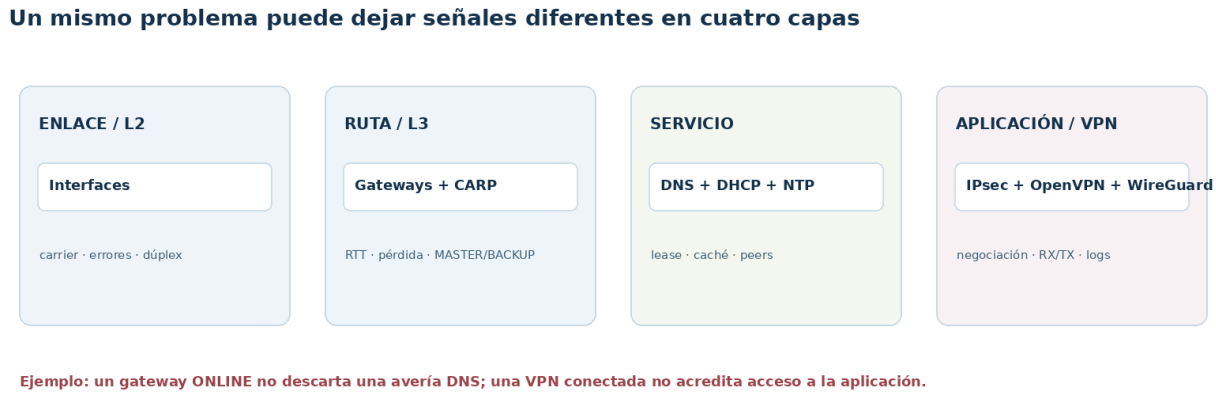


Figura 62.4. Relación entre señales físicas, de enrutamiento, de servicios y de aplicación.

62.14. Procedimiento A: comprobación rutinaria de salud operativa

01 Abrir Status → Dashboard y anotar fecha/hora, uptime y estado general de los widgets seleccionados.

02 Verificar Status → Interfaces y → Gateways; comparar pérdida, latencia y enlaces con la línea base habitual.

03 Revisar Status → Services en los demonios críticos definidos para ese firewall, no todos sin distinción.

04 Examinar Status → System Logs buscando errores nuevos, flapping o eventos inusuales.

05 Contrastar Status → Monitoring con el mismo periodo de jornadas anteriores y documentar desviaciones.

06 Conservar un resumen breve de resultados; no intervenir en estados normales por indicadores aislados.

62.15. Procedimiento B: verificación de un cambio de reglas

01 Antes del cambio, registrar flujo permitido/bloqueado, interfaz de entrada y prueba de conectividad reproducible.

02 Aplicar únicamente la configuración aprobada en el apartado Firewall correspondiente.

03 Consultar Status → Filter Reload hasta que no haya tareas pendientes o errores de recarga.

04 Verificar el flujo real desde origen y destino; consultar Status → System Logs, apartado Firewall, si se registra la regla.

05 Si el tráfico sigue sin funcionar, revisar reglas flotantes, NAT, estados y rutas sin forzar recargas repetidas.

06 Revertir si existe impacto no previsto y validar de nuevo la conectividad administrativa.

62.16. Procedimiento C: supervisión de alta disponibilidad y Multi-WAN

01 Comparar en cada nodo Status → CARP: los estados esperados de VIP son MASTER en uno y BACKUP en el otro.

02 Verificar enlaces físicos, rutas, IP monitorizada de cada gateway y estado de grupos en Status → Gateways.

03 Correlacionar eventos de fallos con System Logs; revisar cambios en RTT, loss, pfsync o CARP.

04 Antes de una conmutación deliberada, garantizar vía de administración alternativa y alcance de la ventana.

05 Realizar una conmutación controlada solamente en plan aprobado y comprobar servicios reales desde clientes.

06 Documentar retorno a estado normal, sesiones afectadas y tiempos de recuperación observados.

62.17. Procedimiento D: observabilidad de una VPN en producción

01 Identificar tecnología, peer/instancia, red origen, destino esperado y servicio de aplicación.

02 Comprobar estado específico en Status → IPsec, OpenVPN o WireGuard y observar contadores/handshake según el caso.

03 Verificar Status → Gateways e Interfaces en el transporte WAN; revisar logs VPN con marca temporal.

04 Comprobar rutas a prefijos remotos, reglas y NAT; no asumir que túnel UP equivale a acceso autorizado.

05 Probar desde un host autorizado acceso a la IP destino, resolución DNS y puerto de aplicación relevante.

06 Registrar evidencia previa/posterior y elevar el incidente si la caída requiere intervención en el peer externo.

62.18. Gobierno operativo: retención, alertas, acceso y responsabilidad

Para supervisar una infraestructura distribuida, la interfaz WebGUI debe complementarse con monitorización externa apropiada: recogida SNMP cuando esté habilitada y securizada, syslog central con cifrado de transporte cuando esté soportado, métricas de tiempo de respuesta y comprobaciones sintéticas de servicios. pfSense no garantiza alertas proactivas para cada elemento mostrado en Status; una consola que nadie consulta no es por sí sola un sistema de alerta.

Las capturas o exports operativos pueden contener usuarios, direcciones IP, hostnames, certificados, claves, prefijos y topología. Los registros centralizados requieren mínimo privilegio, segregación de funciones, control de acceso, retención definida y anonimización al generar documentación o tickets externos. Las pruebas de diagnóstico deben evitar destinos de terceros no autorizados.

Objeto	Línea base mínima recomendada para definir	Motivo
Gateways	RTT y pérdida típicos por enlace y por periodo horario.	Distinguir alarmas reales de fluctuación habitual.
CPU / memoria / estados	Picos, percentiles y horas de carga de negocio.	Anticipar agotamiento sin alarmas por breves ráfagas.
VPN	Túneles esperados, ventanas activas y pruebas por aplicación.	Evitar alertas sobre peers que deben permanecer inactivos.
DHCP	Ocupación esperada y evolución del pool.	Detectar agotamiento antes de cortar nuevos clientes.
DNS	Latencia observada y tasa de fallos de pruebas sintéticas.	Separar caída DNS de fallo de acceso HTTP.
Logs	Reloj/NTP, retención, categorías críticas y receptor central.	Dar valor cronológico y trazabilidad a los eventos.

62.19. Errores de interpretación más frecuentes

Error	Por qué falla	Lectura correcta
«Running significa disponible»	El daemon puede no alcanzar sus dependencias.	Combinar estado, logs y prueba funcional.
«Gateway Online = Internet sano»	Monitoriza un destino y criterio específicos.	Usar varios destinos/servicios y examinar rutas.
«DHCP offline = equipo apagado»	La presencia deriva de la información de vecindad disponible.	Contrastar con switch, ARP/NDP y cliente.
«VPN UP = red remota accesible»	Rutas o ACL pueden bloquear el flujo.	Comprobar tráfico extremo a extremo.
«No aparece en DHCPv6»	SLAAC no genera obligatoriamente lease DHCPv6.	Consultar ND/RA y hosts reales.

Error	Por qué falla	Lectura correcta
«Borro logs y desaparece el problema»	Elimina evidencia, no corrige la causa.	Conservar los eventos y diagnosticar.
«Reiniciar arregla cualquier alerta»	Puede ocultar la causa o romper sesiones.	Identificar hipótesis antes de intervenir.

62.20. Glosario esencial de Status

Término	Definición práctica
Observabilidad	Capacidad de inferir el estado interno por métricas, registros y otras señales.
RTT	Tiempo de ida y vuelta de una sonda o petición.
Pérdida de paquetes	Porcentaje de sondas que no reciben respuesta en el intervalo medido.
RRD	Base de datos de series temporales con consolidación de muestras.
CARP VIP	Dirección IP virtual cuyo rol cambia entre nodos de alta disponibilidad.
pfsync	Mecanismo de sincronización de estados entre firewalls de un clúster.
SA / CHILD_SA	Asociaciones de seguridad IPsec para negociación y transporte protegido.
Lease	Concesión temporal de una dirección entregada por un servidor DHCP.
DUID/IAID	Identificadores empleados por DHCPv6 para identificar clientes y asociaciones.
ALTQ	Tecnología de colas y programación de tráfico de FreeBSD/pfSense.
Syslog	Formato/mecanismo de envío y almacenamiento de registros de eventos.
Failover	Transferencia de funciones al componente alternativo ante fallo o mantenimiento.

62.21. Referencias oficiales verificables

Documentación pública oficial de Netgate consultada para los conceptos y rutas de Status:

[01] Guía de menú Status
[02] Visión general System Monitoring
[03] Dashboard y widgets
[04] Captive Portal Status
[05] CARP Status
[06] DHCPv4 Status
[07] DHCPv6 Status
[08] DNS Resolver Status
[09] Filter Reload
[10] Gateway Status
[11] Interface Status
[12] IPsec Status
[13] NTP Status
[14] OpenVPN Status

[15] ALTQ Queues

[16] Services Status

[17] System Logs

[18] Monitoring Graphs

[19] Traffic Graphs

[20] UPnP IGD & PCP

[21] WireGuard

Las opciones disponibles y sus detalles deben interpretarse respecto a la versión de pfSense Plus y los paquetes efectivamente instalados. La documentación oficial puede ampliar o modificar ciertos comportamientos en actualizaciones posteriores.

63 Status → Captive Portal

Estado de zonas · sesiones activas · usuarios · vales de acceso · comprobación · diagnóstico · seguridad

La página Status → Captive Portal muestra el estado operativo de las zonas de portal cautivo y, cuando están habilitadas, las sesiones autorizadas y las herramientas de supervisión de vales. Su misión principal es responder tres preguntas: ¿existe una zona de portal?, ¿quién tiene acceso en este momento? y ¿qué credenciales de invitado siguen vigentes?

A diferencia de Services → Captive Portal, donde se crean zonas y se define el comportamiento del servicio, Status permite inspeccionar la actividad y ejecutar determinadas acciones sobre sesiones y vales. Esas acciones pueden causar interrupciones inmediatas; no deben confundirse con una consulta de estado.

SEGURIDAD Y ALCANCE Los ejemplos de red y usuarios de este capítulo son neutros. Una sesión autorizada por el portal no garantiza por sí sola conectividad extremo a extremo. La vista y las pestañas dependen de la existencia de zonas, métodos de autenticación y vales configurados.

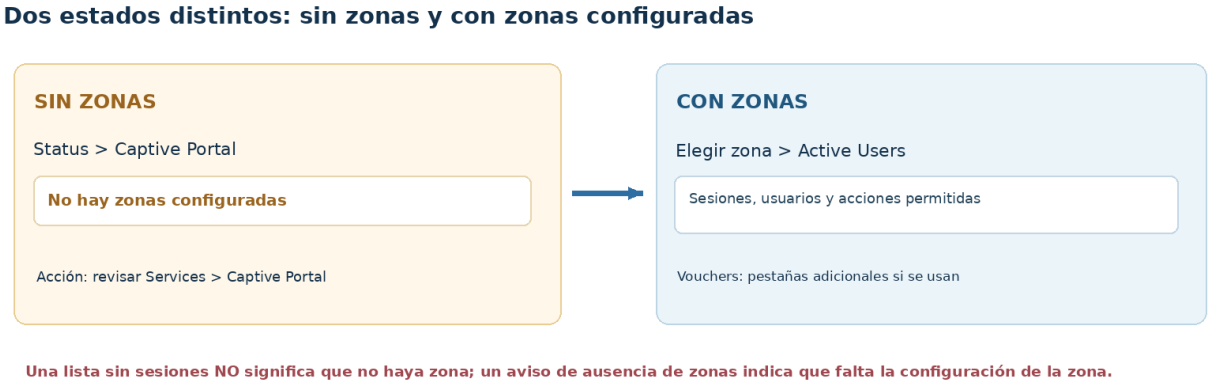


Figura 63.1. Diferencia entre ausencia de zonas y ausencia de usuarios activos; esquema original sin datos de una instalación.

63.1. Fundamento del servicio y finalidad de la página Status

Un portal cautivo intermedia la salida desde determinadas interfaces hasta que un dispositivo satisface la política definida: introducir credenciales, presentar un voucher o aceptar una página de acceso. La zona es una unidad lógica de configuración con interfaces y opciones propias; una interfaz no puede pertenecer a dos zonas simultáneamente. Las reglas del portal actúan además de otros controles de firewall y el acceso efectivo depende también de direccionamiento, rutas, DNS y NAT.

Status no configura el servidor de autenticación, la página HTML, los límites temporales ni las redes permitidas: consulta la consecuencia de esas decisiones. En implantaciones con varias zonas, la supervisión exige seleccionar la zona correcta; mezclar las sesiones de invitados con las de un aula o una sala de reuniones podría llevar a decisiones erróneas.

Ruta exacta de supervisión: Status → Captive Portal. Ruta exacta de configuración de zonas: Services → Captive Portal. Ruta de eventos de autenticación: Status → System Logs → Portal Auth, según la organización de pestañas y la versión de la interfaz.

63.2. Interpretación exhaustiva de la pantalla sin zonas

Cuando no hay ninguna zona de portal cautivo configurada, la página presenta el mensaje: «No Captive Portal zones have been configured. New zones may be added here: Services > Captive Portal». Este mensaje es informativo: no significa que el cortafuegos tenga una avería, un servicio en fallo o una zona activa sin usuarios. Indica que no existe una configuración de zona que supervisar.

Elemento visible	Qué significa	Qué puede hacer el administrador
Ruta «Status / Captive Portal»	Identifica el área de estado del portal cautivo.	Confirmar la pantalla y distinguirla de Services → Captive Portal.

Elemento visible	Qué significa	Qué puede hacer el administrador
Aviso amarillo de ausencia de zonas	No existen zonas creadas para presentar sesiones o vales.	Decidir si el servicio está deliberadamente sin desplegar o debe configurarse.
Enlace «Services > Captive Portal»	Acceso a la pantalla donde se administran zonas.	Abrir configuración cuando exista una necesidad autorizada.
Iconos generales de cabecera	Accesos auxiliares de la interfaz; su función exacta depende de versión/tema.	Consultar su etiqueta emergente y evitar atribuirles acciones no verificadas.

No aparecen las pestañas de actividad ni la tabla de clientes porque no existe una zona sobre la que realizar la consulta. El aviso por sí solo no exige pulsar ningún botón ni habilitar un portal. Si la organización no utiliza esta funcionalidad, la situación puede ser completamente normal.

DIFERENCIA CRÍTICA «No hay zonas» y «no hay usuarios en línea» son diagnósticos diferentes. El primero es un estado de configuración; el segundo es una instantánea de sesiones en una zona existente. No habilitar un portal únicamente para eliminar un aviso informativo.

63.3. Qué cambia cuando existe una zona de portal cautivo

En una instalación con una o varias zonas, la página de estado presenta de forma predeterminada la pestaña Active Users. Cuando hay múltiples zonas, aparece un selector Display Zone para escoger la zona observada. La documentación oficial describe que el estado puede reflejar clientes con nombre/contraseña, vouchers, autenticación por MAC vía RADIUS o acceso sin autenticación mediante una página de aceptación.

La apariencia y disponibilidad exactas de pestañas pueden variar con la versión y los mecanismos habilitados. No se debe interpretar como un error la ausencia de pestañas de vouchers en una zona que no utiliza ese método de acceso.

Contexto	Vista esperada	Interpretación correcta
Ninguna zona configurada	Aviso informativo; no se listan sesiones.	No existe objeto administrativo que supervisar.
Zona creada, cero usuarios	Active Users sin filas para la zona elegida.	Puede no haber clientes autenticados en ese momento.
Zona con usuarios	Filas con información de sesión y acción de terminación.	Hay autorizaciones activas del portal; validar tráfico aparte.
Varias zonas	Selector Display Zone.	La actividad mostrada pertenece a la zona seleccionada.
Zona con vouchers	Pestañas adicionales de estado y gestión de vales.	Su disponibilidad depende de la configuración del portal.

63.4. Pestaña Active Users: campos y semántica

Active Users es la vista de sesiones autorizadas. Su contenido no constituye una relación de todos los clientes conectados al switch o punto de acceso: muestra los equipos con una sesión de portal cautivo asociada. Un dispositivo puede estar conectado por Wi-Fi y aparecer sin acceso al portal hasta que complete el proceso de autenticación.

Campo o control	Descripción técnica	Advertencia de interpretación
Display Zone	Selector de zona cuando se han creado varias.	No sumar usuarios de zonas distintas sin cambiar la selección.
IP address	Dirección del cliente en la sesión del portal.	Puede cambiar tras nueva concesión DHCP.
MAC Address	Dirección física del cliente cuando el portal dispone de ella.	Puede estar vacía si la zona no emplea filtrado MAC.
Username	Usuario, voucher, MAC o «unauthenticated» según método.	No todos los valores identifican a una persona.

Campo o control	Descripción técnica	Advertencia de interpretación
Session Start Time	Instante en que comenzó la sesión autenticada.	No equivale a encendido del equipo o inicio de asociación Wi-Fi.
Actions → papelera	Solicita terminar una sesión, con confirmación.	Interrumpe el acceso y obliga a autenticar nuevamente.

La columna Username requiere especial cuidado: con usuario/contraseña figura la identidad introducida; con vouchers puede mostrar el código del vale; con RADIUS MAC Authentication puede mostrar la MAC; y si no se requiere autenticación aparece «unauthenticated». Por tanto, la pantalla no siempre proporciona trazabilidad nominal suficiente para auditoría de una persona concreta.

Si se desactiva el filtrado MAC, el campo MAC puede quedar vacío. Asimismo, el uso de direcciones MAC aleatorizadas por los clientes puede dificultar relacionar sesiones de distintas conexiones, aunque el registro en ese momento sea correcto.

63.5. Cómo funciona una sesión: del cliente a la autorización



Figura 63.2. Relación entre sesión del cliente, autorización del portal y revocación del acceso.

El cliente primero obtiene conectividad local básica. Al solicitar un recurso HTTP que puede interceptarse, el portal presenta el mecanismo de acceso. Tras autenticar o aceptar, se crea una sesión de portal. Esa sesión aparece en la vista de estado mientras siga vigente; si expira, se revoca o el administrador la desconecta, el usuario deberá autenticarse otra vez.

Es importante separar el control de autorización del transporte. Una sesión puede estar activa mientras falla la resolución DNS, la puerta de enlace upstream, una regla de firewall o el servidor de destino. La presencia de una fila únicamente confirma el estado de autorización en el portal; la validez funcional se verifica con una prueba desde el cliente.

63.6. Acción de terminar sesión: funcionamiento y riesgos

Netgate documenta una acción de papelera por sesión. Al pulsarla y confirmar, el portal termina la autorización y el cliente debe iniciar nuevamente el proceso para volver a tener acceso. Es una herramienta útil para asistencia técnica, control de sesiones anómalas o cierre autorizado de un acceso temporal.

Antes de terminar una sesión: identificar zona y usuario correcto, comprobar la dirección correspondiente, considerar terminales compartidos y consultar el impacto. En entornos empresariales un único cliente puede sostener comunicaciones críticas; la desconexión no es una prueba inocua.

> **ACCIÓN DISRUPTIVA** Finalizar una sesión corta el acceso autorizado del cliente. No garantiza, en todas las versiones o circunstancias, que desaparezcan instantáneamente todas las conexiones previamente establecidas; si se investiga un incidente de seguridad, verificar también los estados y reglas aplicables.

63.7. Vouchers: diferencias entre código, sesión y lote

Un voucher es un código temporal generado dentro de un lote o roll. El código puede permitir acceso durante una duración predefinida. El temporizador comienza cuando se activa por primera vez y no se pausa al desconectar el cliente. Si un mismo vale se utiliza desde otro equipo durante su vigencia, el comportamiento descrito por Netgate es el desplazamiento de la sesión previa.

La sesión del portal, el código de voucher y el lote son objetos distintos. Eliminar la sesión de un cliente puede obligarle a reintroducir su vale, pero no equivale necesariamente a invalidar el vale. La operación Expire Vouchers sí está concebida para dejar de aceptar los códigos indicados.

63.8. Active Vouchers: consulta de códigos activados

La pestaña Active Vouchers, disponible en zonas que utilizan vales, presenta los códigos actualmente activos y sus temporizadores. La documentación de Netgate ilustra información como el propio voucher, su roll, la fecha de activación, el tiempo que resta hasta el vencimiento y el momento previsto de expiración.

Esta vista resulta útil para verificar una reclamación de «mi código no funciona» o «mi tiempo se ha acabado demasiado pronto». Comparar la primera activación, la duración del lote, la hora del firewall y el estado del código antes de generar otro. Un vale no se prolonga desconectando al cliente.

63.9. Voucher Rolls: consumo y capacidad de vales

Voucher Rolls permite examinar los lotes creados y la utilización de sus códigos. Netgate documenta una vista con identificador de lote, duración por ticket, cantidad, comentario y contadores de usados, activos y disponibles. Estos valores permiten calcular la capacidad pendiente para invitados o campañas temporales sin exponer ni exportar los códigos.

Como buena práctica, comparar el número de vales disponibles con la previsión de demanda. No modificar el número de roll ni el count de un lote existente sin evaluar el efecto, porque ciertos cambios invalidan vales emitidos. La emisión y edición de lotes pertenecen al área Services y tienen un impacto distinto a la consulta en Status.

63.10. Test Vouchers: comprobación sin consumirlos

Test Vouchers recibe un código para evaluar si es válido y, en caso afirmativo, mostrar su duración. Según Netgate, la operación de prueba no cuenta el vale como utilizado ni lo consume. Puede servir para comprobar la legibilidad de un código impreso o introducir un código cuando un usuario reporta que no consigue autenticarse.

El resultado de Test Vouchers solo acredita la validez del código en ese contexto. Si el código es válido pero el cliente no navega, revisar la zona elegida, la página HTML del portal, el canal de presentación del vale, la sesión y la conectividad. No compartir códigos reales en tickets visibles por grupos amplios.

63.11. Expire Vouchers: anulación individual o masiva

Expire Vouchers permite introducir uno o varios códigos, separados por líneas, para invalidarlos. Netgate especifica que los vales activos enviados por esta vía también se expiran de forma inmediata. Esta acción puede afectar a numerosos usuarios y no debe usarse para hacer una prueba rutinaria de validez.

En operaciones con lotes grandes, registrar la autorización, el motivo, los códigos afectados y la respuesta posterior. Considerar la revocación de vouchers como una operación de control de acceso de impacto similar a dar de baja credenciales.



Figura 63.3. Cuatro pestañas de vouchers: las tres consultas frente a la expiración de códigos.

Pestaña	Finalidad	¿Puede cambiar accesos?
Active Vouchers	Ver vales activados y vencimiento.	Solo lectura.
Voucher Rolls	Revisar consumo y capacidad de lotes.	Consulta en Status; gestión en Services.
Test Vouchers	Verificar un código sin consumirlo.	La prueba no usa ni caduca el voucher.
Expire Vouchers	Invalidar uno o varios códigos.	Sí, puede retirar acceso inmediatamente.

63.12. Relación con la configuración de zonas

Cuando no hay zonas, la corrección —si el portal es un requisito funcional— se realiza en Services → Captive Portal. El administrador crea un nombre de zona, añade una descripción opcional, selecciona interfaces y define política de autenticación, redirección y comportamiento de los clientes. La creación de zonas no debe proponerse como simple respuesta a un aviso de estado: puede alterar la política efectiva de acceso de una interfaz completa.

La guía oficial limita una interfaz a una sola zona a la vez. Si se requiere segmentación diferente para invitados, empleados y aulas, el diseño habitual distingue interfaces lógicas, VLAN y políticas de acceso, además de zonas apropiadas. La separación administrativa no debe sustituir la segmentación L2/L3 y las reglas explícitas de firewall.

63.13. Limitaciones y dependencias que afectan al diagnóstico

Netgate señala una limitación principal: Captive Portal no es compatible con IPv6 en la implementación documentada. En redes dual-stack debe comprobarse que el comportamiento del cliente y las políticas de acceso corresponden al modelo admitido, evitando asumir que el portal controla de manera equivalente todos los flujos IPv4 e IPv6. Tampoco existe un «reverse portal» para exigir autenticación a tráfico que entra desde Internet.

Una redirección automática del portal requiere que el cliente pueda resolver los nombres necesarios y llegue a producir una petición HTTP susceptible de interceptación; una página inicial HTTPS pura no siempre origina el redireccionamiento esperado. Los sistemas modernos suelen tener detección de portales cautivos, pero esta detección depende del sistema operativo, las políticas DNS y la red.

Otro factor operativo es que los dispositivos existentes detrás de un router intermedio pueden compartir una MAC observada por el portal. En esas topologías la información de la sesión puede no identificar inequívocamente cada equipo final; se requiere revisar el diseño de red y las opciones oficiales de filtrado de MAC.

63.14. Comprobaciones tras crear una zona

01 Confirmar en Services → Captive Portal que la zona existe, está habilitada y vinculada a la interfaz correcta; no alterar otras zonas.

02 Conectar un dispositivo de pruebas a la red correspondiente, sin utilizar credenciales de producción para documentación.

03 Verificar concesión IPv4, puerta de enlace, DNS y capacidad para emitir una petición HTTP apropiada.

04 Completar el método de acceso previsto y comprobar que el dispositivo aparece en Status → Captive Portal → Active Users.

05 Anotar la zona seleccionada, la hora de inicio y el tipo de Username según el método de autenticación.

06 Verificar navegación y acceso a un recurso permitido, diferenciando autorización del funcionamiento del servicio remoto.

07 Cerrar la sesión por el mecanismo ordinario si existe; comprobar su desaparición. No usar la papelera salvo necesidad controlada.

63.15. Procedimiento de soporte: un cliente no aparece en Active Users

01 Comprobar que la zona que se está visualizando coincide con la interfaz donde se conecta el usuario.

02 Confirmar que la zona está activada y que el equipo obtuvo configuración IPv4 válida.

03 Preguntar si el cliente recibió la página de portal o la solicitud de autenticación del sistema operativo.

04 Revisar los registros Portal Auth y, si hay RADIUS, los del servidor de autenticación remoto.

05 Confirmar si existe un bypass autorizado por MAC/IP que explique el acceso sin una sesión típica.

06 Realizar una prueba controlada de login y localizar el nuevo registro por IP/hora sin revelar credenciales.

63.16. Procedimiento de soporte: el portal no redirige



Figura 63.4. Secuencia de diagnóstico para fallos de presentación y autorización del portal.

No asumir que el servicio falla porque un navegador abre una página HTTPS sin interponer el formulario. Verificar una prueba HTTP, la resolución DNS y los filtros de la interfaz. Confirmar la asociación de zona e interfaz y que el servicio Captive Portal esté habilitado.

Si el sistema operativo no detecta el portal, abrir un navegador con una URL de prueba HTTP adecuada y controlada, en lugar de deshabilitar indiscriminadamente HTTPS o modificar la seguridad global del navegador. En dispositivos Apple, Netgate documenta situaciones de Safari y detección automática que justifican contrastar el comportamiento manual.

63.17. Procedimiento de soporte: autenticación y vouchers fallan

En autenticación local, revisar existencia de usuario, contraseña y privilegio de inicio de sesión del portal si se ha exigido. En RADIUS, validar conectividad hacia el servidor, secreto compartido y registros de rechazo o timeout del servidor; no registrar contraseñas en la incidencia. Un error de autenticación y una ausencia de conectividad son causas distintas que requieren soluciones diferentes.

En vouchers, ejecutar Test Vouchers antes de invalidar o emitir códigos nuevos. Si el código está caducado, revisar tiempo desde activación y duración del lote. Si aparece válido pero falla el inicio de sesión, comprobar la integración de la página del portal con el campo de formulario de voucher; la documentación oficial identifica «auth_voucher» para ese flujo.

63.18. Diagnóstico mediante logs, gráficos y fuentes cruzadas

Para confirmar eventos, utilizar Status → System Logs → Portal Auth, donde se registran mensajes de autenticación del portal. Combinar con el log de firewall para investigar bloqueos, con el servidor RADIUS/LDAP si se usa y con los contadores de interfaz. Una tabla Active Users sin filas es una instantánea, no un histórico completo de todos los intentos fallidos.

El grupo de gráficos de Captive Portal permite examinar usuarios concurrentes y eventos de inicio de sesión por intervalo. Un número alto de «Logged In» en una ventana breve puede indicar una llegada masiva de usuarios o una sucesión de reconexiones; no prueba por sí solo un ataque. Las gráficas de Monitoring y los logs poseen granularidad y retención diferentes, por lo que se deben correlacionar por hora y contexto.

Señal	Interpretación posible	Prueba complementaria
Usuario ausente de Active Users	No autenticado, otra zona, sesión expirada.	Display Zone, Portal Auth, prueba de login.
Voucher inválido	Código mal introducido, expirado o anulado.	Test Vouchers y tiempo desde activación.
Login correcto sin navegación	Problema de DNS, firewall, NAT o ruta.	Cliente IPv4, logs de filtro y HTTP/DNS.
Redirección no aparece	HTTPS inicial, DNS o política de interface.	Solicitud HTTP, reglas, estado de zona.
Muchos intentos repetidos	Error de backend, mala página o desconexiones.	Portal Auth, RADIUS y patrones por hora.
Una sesión persiste tras intervención	Estado o conexión anterior no actualizado.	Verificar estado del cliente y conexiones establecidas.

63.19. Tres escenarios empresariales y decisiones apropiadas

63.19.1. Wi-Fi de invitados en una sala de formación

Una organización despliega una VLAN exclusiva para invitados y una zona de portal con aceptación de condiciones. La mesa de soporte consulta Active Users por zona, confirma que los asistentes han completado el formulario y verifica navegación desde una estación de prueba. El campo Username puede indicar «unauthenticated» por diseño; eso no implica fallo de autorización del portal. La VLAN debe continuar aislada de redes internas mediante reglas independientes.

63.19.2. Acceso temporal con vales en un evento

Para invitados de un evento se generan rollos de vouchers con duración concreta. El administrador monitoriza Active Vouchers y Voucher Rolls para comprobar activaciones y capacidad; el personal de soporte usa Test Vouchers para incidencias de lectura. La invalidación solo se emplea cuando procede retirar un acceso: Expire Vouchers puede dejar fuera al participante de inmediato.

63.19.3. Portal federado con RADIUS y reclamación de usuario

Un usuario comunica que su contraseña válida no permite navegar. Se comprueba primero que la zona y la red estén operativas; a continuación se correlaciona el intento con Portal Auth y el registro de RADIUS. Si la autenticación es correcta y la sesión figura activa, se analizan DNS y firewall antes de modificar credenciales o revocar sesiones ajenas. La prueba final se realiza con acceso controlado al recurso autorizado.

63.20. Seguridad, cumplimiento y buenas prácticas

Conceder permisos de lectura a operadores que solo supervisan y restringir el acceso a expulsión de usuarios y revocación de vales. Registrar incidencias con datos mínimos: zona, hora, identificador seudonimizado y resultado. Evitar copiar en tickets códigos de vales, MAC reales, nombres de usuarios, IP reales, tokens y evidencias de autenticación con datos sensibles.

El portal cautivo no sustituye cifrado de Wi-Fi, segmentación VLAN, políticas de firewall ni la autenticación de servicios internos. Los controles de acceso deben diseñarse por capas: aislamiento de red, tráfico permitido, portal y trazabilidad adecuada. Proteger la gestión web con HTTPS y accesos de administración restringidos.

En alta disponibilidad, revisar la sincronización de datos del portal y los vales conforme a la arquitectura utilizada. Netgate documenta mecanismos XMLRPC para sincronizar datos de vouchers; un failover no debe asumirse sin probar qué sucede con sesiones, códigos y acceso del cliente durante el cambio de nodo.

> **PRECAUCIÓN DE PRODUCCIÓN** Antes de borrar sesiones o expirar vales, valorar el impacto y disponer de acceso administrativo independiente del segmento de invitados. Evitar pruebas agresivas en redes con terminales de terceros o servicios de acceso público.

63.21. Errores frecuentes de interpretación y corrección

Conclusión incorrecta	Por qué es errónea	Actuación aconsejada
«El portal está averiado porque no hay zonas».	La pantalla indica ausencia de configuración.	Confirmar si se necesita desplegar el servicio.
«No hay usuarios conectados a Wi-Fi».	La tabla solo refleja sesiones del portal.	Consultar AP/switch y DHCP por separado.
«unauthenticated significa que el portal falló».	Puede ser acceso sin autenticación de usuario.	Contrastar método de zona.
«Con una sesión activa, Internet funciona».	El control de autorización no garantiza conectividad.	Probar DNS, ruta y servicio final.
«Probar un voucher gasta su tiempo».	Test Vouchers no activa ni consume el vale.	Usar prueba antes de realizar cambios.
«Al cerrar la sesión, el vale se reinicia».	El contador de voucher no se pausa.	Consultar duración desde primera activación.
«Expirar vales es una consulta».	Es una revocación de credenciales.	Solicitar autorización y registrar el cambio.

63.22. Glosario técnico del estado Captive Portal

Término	Significado práctico
Zona	Configuración lógica del portal asociada a una o más interfaces.
Active Users	Vista de sesiones de clientes autorizados por el portal.
Display Zone	Selector de zona cuando existen varias.
Voucher	Código temporal de acceso con duración y reglas de activación.
Roll	Lote de vouchers emitidos con parámetros comunes.
Portal Auth	Registro de eventos de autenticación del portal.
RADIUS	Protocolo y servicio de autenticación/contabilidad remota.
MAC filtering	Tratamiento de direcciones MAC para identificar/controlar clientes del portal.
Captive portal detection	Mecanismo del sistema operativo que identifica necesidad de login.
Sesión	Estado temporal de autorización de un cliente en la zona.

63.23. Referencias técnicas y oficiales

Documentación de Netgate, contrastada para describir las opciones presentes al configurar zonas y las vistas de estado disponibles:

[01] Captive Portal Status

[02] Vouchers — opciones y pestañas de Status

[03] Captive Portal Zones

[04] Captive Portal — fundamentos y limitaciones

[05] Zone Configuration Options

[06] Common Captive Portal Scenarios

[07] Troubleshooting Captive Portal

[08] Menú Status

[09] Monitoring Graphs — Captive Portal

[10] System Logs

[11] Log Settings

[12] Available Dashboard Widgets

Nota de compatibilidad: los controles concretos y su disposición pueden cambiar en versiones y ediciones posteriores. Las pestañas adicionales se describen conforme a la documentación publicada; el estado sin zonas no incorpora todavía esas vistas.

64 Status → CARP (failover)

Direcciones virtuales · alta disponibilidad · MASTER/BACKUP · pfsync · mantenimiento · diagnóstico

La página Status → CARP (failover) permite observar qué nodo posee cada dirección IP virtual compartida y realizar operaciones de mantenimiento que pueden transferir el servicio al otro cortafuegos. Es un punto de control esencial en un clúster de alta disponibilidad, pero no sustituye la supervisión de enlaces, tablas de estados, sincronización de configuración ni servicios.

La pantalla analizada presenta el aviso «No CARP interfaces have been defined» y un enlace a la configuración de sincronización de alta disponibilidad. Este estado se documenta en primer lugar; posteriormente se explican las tablas, avisos y acciones que muestra pfSense cuando existen VIP CARP configuradas, conforme a la documentación oficial de Netgate.

ADVERTENCIA OPERATIVA Las acciones de failover pueden trasladar las IP virtuales, interrumpir conexiones y afectar a VPN, NAT, DNS o servicios publicados. En producción, verificar el nodo secundario y disponer de acceso independiente antes de cambiar el estado de CARP.

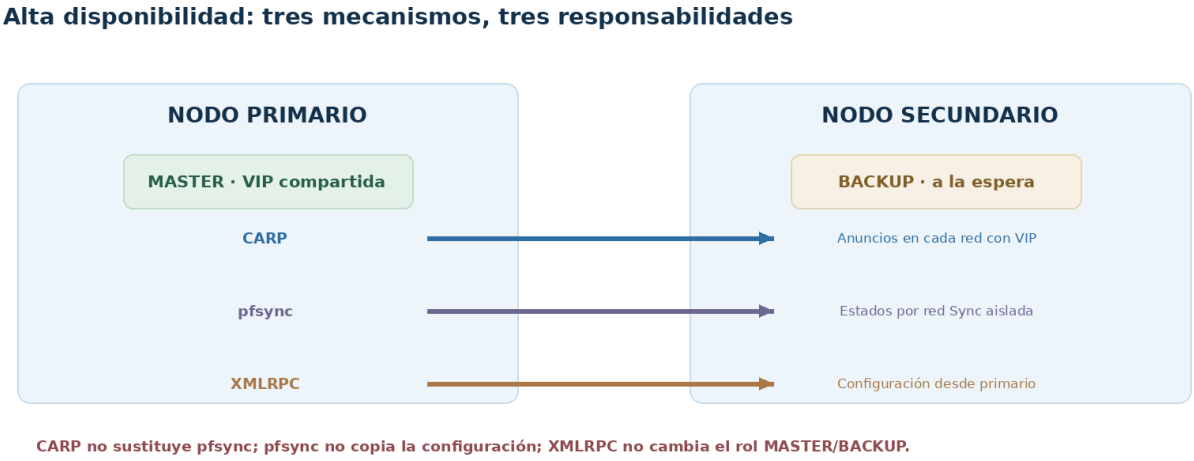


Figura 64.1. Tres mecanismos de alta disponibilidad y sus respectivas funciones; esquema conceptual sin información de infraestructura.

64.1. Qué es CARP y qué problema resuelve

CARP (Common Address Redundancy Protocol) permite que varios cortafuegos conectados al mismo dominio de capa 2 compartan una dirección IP virtual (VIP). Un nodo anuncia que es el propietario activo de la VIP y acepta el tráfico dirigido a ella; el otro vigila los anuncios para asumir el servicio cuando corresponda. La dirección física de administración de cada cortafuegos es independiente y debe permanecer disponible para tareas de mantenimiento.

Netgate documenta la arquitectura soportada de alta disponibilidad para pfSense Plus con dos nodos, normalmente en esquema activo/pasivo. CARP aporta redundancia de direccionamiento; pfsync replica los estados del firewall; XMLRPC replica partes de la configuración; y ciertos servicios, como DHCP, incorporan mecanismos adicionales de continuidad. No es correcto llamar «CARP» a todo el clúster.

64.2. Ruta exacta, alcance de Status y relación con otros menús

Ubicación	Finalidad	¿Modificar desde aquí?
Status → CARP (failover)	Consultar propiedad de VIPs y ejecutar acciones de mantenimiento.	Sí: solo acciones CARP específicas.
Firewall → Virtual IPs	Crear, editar y revisar direcciones virtuales CARP e IP Alias.	Sí, afecta configuración de IP.
System → High Avail. Sync	Configurar sincronización de estados y XMLRPC.	Sí, afecta clúster.

Ubicación	Finalidad	¿Modificar desde aquí?
Status → Interfaces	Inspeccionar enlaces y direcciones de cada interfaz.	Consulta/diagnóstico.
Status → System Logs	Comprobar transiciones, errores y sincronización.	Consulta de evidencia.
Diagnostics → Packet Capture	Analizar anuncios CARP por segmento de red.	Captura controlada.

La página Status no es el asistente de implantación. Activar la sincronización XMLRPC o pfsync sin haber diseñado VIPs, conectividad de capa 2, reglas y direccionamiento no crea una solución HA completa. Las IP virtuales se configuran en Firewall → Virtual IPs; la opción «High availability sync settings can be configured here» dirige a la configuración de sincronización, no a la creación automática de CARP.

64.3. Análisis minucioso de la pantalla sin interfaces CARP

El mensaje amarillo «No CARP interfaces have been defined» significa que no existe ninguna interfaz CARP definida que mostrar. Puede ser perfectamente normal en un firewall independiente o en un clúster que aún no ha habilitado VIPs. Es un estado de configuración, no un fallo de detección de la red ni una alarma de pérdida de su contraparte por sí mismo.

Elemento observable	Interpretación	Acción apropiada
Ruta «Status / CARP»	Identifica la página de supervisión CARP.	Comprobar que se está en el nodo previsto.
Aviso amarillo sin interfaces	No hay VIPs CARP definidas en este equipo.	Verificar si existe requerimiento de alta disponibilidad.
Enlace «High availability sync settings...»	Navega a parámetros de sincronización del clúster.	Abrir para consultar o configurar pfsync/XMLRPC con autorización.
«×» en el aviso	Cierra visualmente el mensaje informativo.	No configura ni habilita CARP.
Iconos de cabecera	Controles globales del tema o edición de pfSense.	Identificar por ayuda emergente; no inferir acciones propias de CARP.

Las tablas de VIP, los controles de mantenimiento y los indicadores de pfsync dependen de que exista una configuración de alta disponibilidad compatible. Su ausencia en un sistema sin CARP configurado no indica por sí sola una avería de la interfaz web.

INTERPRETACIÓN CORRECTA No crear un clúster ni habilitar opciones de sincronización solo para hacer desaparecer el aviso amarillo. El objetivo de Status es informar del estado realmente configurado.

64.4. Arquitectura de clúster y dominios de comunicación

Cada cortafuegos dispone de sus propias direcciones físicas en las interfaces necesarias, además de las VIP compartidas por CARP. Los anuncios de CARP ocurren en cada segmento donde existe una VIP y no en la interfaz Sync por el mero hecho de ser Sync. La interfaz de sincronización sirve para pfsync y XMLRPC y debe estar aislada, preferentemente dedicada entre ambos equipos.

La continuidad requiere que el tráfico de usuarios utilice VIPs cuando corresponda: puerta de enlace, direccionamiento publicado o servicios que deban migrar entre nodos. No basta con sincronizar reglas si los equipos siguen apuntando exclusivamente a la dirección física del nodo primario.

Mecanismo	Qué replica o decide	Riesgo si falla
CARP	Determina quién responde por una VIP en un segmento de capa 2.	Pérdida de VIP o doble MASTER.
pfsync	Estados de conexiones PF entre nodos.	Las sesiones preexistentes pueden cortarse durante failover.
XMLRPC	Configuración seleccionada del nodo principal al secundario.	Divergencia de reglas, VIPs o servicios.
Sincronización DHCP / Kea	Continuidad de arrendamientos según el modo HA configurado.	Concesiones/renovaciones pueden verse afectadas.

Mecanismo	Qué replica o decide	Riesgo si falla
NTP y coherencia de interfaces	Base operativa para tiempos, servicios y correspondencia de puertos.	Incidencias intermitentes difíciles de diagnosticar.

64.5. Elección de MASTER: VHID, anuncios, base y skew

Cada VIP CARP tiene un identificador de grupo VHID y parámetros de frecuencia de anuncio. Los nodos que comparten la VIP deben coordinarse y usar valores compatibles de VHID y contraseña. El mismo VHID no debe competir con otro grupo independiente en el mismo dominio de capa 2. La selección del propietario está relacionada con la cadencia de los anuncios: un skew menor produce anuncios más rápidos y suele ganar el rol MASTER.

El intervalo contiene una parte base (habitualmente 1 segundo) y una fracción skew de 1/256 de segundo. En ejemplos oficiales, el primario emplea skew 0 o 1 y el secundario aproximadamente 100, con diferencias suficientes para producir elección predecible. Estos son valores ilustrativos habituales, no valores universales a aplicar sin revisar el diseño del clúster.

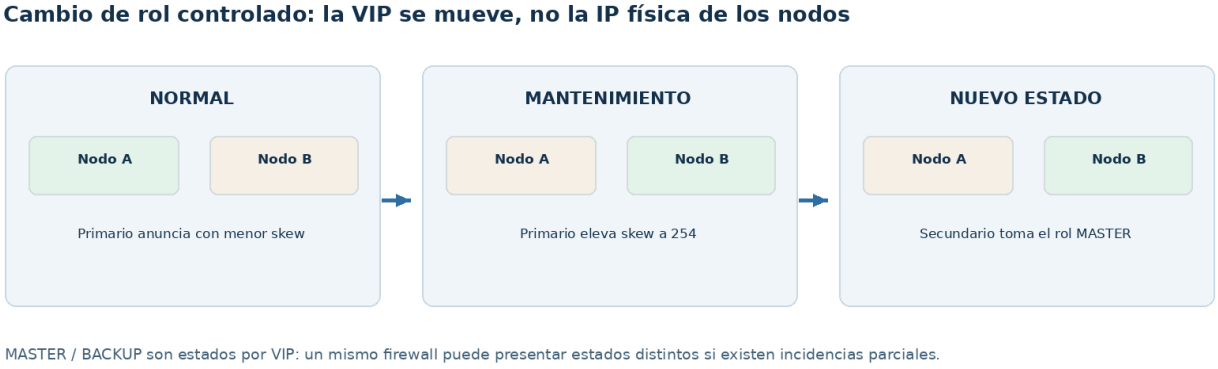


Figura 64.2. Evolución del propietario de la VIP durante mantenimiento programado de un nodo.

64.6. Tabla de estado con VIPs existentes

Cuando existen direcciones virtuales CARP, Status → CARP muestra la tabla CARP Status. Cada fila corresponde a una VIP CARP y puede incluir direcciones IP Alias dependientes de la VIP principal. La documentación describe los siguientes campos, que no aparecen en la captura sin CARP pero son propios de la vista operativa.

Columna documentada	Significado	Comprobación
Interface and VHID	Interfaz y grupo de redundancia, p. ej. WAN@11 (ejemplo ficticio).	Coincide en los nodos del mismo grupo.
Virtual IP Addresses	VIP CARP y alias IP subordinados a su VIP padre.	Direcciones y máscaras coherentes.
Status	Estado local de cada VIP: MASTER, BACKUP, INIT o vacío.	Leer simultáneamente ambos nodos.

64.7. Interpretación de MASTER, BACKUP, INIT y estados anómalos

MASTER significa que este equipo acepta el tráfico destinado a la VIP. BACKUP indica que escucha los anuncios y no debe actuar como propietario activo. INIT o un estado vacío suelen reflejar una VIP no instalada correctamente, una interfaz caída o una incidencia de enlace/configuración. Si la arquitectura es primaria/secundaria convencional, el primario debe mostrar MASTER y el secundario BACKUP en las mismas VIPs.

El caso MASTER/MASTER en ambos extremos es especialmente grave: suele indicar que las emisiones CARP no llegan entre nodos, por ejemplo por filtrado de multicast, aislamiento VLAN o configuraciones de switches o hipervisores. No basta con comprobar el cable Sync: CARP se anuncia en las interfaces que alojan las VIPs.

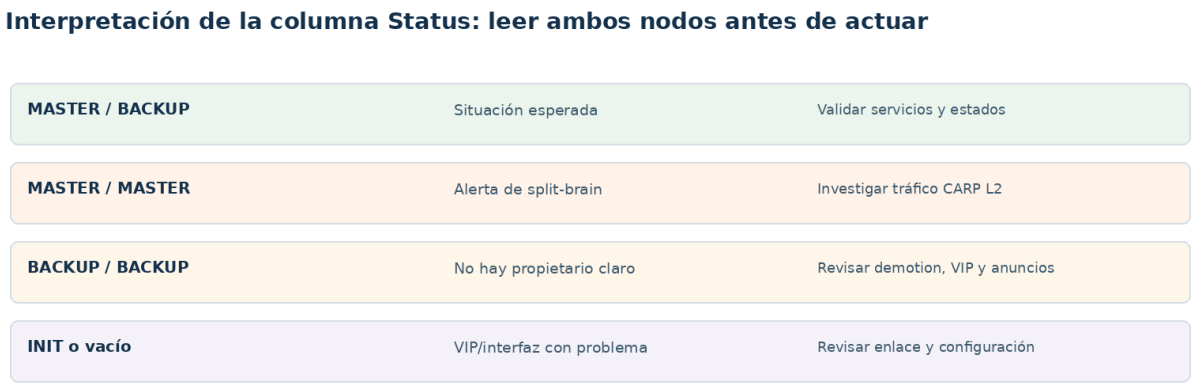


Figura 64.3. Matriz de interpretación de estados, con medidas de respuesta sugeridas.

64.8. Controles de mantenimiento disponibles con CARP activo

La zona superior de la pantalla CARP Status puede mostrar controles para cambiar el estado de CARP en este nodo. Son acciones operativas, no conmutadores meramente cosméticos: pueden hacer que el nodo contrario asuma direcciones y servicios. Netgate advierte que la interfaz puede actualizarse antes de completarse la elección, por lo que conviene esperar brevemente y recargar manualmente el estado.

Control documentado	Efecto técnico	Duración / riesgo
Temporarily Disable CARP	Deshabilita CARP y retira temporalmente las VIPs del sistema operativo en ese nodo.	No persiste tras reinicio; puede provocar failover.
Enable CARP	Vuelve a configurar las VIPs y a participar en la elección de rol.	El primario puede recuperar MASTER al concluir.
Enter Persistent CARP Maintenance Mode	Conserva las VIPs configuradas, pero eleva skew de todas a 254 para ceder el rol.	Permanece tras reiniciar; apto para mantenimiento programado.
Leave Persistent CARP Maintenance Mode	Retira la marca de mantenimiento y restaura skew configurado.	Puede retornar el rol MASTER al equipo preferido.
Reset CARP Demotion Status	Pone a cero el valor de penalización acumulado que puede impedir MASTER.	Solo para desajuste residual, no para fallos activos.

64.9. Diferencias críticas: desactivación temporal y modo persistente

Desactivar CARP temporalmente retira del sistema las VIPs mientras permanezca desactivado; ese estado no se conserva después de reiniciar el firewall. El modo de mantenimiento persistente conserva la VIP en el sistema pero aumenta su skew de anuncio a 254 para que otro nodo con menor skew tome el control. Esta marca persiste tras reinicios: es preferible durante trabajos donde no se desea que el primario vuelva a asumir carga antes de finalizar la intervención.

No poner ambos nodos simultáneamente en mantenimiento persistente: competirían con skew 254, y el resultado sería impredecible. Tampoco es una garantía de continuidad de sesiones si no existe sincronización pfsync ni rutas/NAT/servicios correctos en el nodo secundario.

> **ACCIÓN DISRUPTIVA** Antes de entrar o salir del modo persistente, comprobar el papel de ambos nodos y reservar una ventana de mantenimiento. El retorno a MASTER puede alterar rutas de retorno, estados PF y conexiones si hay asimetrías.

64.10. Demotion: por qué un nodo puede ceder el rol

pfSense mantiene un valor de democión que puede incrementarse ante incidencias locales, por ejemplo al caer una interfaz con una VIP CARP. Netgate documenta un incremento de 240 que se añade internamente a los skew; al recuperarse la interfaz se resta normalmente la penalización. Así, un nodo con fallos locales puede ceder la VIP al otro sin necesidad de apagar el equipo.

La página puede presentar una advertencia y el botón «Reset CARP Demotion Status» cuando el valor no es cero. Antes de usarlo, comprobar físicamente interfaces, enlace, direcciones y servicios. Si la causa sigue presente, el reajuste puede desordenar el estado de democión o provocar un nuevo cambio de rol. La corrección normal consiste en solucionar la causa para que el valor vuelva a su nivel correcto.

64.11. State Synchronization Status / pfsync Nodes

En su parte inferior, la página CARP muestra identificadores de los nodos que han creado estados en la tabla PF. Si pfsync funciona, las vistas de ambos nodos deberían contener entradas procedentes de sus respectivos identificadores, con diferencias transitorias posibles. La coincidencia casi completa es indicio de sincronización; no equivale a probar que todos los servicios sobreviven a una conmutación.

El Filter Host ID puede fijarse en System → High Avail. Sync; cada nodo necesita un valor distinto. En versiones actuales, Netgate utiliza por defecto los últimos ocho caracteres del NDI del equipo, mientras que versiones anteriores generaban valores aleatorios al recargar el filtro. La identificación concreta debe comprobarse en el sistema, no inferirse de la captura.

Observación	Interpretación probable	Paso de comprobación
Aparecen IDs de ambos nodos	Hay estados que parecen sincronizarse.	Comparar listas y realizar prueba real.
Solo aparece ID propio	Puede faltar comunicación o actividad de sincronización.	Revisar interfaz Sync, reglas y pfsync.
IDs distintos entre consultas	Cambios transitorios, filtro o ID personalizado.	Revisar cambio de configuración y observar evolución.
Estados sincronizados, corte de sesión	Falla NAT, ruta, interfaz o servicio dependiente.	Probar continuidad extremo a extremo.

64.12. Seguridad del canal de sincronización

pfsync no incorpora autenticación propia, por lo que Netgate recomienda una conexión dedicada y aislada o una VLAN restringida y correctamente protegida. Exponer este tráfico a estaciones no confiables permitiría interferir en la tabla de estados. La sincronización XMLRPC requiere conectividad de administración autorizada entre nodos y credenciales adecuadas, separadas de redes de usuarios.

No confundir enlace Sync con anuncios CARP. Una regla que autorice pfsync únicamente en Sync no repara anuncios CARP bloqueados en una VLAN WAN o LAN. También debe verificarse que la correspondencia física y lógica de interfaces entre ambos nodos sea coherente con el diseño.

64.13. VLAN, switch, virtualización y multicast CARP

Los problemas de doble MASTER surgen con frecuencia por impedir la recepción de anuncios. En modo multicast los switches y equipos intermedios deben permitir ese tráfico, admitir varias MAC asociadas a los puertos y posibilitar que la MAC virtual cambie de ubicación durante el failover. IGMP snooping, seguridad de puertos, políticas de hipervisor y enlaces trunk mal configurados pueden bloquear o alterar esta comunicación.

La documentación de pfSense Plus contempla CARP unicast cuando el modo multicast no es viable, siempre que su uso y correspondencia entre pares estén configurados de forma consistente. No elegir unicast como solución automática sin confirmar primero el alcance del problema L2. En máquinas virtuales comprobar también políticas de direcciones MAC y capacidades de los switches virtuales.

64.14. Conectividad y puertos: qué comprobar realmente

CARP utiliza el protocolo IP 112; no es una aplicación que dependa de un puerto TCP o UDP. pfsync utiliza su propio protocolo; XMLRPC emplea acceso administrativo conforme a la configuración del sistema. La regla de firewall necesaria para permitir anuncios o sincronización depende de la interfaz y topología. No abrir indiscriminadamente todo el tráfico entre redes para solucionar una alarma de CARP.

Los equipos deben comunicarse en cada segmento compartido con VIPs. Compruebe que las VLAN corresponden a los mismos dominios L2, que la subred y máscara de las VIPs coinciden, que la contraseña del grupo es idéntica en cada extremo y que los VHID no colisionan con otras parejas en el segmento.

64.15. Procedimiento: interpretar un clúster sano sin modificarlo

01 Abrir Status → CARP (failover) desde el primario con acceso administrativo fuera de las VIPs a probar.

02 Registrar por VIP el valor Interface and VHID, dirección virtual asociada y estado local.

03 Abrir la misma vista en el secundario; confirmar que la VIP MASTER en uno es BACKUP en el otro.

04 Comprobar State Synchronization Status en ambos nodos; comparar los Filter Host ID observados.

05 Verificar Status → Interfaces, logs de sistema y que no hay advertencias de demotion persistentes.

06 Probar desde un cliente de laboratorio el acceso permitido a la VIP, DNS, NAT y servicios críticos.

07 Guardar únicamente datos mínimos de la prueba y no exportar IP reales ni capturas operativas a documentos externos.

64.16. Procedimiento: prueba de failover controlada

Una prueba de conmutación debe realizarse con autorización y plan de reversión. Se recomienda disponer de acceso a las IP físicas de ambos equipos, de supervisión externa y de un cliente de prueba representativo. La secuencia siguiente emplea el modo de mantenimiento persistente porque permite devolver el primario de manera explícita al finalizar los trabajos.

01 Confirmar antes de iniciar que el primario es MASTER y el secundario BACKUP, con sincronización sana.

02 Tomar una referencia de tráfico y verificar un servicio representativo (por ejemplo, navegación desde cliente de prueba).

03 En el primario pulsar «Enter Persistent CARP Maintenance Mode», solo después de validar el secundario.

04 Esperar a que concluya la elección y recargar manualmente Status → CARP en ambos equipos.

05 Confirmar que el secundario ha pasado a MASTER en todas las VIPs previstas y que el primario ha cedido el rol.

06 Repetir las pruebas de DNS, salida, conexiones establecidas, VPN y servicios locales que apliquen.

07 Tras finalizar, pulsar «Leave Persistent CARP Maintenance Mode» únicamente en el primario.

08 Confirmar retorno estable, eventos en logs y continuidad después de la reversión. Documentar cualquier corte.

PRUEBA DE PRODUCCIÓN Las conexiones VoIP u otros flujos sensibles pueden sufrir una interrupción aunque pfsync funcione. No prometer failover sin pérdida de paquetes; medir continuidad del servicio y comprobar el plan de reversión.

64.17. Diagnóstico: ambos nodos muestran MASTER

Este síntoma indica que cada nodo cree ser propietario de la misma VIP. Priorizar la comunicación de los anuncios en las interfaces que alojan CARP: estado físico, VLAN, switch, multicasting, filtrado, MAC virtual y visibilidad de paquetes. Revisar después VHID, contraseña y máscara. No resolverlo deshabilitando arbitrariamente el firewall completo o borrando VIPs existentes.

Consultar Status → System Logs para buscar transiciones repetidas, errores de hash y avisos. Una captura CARP en cada equipo permite comprobar si los anuncios que salen por uno llegan al otro. Si no llegan, el problema se encuentra probablemente en el trayecto de capa 2. Si llegan pero no se reconocen, revisar coherencia del grupo CARP y documentación de compatibilidad.

64.18. Diagnóstico: nodo primario permanece BACKUP

Tras una conmutación puede ser normal que el primario tarde unos instantes en retomar MASTER. Si la situación persiste, comprobar que no está en mantenimiento persistente ni deshabilitado, examinar demotion y salud de interfaces, y verificar skew/configuración. No pulsar Reset Demotion como primera medida; suele ser mejor corregir el enlace o la causa que impide elegir al primario.

64.19. Diagnóstico: INIT o VIP ausente

El estado INIT o vacío suele apuntar a VIP no aplicada, enlace de interfaz caído o problema de asignación. Examinar el estado de interfaz, cableado, switch/VLAN y la configuración efectiva en Firewall → Virtual IPs. La documentación de Netgate también describe que, si hay enlace físico pero la VIP queda INIT, puede ser necesario volver a guardar y aplicar la configuración de esa VIP tras comprobar el resto del estado.

64.20. Captura de anuncios CARP sin alterar la política

En Diagnostics → Packet Capture seleccionar la interfaz física/VLAN donde se encuentra la VIP, un filtro de protocolo CARP y un número acotado de paquetes. En pfSense, la opción de vista para CARP permite interpretar los anuncios al descargar o consultar el resultado. Para un diagnóstico fiable, capturar por separado en ambos nodos, comparar origen, frecuencia y VHID, y proteger las capturas como datos sensibles.

Como alternativa avanzada, el manual oficial documenta «tcpdump -i <interfaz> -T carp carp», donde <interfaz> representa una interfaz real del entorno y no debe copiarse sin verificarla. El protocolo CARP es IP 112; no tiene sentido filtrar por puerto UDP 112. No es necesario habilitar modo promiscuo salvo que la topología de captura lo exija.



Figura 64.4. Orden de diagnóstico para incidencias CARP, pfsync y continuidad de los servicios.

64.21. Diagnóstico de pfsync y XMLRPC: no confundir síntomas

Síntoma	Origen probable	Comprobación dirigida
VIP cambia pero se cortan sesiones	Estados PF no sincronizados o rutas/NAT distintos.	IDs pfsync; estados; pruebas de tráfico.
La secundaria tiene reglas desactualizadas	Fallo de sincronización XMLRPC.	Avisos de sincronización y logs generales.
Duplicidad de MASTER	Fallo de anuncios CARP o configuración de grupo.	Captura CARP en cada segmento.
El secundario no sirve DNS	Servicio no escucha VIP o regla local ausente.	Interfaz, DNS Resolver y reglas.
No concede DHCP tras failover	HA de DHCP incompleta o retardo de failover.	Estado Kea, NTP, comunicación y logs.
IP alias no sigue a VIP	Dependencia o padre CARP incorrecto.	Firewall → Virtual IPs y configuración en ambos.

Un failover de direcciones no implica failover automático de todas las aplicaciones. Un servidor OpenVPN, IPsec o DNS puede requerir parámetros de escucha sobre VIPs, servicio activo y reglas correctas. La validación debe contemplar no solo el estado MASTER sino tráfico real antes y después del cambio.

64.22. Escenario práctico: salida empresarial redundante

Dos cortafuegos protegen una salida compartida y ofrecen a los equipos una misma puerta de enlace virtual. En operación normal, el principal es MASTER y la secundaria BACKUP. Una avería en el principal fuerza el traslado de la VIP; con pfsync configurado y NAT equivalente, parte de las sesiones pueden mantenerse. El procedimiento de aceptación comprueba navegación, resoluciones y aplicaciones sensibles al cambio de ruta.

64.23. Escenario práctico: servicios expuestos y VPN

La organización publica servicios por NAT sobre VIPs de WAN y dispone de una VPN corporativa. Durante el failover, la dirección pública virtual debe permanecer accesible y el nuevo propietario debe tener reglas NAT, certificados, interfaz de escucha y rutas adecuadas. La continuidad de una VPN depende de su implementación y estado; debe medirse en pruebas específicas, no inferirse del indicador MASTER.

64.24. Escenario práctico: HA virtualizada y trunk VLAN

Dos appliances virtuales comparten segmentos WAN y LAN a través de un hipervisor. Una política de seguridad de puerto o filtrado multicast impide que un nodo reciba anuncios del otro y ambos pasan a MASTER. La corrección exige comprobar switch virtual y físico, trunk, VLAN y políticas de MAC, nunca asumir que se trata de un fallo de pfsync simplemente porque la interfaz Sync responde a ping.

64.25. Buenas prácticas de explotación y control de cambios

Mantener versiones compatibles, inventario de VIPs, VHIDs no conflictivos, configuración de NTP, respaldo de reglas y pruebas de conmutación calendarizadas. Monitorizar cambios de rol inesperados y elevaciones de demotion; crear procedimientos explícitos de entrada y salida de mantenimiento. No reiniciar ambos equipos simultáneamente como método habitual de resolución de incidencias.

Reservar una ruta administrativa que no dependa exclusivamente de una VIP; proteger el segmento Sync de terceros; registrar intervenciones y limitarlas a ventanas autorizadas. En los informes, evitar nombres y direcciones reales, hashes, contraseñas CARP y capturas de tráfico sensibles. Anotar si los resultados se obtuvieron de las pantallas visibles o mediante documentación adicional.

64.26. Checklist técnico antes de dar por bueno el failover

Control	Criterio de aceptación	Resultado
CARP por VIP	Solo un MASTER y contraparte BACKUP.	☐
Estado físico	Enlaces y VLAN sin errores relevantes.	☐
Demotion	Sin penalización residual injustificada.	☐
pfsync	IDs de ambos nodos presentes cuando corresponda.	☐
XMLRPC	Sin errores de sincronización; configuración coherente.	☐
Servicios	DNS, NAT, salida y aplicaciones aceptadas en ambos roles.	☐
Reversión	Salida de mantenimiento validada y registrada.	☐

64.27. Glosario de alta disponibilidad

Término	Definición práctica
VIP	Dirección IP virtual que puede cambiar de nodo propietario.
MASTER	Nodo que atiende el tráfico para una VIP.

Término	Definición práctica
BACKUP	Nodo que monitoriza anuncios y no posee la VIP de forma activa.
INIT	Estado de inicialización o condición anómala de la VIP.
VHID	Identificador del grupo CARP dentro del segmento.
advskew	Fracción de intervalo que influye en prioridad de anuncios.
Demotion	Penalización dinámica que dificulta tomar MASTER.
pfsync	Protocolo de sincronización de estados del filtro PF.
XMLRPC	Mecanismo de sincronización de configuración entre equipos.
Split-brain	Dos nodos se consideran simultáneamente MASTER para la misma VIP.
IP Alias	VIP adicional que puede depender de una VIP CARP principal.

64.28. Plan de recuperación: cuándo detener una intervención

En una incidencia de alta disponibilidad, actuar sobre el estado CARP solo después de establecer cuál es el nodo que mantiene realmente el servicio y cuál es el alcance del fallo. Si la VIP aparece en MASTER en ambos equipos, la prioridad es contener el riesgo de respuestas duplicadas y recuperar la comunicación de los anuncios; forzar la elección sin entender la causa puede producir oscilaciones. Si uno de los nodos está en mantenimiento persistente, documentar el motivo antes de sacarlo de ese modo.

El procedimiento de recuperación debe tener tres vías separadas: una para el tráfico de los clientes que utilizan VIPs, otra para administrar las IP físicas de cada firewall y una tercera para comprobar la continuidad de los servicios dependientes. No depender únicamente del acceso por la dirección virtual: cuando una VIP cambia de propietario, la sesión administrativa y el camino de red del operador también pueden modificarse.

Situación durante la intervención	Decisión prudente	Condición para reanudar
Secundario no accesible por IP física	Detener ensayo de failover; investigar gestión y enlace.	Acceso administrativo a ambos nodos.
Ambos nodos MASTER	No activar operaciones de mantenimiento en ambos.	Anuncios CARP y grupo VHID verificados.
pfsync no replica estados	No prometer continuidad de sesiones existentes.	Sincronización comprobada en Status.
Se pierde servicio al ceder VIP	Revisar NAT, rutas, reglas y escucha de servicios.	Pruebas exitosas desde cliente controlado.
Una interfaz sigue penalizada	Corregir causa antes de resetear demotion.	Interfaz estable y valor explicado.

Como evidencia técnica, conservar una línea temporal mínima: estado previo de cada VIP, acción autorizada, momento de cambio de rol, mediciones de conectividad, estado de sincronización y resultado de reversión. Esta documentación permite distinguir una conmutación de dirección correcta de un fallo posterior de DNS, NAT o aplicación, y evita atribuir todos los cortes a CARP.

64.29. Referencias oficiales de Netgate

Las fuentes siguientes permiten ampliar las funciones, comportamientos y precauciones de CARP y pfsync. Los controles de clúster requieren una configuración de alta disponibilidad compatible:

[01] CARP Status — controles y estados

[02] High Availability — fundamentos

[03] High Availability Configuration Example

[04] High Availability Synchronization Settings

[05] Verifying Failover Functionality
[06] Troubleshooting High Availability
[07] CARP Virtual IP Options
[08] High Availability Prerequisites
[09] Components of a High Availability Cluster
[10] HA Troubleshooting — XMLRPC, pfsync, servicios
[11] Packet Capture GUI
[12] tcpdump on the Command Line
[13] Status Menu Guide
[14] Dashboard CARP Status Widget

Los textos y controles condicionales pueden variar con la versión, el modo de alta disponibilidad y la configuración. Los ejemplos son didácticos y no reproducen una instalación real.

65 Status → Dashboard

Supervisión integral · indicadores · widgets · rendimiento · VPN · gateways · diagnóstico

El Dashboard proporciona una vista consolidada del estado de pfSense Plus: inventario del sistema, señales de hardware, interfaces, gateways, sesiones VPN, almacenamiento y soporte. Está diseñado para orientar la vigilancia diaria, detectar desviaciones y ofrecer accesos rápidos; no sustituye la verificación detallada de conectividad ni el análisis de registros.

Entre los principales widgets de supervisión figuran System Information, Disks, Netgate Services and Support, Interfaces, OpenVPN y Gateways. Se estudian sus campos y operaciones de gestión, junto con otros widgets documentados por Netgate cuya disponibilidad depende de la configuración, los paquetes, la plataforma y la versión.

CONFIDENCIALIDAD Y ALCANCE Los esquemas y ejemplos utilizan únicamente denominaciones genéricas. Las direcciones reales, identidades de usuarios, números de serie, identificadores de dispositivo y otros datos operativos deben protegerse en los inventarios e informes.



Figura 65.1. Organización conceptual de los widgets visibles y sus dominios de supervisión.

65.1. Fundamento técnico y función operativa del Dashboard

El Dashboard es el punto de entrada a una instancia pfSense y también se alcanza desde Status → Dashboard. Reúne widgets independientes que combinan datos locales del sistema, estados de demonios, estadísticas PF, monitorización de gateways, contenido de paquetes instalados y, cuando corresponde, información consultada a los servicios de Netgate. La presencia de datos no implica una garantía de actualidad absoluta: algunos módulos se refrescan por AJAX y otros se calculan cuando se abre la página.

Su valor operativo aparece al correlacionar indicadores: una interfaz puede mantener enlace físico, mientras el monitor del gateway detecta pérdida; una VPN puede mostrar proceso activo pero carecer de rutas válidas; un uso de memoria elevado puede corresponder a caché y no a escasez de RAM. Una conclusión técnica requiere reunir varias observaciones y realizar una prueba desde el punto correcto de la red.

65.2. Ruta, alcance y acceso administrativo

Elemento	Función	Consideración
Status → Dashboard	Regresa a la página principal de supervisión.	No ejecuta por sí mismo un diagnóstico completo.
System → General Setup	Opciones generales de presentación del panel.	El número de columnas puede variar.
System → User Manager	Determinadas preferencias por usuario.	La disposición puede depender del usuario.

Elemento	Función	Consideración
Status → Gateways / Interfaces	Detalle de WAN, enlaces y métricas.	Mejor fuente para investigación específica.
Status → OpenVPN / System Logs	Estado de instancias VPN y eventos.	Correlacionar sesión con tráfico real.
System → Update	Actualizaciones, comprobación y opciones.	Cambiar/actualizar solo con plan de mantenimiento.

65.3. Controles globales y gestión de widgets

La cabecera del Dashboard incluye un botón «+» para abrir Available Widgets y un icono de ayuda «?». Los iconos disponibles pueden variar entre temas y versiones. Netgate documenta además el control «Save» de la cabecera cuando hay cambios de disposición que deban persistirse. La vista utilizada puede mostrar únicamente parte de los controles según su estado.

Control	Acción y efecto	Qué comprobar
«+» de la cabecera	Abre la lista de widgets disponibles para añadirlos.	Identificar el widget deseado; se recarga el panel.
Icono «?»	Acceso a ayuda contextual de la interfaz.	No altera la configuración del firewall.
Barra de título	Permite arrastrar y reorganizar las tarjetas.	Guardar ubicación mediante el control global.
Llave inglesa	Abre ajustes de un widget que los tenga.	Guardar dentro del panel de ajustes.
Círculo «−» / «+»	Contrae o expande el contenido del widget.	Guardar estado del diseño si corresponde.
Círculo «×»	Retira el widget del Dashboard.	No desinstala el servicio ni apaga la función.
Icono de actualización	Recarga datos del widget que lo proporciona.	No equivale a reiniciar un daemon.

INTERPRETACIÓN Quitar un widget no deshabilita Netgate Services, OpenVPN, monitorización ni otro subsistema. Para preservar el diseño, guardar cambios en la cabecera cuando el sistema lo indique.

65.4. System Information: identidad, plataforma y versión

El widget System Information es la referencia rápida para identificar la instalación y revisar su estado global. Incluye valores de inventario y de funcionamiento; varios son sensibles y no deben circular en informes públicos. La identificación puede proceder de hardware reconocido, hipervisor o plataforma no específica.

Campo visible	Qué representa	Lectura y cautela
Name	Nombre completo configurado en el sistema.	Identifica el equipo; no informa de salud.
User	Usuario autenticado y origen de autenticación.	Revisar privilegios y sesión compartida.
System	Modelo o tipo de plataforma; puede incorporar serial y NDI.	Identificadores operativos confidenciales.
BIOS	Proveedor, versión y fecha de firmware si son detectables.	Contrastar con avisos del fabricante.
Boot Environment	Entorno ZFS actual y próximo arranque, si es compatible.	En Plus con ZFS; no implica respaldo completo.
Version	Versión pfSense, arquitectura, build y base FreeBSD.	Verificar soporte y compatibilidad antes de actualizar.
Actualización	Resultado del control de nueva versión.	«Checking» no es fallo por sí mismo.

Campo visible	Qué representa	Lectura y cautela
CPU Type	Modelo, CPUs y posibles capacidades criptográficas.	No confundir número de CPU con rendimiento real.
Hardware crypto	Algoritmos o motores acelerados compatibles.	La presencia no garantiza uso en cada flujo.

El Netgate Device ID (NDI) se usa en funciones de soporte y administración de licencias; el número de serie es información de inventario. Ambos deben protegerse. El campo Boot Environment solo aparece si el sistema admite entornos de arranque ZFS; su estado «Current/Next» informa de la selección actual y del siguiente inicio, no de la existencia de un punto de restauración válido para todos los datos.

65.5. System Information: tiempo, DNS y cambios

Campo visible	Interpretación técnica	Qué hacer si es anómalo
Uptime	Tiempo transcurrido desde el último reinicio.	Relacionar con mantenimientos y logs.
Current date/time	Reloj local y zona horaria del firewall.	Confirmar NTP y zona antes de correlacionar eventos.
DNS Server(s)	Resolutores usados por el firewall, locales o externos.	Probar consultas con Diagnostics → DNS Lookup.
Last config change	Momento del último cambio registrado.	Consultar historial de configuración y autoría.
Boot Environment	Entorno activo/seleccionado en instalaciones compatibles.	Comprobar estado en System → Boot Environments.

Los resolutores listados pueden incluir loopback cuando DNS Resolver/DNS Forwarder atienden al firewall y servidores externos configurados o recibidos. Esto no demuestra por sí mismo que los clientes internos usen esas mismas direcciones. Un reloj desfasado puede afectar certificados TLS, correlación de eventos, autenticación y tareas programadas. La marca Last config change indica cuándo cambió la configuración, pero no explica qué se alteró ni si afectó a la conectividad.

65.6. System Information: tabla de estados, MBUF y carga

Indicador	Qué mide	Interpretación operativa
State table size	Estados del filtro PF en uso respecto al límite.	El porcentaje redondeado puede ocultar sesiones activas.
Show states	Enlace hacia el listado de estados.	Analizar pares origen/destino y reglas, con cautela.
MBUF Usage	Clústeres de buffers de memoria utilizados por la red.	Cercanía sostenida al límite puede causar problemas.
Load average	Promedio de carga del sistema en varias ventanas.	No es directamente un porcentaje de CPU.
CPU usage	Uso instantáneo del procesador.	La propia página puede elevar la medición.
Memory usage	RAM en uso, incluyendo usos legítimos de caché.	Comparar con presión de memoria y swap.
Swap usage	Intercambio a disco, si existe swap.	Crecimiento sostenido puede indicar presión RAM.
Temperature	Temperatura, si hay sensor compatible.	Interpretar con umbrales del fabricante.

PF crea estados para gestionar conexiones permitidas y sus retornos. Un contador alto no es necesariamente una incidencia si las tasas de creación, caducidad y memoria se mantienen estables; un máximo cercano combinado con pérdidas o latencia sí requiere atención. Los MBUF son buffers usados por la pila de red; agotarlos puede degradar la conectividad aun cuando el procesador no esté totalmente ocupado.

La carga promedio refleja procesos ejecutables o en espera según el sistema, mientras CPU usage mide actividad de procesador; los valores deben interpretarse en relación con el número de CPU, el tiempo y la naturaleza de la carga. En máquinas con pocos recursos, mantener el Dashboard abierto puede incrementar el uso observado. La RAM usada para cachés no equivale a memoria insuficiente: vigilar también swap, fallos de asignación y tendencias.



Figura 65.2. Indicadores de recursos que deben correlacionarse; barras exclusivamente ilustrativas.

65.7. Widget Disks: almacenamiento y estructura ZFS

El widget Disks muestra puntos de montaje o conjuntos de datos, tamaño, espacio ocupado y porcentaje de uso. En instalaciones ZFS permite desplegar niveles y datasets; el contenido depende del diseño del sistema, dispositivo y versión. La capacidad total visible puede reflejar un conjunto o sistema de archivos concreto y no toda la capacidad física del soporte.

Columna / control	Significado	Acción recomendable
Mount	Punto de montaje o dataset seleccionado.	Expandir si existe una jerarquía de ZFS.
Used	Cantidad de espacio utilizado.	Comparar evolución con días anteriores.
Size	Capacidad presentada para ese volumen.	Tener en cuenta cuotas y reservas ZFS.
Usage	Barra/porcentaje de ocupación.	Evaluar crecimiento y umbrales de alerta.
«>» / expansión	Muestra detalles de niveles inferiores.	No modifica discos ni particiones.
Llave inglesa	Ajustes de elementos fijados/umbral cuando existen.	Evitar ocultar datasets críticos.

Los porcentajes de uso de disco deben correlacionarse con registros, snapshots, paquetes instalados y bases locales. Un porcentaje bajo no sustituye una comprobación de integridad del almacenamiento; para estado de pools, considerar widget ZFS y herramientas específicas. No borrar instantáneas ni logs de forma improvisada para liberar espacio.

65.8. Netgate Services and Support: contrato y disponibilidad

El widget Netgate Services and Support consulta información del estado de soporte del firewall a través de los servicios de Netgate. Sus campos incluyen Contract Type y Support Status, junto con un icono de actualización de la consulta cuando está disponible. Los nombres exactos de los planes y derechos de soporte dependen del equipo, licencia y contrato contratado.

Campo / control	Qué representa	Precaución
Contract Type	Modalidad de cobertura asociada a la instalación.	No inferir SLA ni canales sin consultar contrato.

Campo / control	Qué representa	Precaución
Support Status	Estado del soporte comunicado por Netgate.	La ausencia de respuesta no prueba expiración.
Actualizar	Repite la consulta cuando el widget lo ofrece.	Requiere conectividad/DNS apropiados.
NDI	Identificador que Netgate usa para consultas.	No compartirlo públicamente.

El panel no demuestra que cualquier incidente tenga cobertura completa: el alcance depende del contrato. Si el estado no se actualiza, separar un posible problema de conectividad a servicios de Netgate de un cambio real de cobertura. Las comprobaciones automáticas de actualizaciones también generan comunicaciones HTTPS autorizadas a servidores de Netgate; revisar la política corporativa de privacidad y salida.

65.9. Interfaces: enlace, velocidad, direcciones y tipos

El widget Interfaces resume las interfaces administradas por pfSense. Las filas pueden representar WAN, LAN, interfaces OPT, VLAN o puertos de switch integrados según hardware. Muestra iconos de estado, velocidad y modo dúplex cuando están disponibles, además de direcciones IPv4/IPv6 o marcadores de ausencia. Una denominación de interfaz es etiqueta lógica: no basta para deducir cableado ni ubicación física.

Señal visible	Significado	Lo que NO demuestra
Flecha hacia arriba	Interfaz/enlace en estado operativo según la GUI.	No garantiza Internet, DNS ni ruta correcta.
Flecha hacia abajo	Interfaz no activa o sin estado esperado.	No identifica por sí sola si falla cable o operador.
Icono de error / X	Interfaz no disponible o no operativa, según su tipo.	No autoriza a eliminar su configuración.
Velocidad / dúplex	Negociación Ethernet reportada por el sistema.	No equivale al caudal real disponible.
IPv4/IPv6 / n/a	Direcciones configuradas o ausencia de una dirección.	«n/a» puede ser normal en puertos no L3.
Nombre clicable	Acceso a detalle de interfaz según widget.	No implica cambios sin acceder a configuración.

Si una WAN informa enlace «up» y el gateway está en fallo, comprobar primero el monitor, resolución, rutas y conectividad externa. Si una interfaz aparece sin velocidad («none»), revisar su tipo, estado, transceptor, cableado o si se trata de un enlace lógico. Los puertos con función de switch pueden no tener una IP individual; no debe interpretarse «n/a» como avería.

65.10. Gateways: RTT, RTTsd, pérdida y estado

La tabla Gateways refleja el resultado del subsistema de monitorización de gateways. La métrica RTT es el tiempo de ida y vuelta; RTTsd expresa dispersión o desviación típica de la latencia medida y aproxima su variabilidad (no representa un test completo de jitter de aplicaciones); Loss es la fracción de sondas perdidas en la ventana observada. Las mediciones dependen del destino configurado para monitorización y de sus umbrales.

Columna	Lectura correcta	Posible problema / verificación
Name	Nombre lógico y referencia al gateway.	Confirmar que monitoriza el enlace previsto.
RTT	Latencia observada mediante sondas.	Si crece, comparar con otras horas/destinos.
RTTsd	Variabilidad estadística del retardo.	Puede anticipar inestabilidad con RTT medio bajo.

Columna	Lectura correcta	Posible problema / verificación
Loss	Porcentaje de sondas sin respuesta.	No equivale exactamente a pérdida de toda aplicación.
Online	Monitor cumple condiciones de disponibilidad.	Comprobar servicio real y rutas del cliente.
Warning	Condición degradada conforme a umbrales.	Correlacionar RTT/Loss y logs de gateway.
Down	El monitor considera la ruta no disponible.	Verificar enlace, IP de monitor y rutas.
Unknown / Pending	Datos insuficientes o monitor aún no establecido.	No confundir con prueba positiva ni fallo definitivo.

En entornos Multi-WAN es importante comprobar también el gateway por defecto, los grupos, los umbrales y las políticas de routing. Un gateway «Unknown» podría deberse a una interfaz no activa, monitor en arranque, monitorización deshabilitada o estado transitorio, según configuración; la explicación definitiva debe buscarse en Status → Gateways y sus logs. Un gateway «Online» no acredita conectividad con todos los destinos remotos ni con cada servicio.

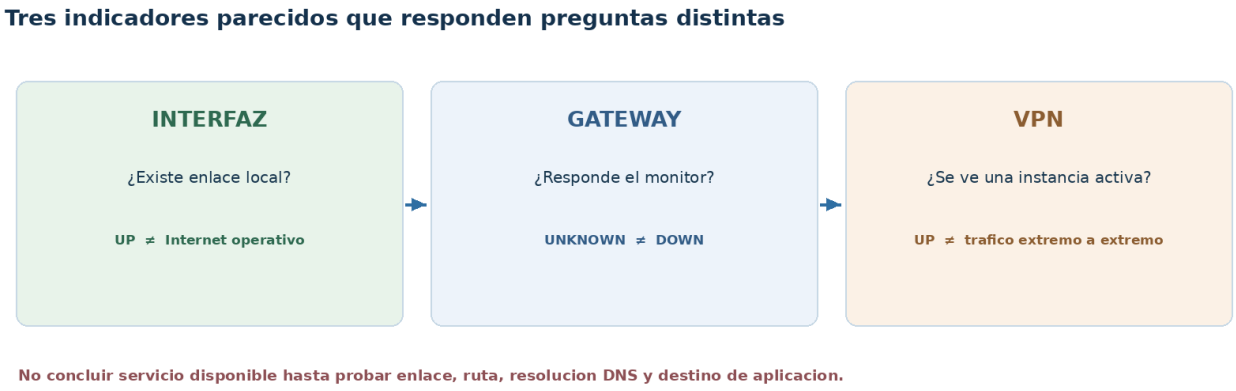


Figura 65.3. Diferencia entre estado de interfaz, monitor de gateway y servicio VPN.

65.11. OpenVPN: instancias, conexión, tráfico y tiempo

El widget OpenVPN presenta servidores y clientes configurados. El formato varía según el modo de la instancia: en un servidor SSL/TLS puede listar usuarios conectados, mientras que en peer-to-peer muestra un estado de enlace. En las instancias cliente puede aparecer el bloque Client Instance Statistics con nombre de instancia y protocolo, extremo remoto o dirección virtual, instante de conexión e icono de estado.

Elemento	Interpretación técnica	Validación
Client Instance Statistics	Grupo de instancias OpenVPN actuando como clientes.	Consultar Status → OpenVPN para estados completos.
Name / Time	Nombre de instancia y marca temporal asociada.	No equivale a duración garantizada de sesión.
Remote / Virtual IP	Extremo remoto y direccionamiento virtual relacionado.	Proteger estos datos como información de red.
Flecha verde / estado	Instancia aparentemente conectada.	No asegura rutas, DNS ni acceso al destino.
Protocolo / modo	Transporte configurado (según widget).	Comprobar puerto, certificados y cifrado en configuración.

Cuando un túnel está levantado pero no circula tráfico útil, seguir la cadena: tabla de rutas → reglas de firewall → NAT si procede → redes remotas → DNS de clientes → logs OpenVPN. No reiniciar una instancia usada por sedes o teletrabajadores únicamente para corregir un icono sin corroborar la pérdida real del servicio.

65.12. Correlación de indicadores: cuatro ejemplos frecuentes

Observación combinada	Hipótesis inicial	Prueba no destructiva
Interfaz UP, gateway Down	Enlace local sí; salida/monitor no.	Ping a monitor y a otro destino desde origen correcto.
OpenVPN UP, aplicaciones caídas	Fallo de rutas, reglas o destino.	Traceroute y prueba por IP y DNS en cada extremo.
CPU alta, estados normales	Tarea puntual, logging o cifrado.	Tendencia de CPU y procesos; comparar horarios.
RAM alta, disco normal	Caché o presión de RAM; no inferir.	Swap, procesos, errores de memoria.
Support no disponible, WAN Online	Problema selectivo HTTPS/DNS/servicio remoto.	Consultar Netgate y verificar resolución TLS.
Disco crece y logs muy activos	Crecimiento de registros/snapshots.	Tamaño por dataset y rotación configurada.

65.13. Procedimiento: auditoría de salud diaria

01 Abrir Status → Dashboard con cuenta individual de mínimo privilegio; confirmar que se está en la instancia esperada.

02 Verificar reloj, zona horaria, uptime, versión y resultado de actualización sin ejecutar cambios.

03 Comprobar State table, MBUF, CPU, RAM, swap si existe y espacio de discos, anotando tendencias.

04 Comparar Interfaces con Gateways: enlaces operativos, métricas RTT/RTTsd/Loss y estados transitorios.

05 Revisar el estado de las VPN relevantes y comprobar al menos un destino de cada clase crítica.

06 Consultar System Logs y Status → Services ante alertas; verificar la última modificación de configuración.

07 Registrar hallazgos anónimos, fecha de muestreo, evidencia y responsable de seguimiento.

65.14. Procedimiento: fallo de conectividad WAN

01 Anotar qué usuario o aplicación falla y si el problema afecta a una sede, una VLAN o toda la organización.

02 Verificar estado físico de la WAN en Interfaces; si no hay enlace, revisar operadora, puerto y cabling autorizado.

03 Abrir Status → Gateways para comprobar monitor, pérdida, RTT, gateway efectivo y eventos.

04 Usar Diagnostics → Ping desde la interfaz apropiada con un destino de prueba controlado, después otro independiente.

05 Comparar resolución DNS con conectividad directa por IP y comprobar políticas Multi-WAN si existen.

06 Correlacionar logs de firewall y gateway; evitar modificar rutas o reiniciar el firewall antes de identificar la causa.

07 Después de cualquier ajuste autorizado, repetir pruebas y consignar resultado y plan de reversión.

65.15. Procedimiento: VPN figura UP pero no comunica

01 Comprobar el widget OpenVPN y después Status → OpenVPN para estado detallado, reconexiones y sesiones.

02 Confirmar red del túnel y rutas esperadas desde pfSense y desde un equipo de prueba en cada extremo.

03 Verificar en Firewall → Rules las reglas de interfaz OpenVPN o interfaz asignada; revisar NAT cuando aplique.

04 Probar conectividad a IP del destino; si funciona, probar DNS y dominios internos.

05 Correlacionar logs, tiempos de reconexión y cambios recientes de configuración.

06 Escalar con información mínima suficiente, sin exportar certificados, claves o configuraciones sensibles.

65.16. Administración de la disposición: procedimiento reproducible

01 En el Dashboard hacer clic en «+» y seleccionar un widget documentado que aporte un indicador nuevo.

02 Arrastrar su barra de título a la columna deseada, verificando que no oculta tarjetas más críticas.

03 En widgets con llave inglesa, abrir ajustes y establecer umbrales o elementos a mostrar cuando existan.

04 Minimizar un widget de consulta secundaria mediante «−», o eliminarlo del panel con «×» si es innecesario.

05 Pulsar Save en los controles de cabecera para persistir disposición o estado.

06 Recargar la página y confirmar que el diseño elegido continúa disponible.

Netgate enumera widgets adicionales, entre ellos CARP Status, Captive Portal Status, Dynamic DNS, Firewall Logs, Interface Statistics, IPsec, NTP, Services Status, Traffic Graphs, Wake On LAN, Installed Packages, ZFS y Thermal Sensors. Su disponibilidad depende del sistema, los servicios configurados y los paquetes instalados; no todos se muestran simultáneamente en una distribución habitual del Dashboard.

65.17. Configuración recomendada de un panel de operaciones

Zona	Widgets prioritarios	Objetivo
Alta / siempre visibles	System Information, Interfaces, Gateways	Detectar cambios de conectividad y recursos.
VPN / sedes	OpenVPN, IPsec, WireGuard si existen	Detectar caída de instancias y sesiones.
Rendimiento	Disks, Traffic Graphs, Interface Statistics	Detectar tendencias de saturación.
Seguridad y servicios	Firewall Logs, Services Status	Revisar eventos y demonios.
HA / plataforma	CARP Status, ZFS, Thermal Sensors según soporte	Valorar redundancia y estado físico.

Es preferible un panel breve y útil a una pantalla sobrecargada que eleve CPU o dificulte reconocer incidencias. No concentrar toda la supervisión en una única sesión web: para alertas y series históricas usar sistemas adecuados de monitorización, como SNMP autorizado, syslog remoto, métricas y registros centralizados.

65.18. Alertas de capacidad: criterios de decisión, no umbrales universales

Los colores y barras del Dashboard son una representación de métricas locales; sus umbrales no siempre equivalen a compromisos de rendimiento empresariales. La política de alertas debe basarse en hardware, carga habitual y nivel de servicio. Se recomienda actuar sobre cambios sostenidos y correlacionados: incremento de RTT junto a pérdida, MBUF cerca del máximo con errores de red, saturación de disco con fallos de escritura o aumento de CPU coincidente con latencia de VPN.

No recomendar porcentajes fijos universales sin validar el contexto. Un pico de CPU durante actualización, comprobación de paquetes o cifrado puede ser normal, mientras una pérdida reducida pero constante en un enlace de voz puede ser crítica. Documentar líneas base y variabilidad por horario.

65.19. Seguridad y privacidad del Dashboard

La pantalla puede revelar hostnames, identidades de usuario, IPs, seriales, NDI, versiones de firmware, endpoints VPN, información de soporte y topología. Controlar quién accede al webConfigurator, usar HTTPS y MFA donde proceda, revisar privilegios, limitar sesiones compartidas y aplicar protección de datos en reportes y tickets. Una captura de Dashboard no es un material público inocuo.

Para compartir resultados con proveedores o documentar incidencias, redactar inventario técnico mínimo y sustituir IPs por rangos reservados 192.0.2.0/24, 198.51.100.0/24 o 203.0.113.0/24 y dominios example.com cuando se necesiten ejemplos. No conservar credenciales, identificadores únicos, usuarios ni certificados en propiedades del documento.

ADVERTENCIA DE CAMBIO Las acciones de mantenimiento no se ejecutan desde el Dashboard como primer paso. Reiniciar servicios, alterar gateways, instalar actualizaciones o cambiar interfaces puede cortar la administración, los túneles VPN y las aplicaciones corporativas.

65.20. Escenarios prácticos de explotación empresarial

65.20.1. Empresa con dos enlaces de Internet

La WAN principal muestra enlace activo, pero el widget Gateways señala pérdida persistente y el grupo Multi-WAN conmuta el tráfico. El operador debe comprobar el monitor y la ruta realmente aplicada, después validar DNS, acceso a Internet y continuidad de las aplicaciones desde una VLAN de prueba. El estado «up» de la tarjeta física no contradice la degradación de la conectividad externa.

65.20.2. Oficina enlazada mediante OpenVPN

El indicador VPN permanece conectado, pero un servicio alojado en la sede remota deja de responder. La investigación se dirige a rutas, ACL, NAT, túnel y DNS antes que a certificados; el Dashboard solo presenta el punto de partida. Se validan los equipos por IP y posteriormente por nombre para separar conectividad y resolución.

65.20.3. Instalación con ZFS y crecimiento de logs

El espacio disponible cae en varias semanas sin señales evidentes en CPU. El widget Disks permite detectar el volumen afectado; el administrador confirma datasets y snapshots por las herramientas adecuadas y ajusta retención según política. No borra archivos arbitrariamente ni reduce registros antes de preservar la evidencia necesaria.

65.21. Matriz de resolución de incidencias

Síntoma	Posibles causas	Orden de comprobación
Un widget no carga	AJAX, sesión, DNS, backend o permiso.	Recargar página, revisar logs y estado del servicio.
Update check bloqueado	Salida HTTPS, DNS o servidor remoto.	Probar resolución, TLS, proxy y System → Update.
Gateway Unknown	Sin datos, monitor no disponible, estado transitorio.	Abrir Status → Gateways y ver configuración de monitor.
Interfaz Down	Enlace físico, puerto deshabilitado, interfaz lógica.	Cable/transceptor, estado, VLAN y errores.
OpenVPN UP, destino inaccesible	Ruta, reglas, DNS, NAT o destino.	Prueba por IP, rutas y logs de OpenVPN.
RAM alta	Caché normal o presión real.	Swap, memoria libre disponible y tendencias.
MBUF alto	Demanda de buffers o límites de memoria red.	Vigilar errores/agotamiento y hardware tuning.
Discos con poco espacio	Logs, snapshots, datos, paquetes.	Uso por volumen; política de retención.



Figura 65.4. Método de diagnóstico en cinco etapas, sin actuar sobre la producción a ciegas.

65.22. Checklist de validación para el responsable de sistemas

Comprobación	Criterio de aceptación	Registro
Identidad y versión	Instancia correcta, versión reconocida, sin exposición de IDs.	☐
Reloj y DNS	Hora coherente, resolución local y externa esperadas.	☐
Interfaces	Estado físico y direccionamiento esperados.	☐
Gateways	Monitores con RTT/Loss interpretados correctamente.	☐
VPN	Instancias críticas y tráfico funcional validados.	☐
Estados / MBUF / CPU	Sin degradación sostenida no explicada.	☐
Discos y ZFS	Espacio de volúmenes y salud de almacenamiento comprobados.	☐
Soporte y cambios	Estado de soporte verificado y cambios revisados.	☐
Evidencia	Resultado registrado sin datos identificativos.	☐

65.23. Glosario técnico aplicado al Dashboard

Concepto	Definición útil
Widget	Tarjeta configurable que presenta un subconjunto de indicadores.
AJAX	Actualización parcial de contenido web sin recargar toda la página.
NDI	Identificador de dispositivo usado por Netgate para determinados servicios.
State table	Tabla de estados de conexiones administrada por PF.
MBUF	Buffer de memoria usado por la pila de red del sistema operativo.
RTT	Tiempo de ida y vuelta de una sonda de monitorización.
RTTsd	Desviación típica de mediciones RTT; expresa variabilidad.

Concepto	Definición útil
Packet loss	Porcentaje de sondas de monitorización no respondidas.
Dataset ZFS	Unidad lógica de almacenamiento con propiedades propias.
Boot Environment	Entorno de arranque ZFS usado para gestionar cambios y reversión en Plus.
Dúplex	Capacidad de comunicación bidireccional simultánea en Ethernet.
VPN peer	Extremo remoto que participa en un túnel cifrado.

65.24. Referencias oficiales y documentación verificable

Las fuentes siguientes fundamentan la gestión de widgets y la interpretación de datos. La presencia de determinados widgets y controles depende de la versión, la plataforma, los paquetes y los servicios configurados.

[01] Dashboard — conceptos y personalización

[02] Managing Widgets — añadir, mover, minimizar, eliminar y guardar

[03] Available Widgets — campos y funciones por widget

[04] Status Menu Guide

[05] Interface Status — estados y contadores

[06] Gateway Status — monitorización y valores

[07] OpenVPN Server and Client Status

[08] Troubleshooting OpenVPN

[09] Service Status

[10] Boot Environment Status

[11] Contact with Netgate Servers

[12] Upgrade Guide — Dashboard check

[13] pfSense Plus — funciones específicas

[14] System Monitoring — navegación

Los controles del Dashboard dependen del hardware, los paquetes, el tema de interfaz, las preferencias del usuario y la versión de pfSense Plus. Los números y esquemas ilustrativos son didácticos y no describen una instalación en servicio.

66 Status → DHCP Leases

Concesiones IPv4 · búsqueda · asignaciones estáticas · ocupación · diagnóstico · alta disponibilidad

La supervisión de concesiones DHCP es una herramienta central de administración: permite identificar qué dirección recibió un equipo, durante qué período, si existe un registro de asignación estática y qué acciones ofrece la interfaz. Sus datos deben interpretarse junto con la tabla ARP, los registros del servicio y las pruebas de conectividad.

El alcance de esta pantalla se concentra en DHCPv4. La administración del servidor reside en Services → DHCP Server y las concesiones IPv6 se consultan separadamente en Status → DHCPv6 Leases. Los elementos disponibles pueden variar según el backend DHCP, la configuración HA y la versión instalada.



Figura 66.1. Una concesión vigente, una entrada ARP y la conectividad efectiva son evidencias distintas.

66.1. Función operativa y conceptos previos

Una concesión (lease) es la asignación temporal de una dirección IPv4 por un servicio DHCP a un cliente identificado por los atributos que utiliza el backend. El servidor mantiene plazos, opciones de red y estado de asignación; el cliente puede renovar o solicitar otra dirección. La página de estado no sustituye un inventario de activos ni demuestra propiedad o legitimidad del equipo.

Concepto	Qué expresa	Qué NO garantiza
Concesión activa	Existe un registro con vigencia actual	El host está encendido
Online	Hay evidencia de presencia en ARP	Responde aplicaciones o Internet
Asignación estática	Existe una correspondencia configurada	La MAC es una identidad segura
Utilización	Direcciones consumidas en un pool	Número exacto de equipos físicamente activos

66.2. Ruta de acceso, permisos y relación con otras pantallas

Ruta: Status → DHCP Leases. La sección Search filtra registros; Leases presenta las filas y las acciones; Lease Utilization resume el consumo. La configuración del servidor y de mapeos estáticos se encuentra en Services → DHCP Server, mientras los registros de solicitudes se consultan en Status → System Logs, apartado DHCP.

Ruta	Propósito	Uso principal
Status → DHCP Leases	Consultar concesiones IPv4	Inventario operativo y acciones sobre registros
Services → DHCP Server	Administrar pools y opciones	Cambios planificados; potencial impacto
Diagnostics → ARP Table	Contrastar presencia ARP	Investigar indicadores Online/Offline
Status → System Logs → DHCP	Revisar peticiones y errores	Diagnóstico de DORA, renovación y rechazos
Status → DHCPv6 Leases	Consultar concesiones IPv6	No mezclar con DHCPv4

PRIVILEGIOS Limitar las acciones que modifican el servicio y las asignaciones a operadores autorizados. La mera consulta de un registro no exige borrar concesiones ni reiniciar demonios.

66.3. Fundamento DHCP: ciclo DORA y renovación

En la negociación IPv4 ordinaria el cliente emite DHCPDISCOVER, el servidor responde con DHCPOFFER, el cliente selecciona mediante DHCPREQUEST y el servidor confirma con DHCPACK. También existen DHCPNAK, DHCPRELEASE y solicitudes de renovación, por lo que no todos los intercambios reproducen exactamente la secuencia inicial.



Figura 66.2. Esquema simplificado del intercambio DHCPv4 (habitualmente UDP 67/68).

La duración de una concesión depende de la configuración del servidor. Conceptualmente, los clientes suelen intentar renovar hacia la mitad de la duración (T1) y renovar con alcance ampliado más tarde (T2), según los temporizadores recibidos; no es correcto deducir el estado del cliente únicamente a partir de las horas Start y End. Al vencer, la asignación puede reutilizarse siguiendo la lógica del backend.

66.4. Panel Search: controles y expresiones regulares

En la pantalla estudiada, Search contiene un campo Search Term, un selector de alcance mostrado inicialmente como All y dos botones: Search y Clear. El texto de ayuda admite una cadena o expresión regular de sintaxis *nix; el resultado filtra los registros que aparecen en la tabla.

Control visible	Comportamiento documentado	Recomendación
Search Term	Texto de búsqueda o patrón de expresión regular Unix	Preferir texto simple salvo necesidad específica
Selector All	Búsqueda en todos los campos; puede restringirse a un campo	Elegir IP, MAC o nombre según el caso; opciones dependen de la vista
Search	Aplica el filtro	No modifica la base de concesiones
Clear	Limpia el criterio de búsqueda en la interfaz	No confundir con Clear All DHCP Leases
Icono de contraer −	Pliega visualmente el bloque de búsqueda	No cambia la configuración de DHCP

Ejemplo profesional: buscar un sufijo de hostname o una MAC parcial para identificar registros asociados a un equipo. Una búsqueda sin coincidencias no demuestra que el cliente no exista: puede figurar como concesión inactiva, usar otra MAC, pertenecer a otra interfaz o utilizar un servidor DHCP externo.

66.5. Tabla Leases: columnas e interpretación

Columna	Significado técnico	Observaciones
Estado sin título	Iconos de tipo de concesión y presencia ARP	Consultar tooltip para la variante exacta
IP Address	IPv4 concedida o definida en mapeo estático	No verifica unicidad real fuera de DHCP
MAC Address	Dirección física declarada/observada del cliente	Puede cambiar por privacidad o virtualización
Hostname	Nombre enviado por el propio cliente	Dato no autenticado; no es DNS necesariamente

Columna	Significado técnico	Observaciones
Description	Descripción administrativa de mapeos estáticos	Puede estar vacía en dinámicos
Start	Inicio registrado del plazo	En estáticas puede figurar n/a
End	Vencimiento registrado del plazo	No equivale a desconexión física
Actions	Atajos sobre mapeos, WOL o borrado	Depende del tipo y del estado de la fila

Los valores de Start y End deben relacionarse con la zona horaria del sistema y, cuando corresponda al backend ISC, con la opción específica de formato horario. Una dirección visible en una fila puede no ser la dirección que el dispositivo usa en ese preciso instante si estática/manual, cambió la red o la interfaz ARP se ha actualizado.

66.6. Iconos de concesión: Static, Active, Expired

Clase	Interpretación	Intervención prudente
Static	Registro derivado de un mapeo configurado	Editar desde su formulario, no borrar a ciegas
Active	Concesión temporal todavía vigente	Correlacionar con cliente y registro
Expired	Venció antes de renovarse	No implica siempre equipo apagado

La primera columna puede mostrar dos símbolos distintos: uno relacionado con el tipo de lease y otro con la presencia ARP. Los colores y dibujos pueden variar por versión; pasar el cursor por cada icono revela su significado concreto. No es correcto interpretar todas las flechas verdes como prueba de que una aplicación responde.

66.7. Online/Offline y tabla ARP: cómo evitar diagnósticos erróneos

Netgate documenta que el indicador Online se basa en la presencia de la MAC en la tabla ARP local del firewall. Una concesión activa puede figurar Offline si el equipo no ha contactado recientemente con pfSense, aunque tenga conectividad con otros dispositivos; también puede quedar presencia ARP durante un tiempo tras apagarlo.

1. Comprobar en Status → DHCP Leases el tipo y vigencia de la concesión.
2. Abrir Diagnostics → ARP Table y localizar la IPv4 y la MAC esperada.
3. Si procede, emitir ping desde Diagnostics → Ping y repetir la comprobación ARP.
4. Comparar IP, máscara, VLAN e interfaz del cliente con el segmento esperado.
5. Si se trata de una red remota a través de relay, distinguir el tráfico local de la presencia ARP observada en el segmento del firewall.

CRITERIO DE DIAGNÓSTICO Ni un estado «offline» ni un ping fallido bastan para concluir que un dispositivo está apagado; puede filtrar ICMP o no haberse comunicado a través del firewall.

66.8. Actions: convertir concesión dinámica en asignación estática

El icono de más de contorno (Add static mapping) de una concesión lleva al editor de mapeos estáticos y precarga la dirección MAC. El administrador debe revisar la interfaz correcta, la dirección solicitada y las opciones de red antes de guardar. Un registro prellenado es un punto de partida, no una reserva automáticamente aplicada.

1. Localizar la concesión correspondiente y confirmar físicamente la identidad del equipo.
2. Pulsar Add static mapping en esa fila.
3. Comprobar MAC, interfaz y nombre; seleccionar una dirección adecuada fuera del pool cuando el comportamiento del backend así lo requiera.
4. Guardar, aplicar cambios si la interfaz lo solicita y revisar que no haya solapamientos.
5. Renovar la concesión en el cliente y comprobar el resultado en la tabla, sin alterar otros dispositivos.

En ISC DHCP, los mapeos estáticos dentro del pool no excluyen automáticamente la IP de asignaciones dinámicas y pueden producir conflictos. La documentación de Netgate indica como buena práctica utilizar

direcciones fuera del rango para este backend y la GUI aplica esa validación. Con Kea deben verificarse las reglas y reservas propias del backend.

66.9. Actions: editar un mapeo estático existente

Cuando la fila representa un registro estático, el icono de lápiz permite abrir su editor. Si el dispositivo ha cambiado de NIC, de segmento o de política DNS, modificar únicamente los parámetros planificados. Una descripción administrativa coherente facilita auditoría, pero no sustituye la documentación de activos.

66.10. Actions: Wake-on-LAN y entradas persistentes WOL

La vista de concesiones puede ofrecer un botón de encendido (envío directo de Magic Packet) para equipos marcados Offline y otro icono con signo más para crear una entrada persistente de Wake-on-LAN. La disponibilidad del envío depende de la presencia ARP y de otras condiciones de la instalación; los iconos no equivalen a un reinicio remoto garantizado.

Acción	Resultado esperado	Limitación
Enviar WOL	Transmite paquete especial a la MAC	La NIC/BIOS/energía deben soportarlo
Añadir entrada WOL	Guarda MAC e identificación en Services → Wake-on-LAN	No confirma arranque
Consultar WOL	Volver a Services → Wake-on-LAN	Puede requerir que la entrada de lease siga visible

66.11. Actions: eliminación individual de concesiones inactivas

Netgate limita el borrado manual por fila a concesiones expiradas o inactivas; no está disponible para leases activas ni mapeos estáticos. Suprimir un registro no fuerza necesariamente al host a soltar inmediatamente la dirección ya configurada; tras la operación debe observarse la negociación DHCP y la presencia real en la red.

66.12. Mostrar todas las concesiones: alcance de la lista

La vista predeterminada enseña concesiones activas y estáticas. Show All Configured Leases amplía el listado a registros inactivos y vencidos; el control cambia a Show Active and Static Leases Only para restaurar la selección predeterminada. Esto modifica la presentación, no renueva, borra ni reserva direcciones.

66.13. Lease Utilization: lectura de la ocupación y capacidad

La tabla Lease Utilization muestra Interface, Pool Start, Pool End, Used, Capacity y Utilization. El denominador se corresponde con la cantidad de direcciones asignables del pool presentado, no automáticamente con el tamaño completo de la subred CIDR. En varios pools o interfaces deben interpretarse los resultados individualmente.

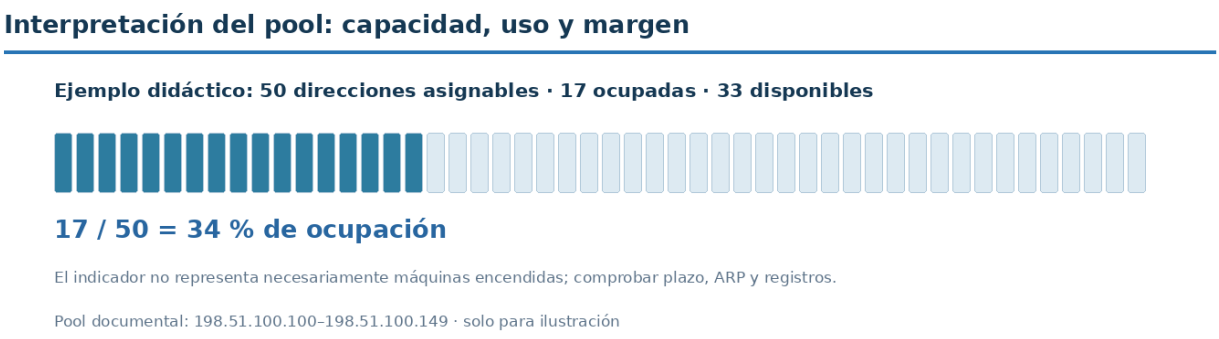


Figura 66.3. Relación entre direcciones ocupadas y libres en un pool documental.

Indicador	Lectura práctica	Posible error
Interface	Segmento al que pertenece el pool	Asumir que toda la LAN usa una sola red

Indicador	Lectura práctica	Posible error
Pool Start / End	Extremos inclusivos del rango configurado	Contar la red completa en lugar del pool
Used	Entradas que ocupan capacidad en el pool	Equipararlo al número de dispositivos online
Capacity	Total de direcciones potencialmente asignables	Ignorar exclusiones u otros pools
Utilization	Proporción Used/Capacity representada en barra	Tomar una ocupación puntual como previsión

En el ejemplo la capacidad es de 50 direcciones y 17 están ocupadas: 17 / 50 × 100 = 34 %. Un porcentaje alto sugiere examinar renovación, tiempo de lease, volumen de clientes y crecimiento; no justifica eliminar masivamente las concesiones como primera respuesta.

66.14. Clear All DHCP Leases: funcionamiento exacto y riesgo

El control rojo Clear All DHCP Leases no es un simple filtro ni una recarga de la pantalla. Netgate indica que detiene el demonio DHCP, elimina la base íntegra de leases dinámicas y vuelve a iniciar el servicio. No elimina los mapeos estáticos. Los clientes que mantienen una dirección todavía pueden seguir utilizándola hasta que necesiten renovar, por lo que se requiere supervisión posterior para evitar situaciones inesperadas.

> **ADVERTENCIA CRÍTICA** No utilizar Clear All DHCP Leases como método rutinario para «limpiar» una red. Puede afectar renovaciones, asignaciones y disponibilidad del servicio; el impacto depende de clientes, backend y alta disponibilidad.

1. Identificar el problema concreto y descartar agotamiento del pool, cliente con IP manual, ARP obsoleta o segundo servidor DHCP.
2. Registrar estado previo, backend, alta disponibilidad, rangos, leases relevantes y comunicaciones afectadas.
3. Disponer de ventana de mantenimiento, copia de configuración y mecanismo de recuperación.
4. Ejecutar la operación solo si existe justificación técnica y autorización para interrumpir el servicio.
5. Comprobar que el demonio vuelve a funcionar, observar nuevas solicitudes y validar equipos de prueba; revisar ambos nodos cuando hay HA.

66.15. Controles superiores e iconografía de la página

La cabecera incluye acceso a ayuda, vistas de estado y controles de actualización, con iconos cuya disponibilidad depende de versión y permisos. Su función exacta debe confirmarse mediante el texto emergente de cada icono. El símbolo de pausa/detención visible en algunas interfaces no debe confundirse con el botón rojo Clear All DHCP Leases. Los controles de acciones sobre filas pertenecen a la tabla Leases; el signo «+» de WOL y el de asignación estática tienen destinos distintos.

66.16. Backend DHCP: Kea frente a ISC DHCP

Aspecto	Kea DHCP	ISC DHCP
Evolución	Backend actual y desarrollado activamente	Backend heredado y deprecado
Ubicación de estado HA	Sección al final de las leases	Pool Status al inicio, si hay failover
Registro DNS	Integración dinámica y específica de Kea	Comportamiento y opciones heredados
Mapeos	Reservas y opciones de Kea según configuración	Las estáticas dentro del pool implican riesgos
Migración	Requiere plan y validación de HA	No mantener como solución futura por inercia

La selección del backend se realiza en System → Advanced → Networking, Server Backend. El administrador no debe deducir cuál está activo solo por un icono de la vista DHCP Leases. Cambiarlo es una operación de configuración y migración, no un ajuste de la pantalla de estado.

66.17. Alta disponibilidad: estado con ISC DHCP

Si se utiliza ISC DHCP con failover, Netgate documenta un bloque Pool Status en la parte superior de la pantalla. Los campos Failover Group, My State, Since, Peer State y Since muestran el nombre del pool y el estado local y remoto. Los estados de sincronización deben leerse de forma bilateral: un nodo aislado puede presentar una visión incompleta de su compañero.

66.18. Alta disponibilidad: Kea DHCP y estados de nodos

Campo/estado	Interpretación operativa
Node Name	Nombre del miembro y símbolo de salud
Node Type / Role	Local o remoto; primary o standby
Latest Heartbeat	Tiempo transcurrido desde la señal del compañero
waiting / syncing	Pendiente de comunicación / sincronizando
ready	Sincronización completada y preparado para servicio
hot-standby	Primario atiende; standby mantiene estado compartido
partner-down	Standby asume función activa por fallo del primario
unavailable	Nodo no responde y se considera fuera de servicio

En Kea se incluyen indicadores de corazón normal, interrumpido y desconectado, además de rol, estado y heartbeat. Un despliegue HA exige verificar reloj y conectividad entre nodos, así como la salud de ambos, antes de operar sobre la base de concesiones.

66.19. Procedimiento: localizar un host y verificar su identidad

1. Buscar por dirección, nombre o fragmento MAC, usando el campo más específico disponible.
2. Comprobar que el registro pertenece al segmento esperado y analizar Start/End.
3. Consultar ARP y, si hace falta, la tabla de switches, inventario o controlador de acceso para corroborar la MAC.
4. Revisar la configuración real del cliente y los registros DHCP.
5. Registrar resultado y fecha de la comprobación; evitar modificar la concesión solo por un hostname sospechoso.

66.20. Procedimiento: comprobar agotamiento de pool

1. Identificar pool, capacidad, utilización e intervalo real de crecimiento.
2. Activar visualización de expiradas para diferenciar registros históricos y concesiones vigentes.
3. Consultar duración de leases, estaciones temporales y equipos con MAC aleatoria.
4. Evaluar ampliar el rango dentro de la subred o rediseñar el direccionamiento, con revisión de exclusiones y rutas.
5. Tras cambios autorizados, observar clientes de prueba y comprobar que las nuevas ofertas DHCP no producen colisiones.

66.21. Procedimiento: alta de mapeo para impresora o equipo fijo

1. Identificar el dispositivo mediante inventario y confirmar su MAC real.
2. Desde la concesión dinámica, abrir Add static mapping.
3. Definir una IP documental fuera del rango dinámico cuando corresponda; verificar que está libre y es de la interfaz apropiada.
4. Guardar la configuración y renovar el cliente en una ventana de bajo impacto.
5. Validar dirección, gateway, DNS, conectividad y registro del activo.

66.22. Procedimiento: validar un equipo marcado Offline

1. No interpretar Offline como falla confirmada: revisar plazo del lease.
2. Consultar Diagnostics → ARP Table para confirmar presencia de la dirección MAC.
3. Emitir ping desde el segmento correcto si las reglas permiten realizar la prueba.
4. Verificar de forma independiente el acceso a la aplicación, impresora o servicio.
5. Documentar la causa: ARP expirado, equipo apagado, red aislada o firewall local.

66.23. Procedimiento: detectar servidor DHCP no autorizado

Los síntomas incluyen gateways/DNS inesperados, direcciones fuera del pool esperado y respuestas concurrentes a la misma solicitud. Status → DHCP Leases contiene únicamente los registros que conoce el servidor local, por lo que por sí sola no identifica necesariamente un DHCP ajeno.

1. Capturar tráfico en la VLAN problemática y filtrar UDP 67/68 para localizar respuestas DHCPOFFER.
2. Identificar MAC y dirección origen de cada servidor que responde.
3. Contrastar con la configuración aprobada de pfSense, relay y switches.
4. Aplicar medidas en capa 2 como DHCP snooping donde exista soporte, sin bloquear al servidor legítimo.
5. Verificar renovación de un cliente de prueba y revisar los logs del servicio.

66.24. Diagnóstico estructurado: de los síntomas a las pruebas

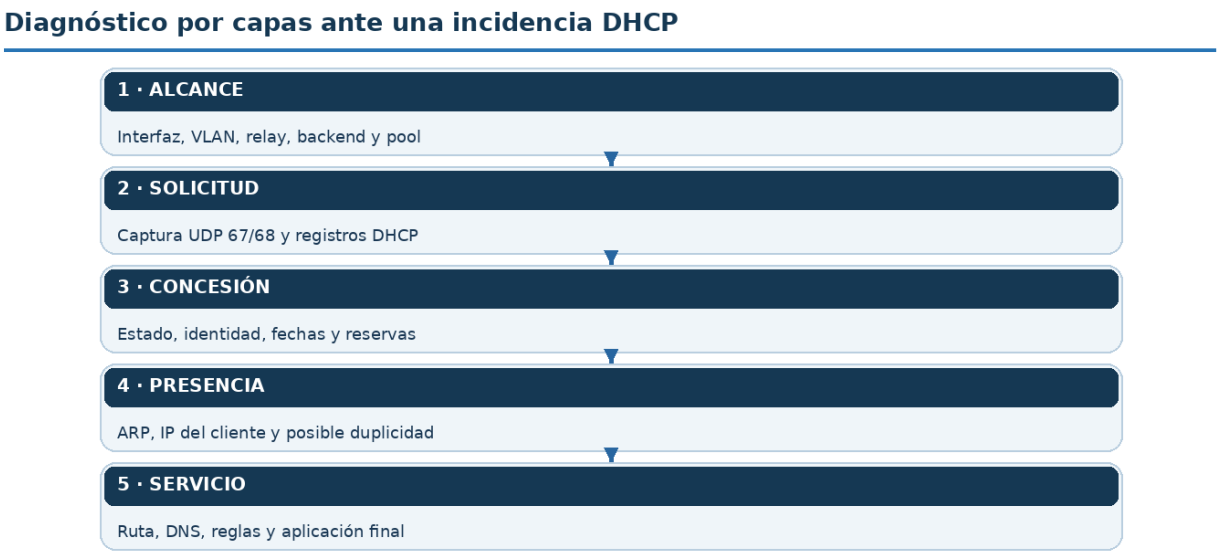


Figura 66.4. Secuencia de diagnóstico desde conectividad de capa 2 hasta DNS y aplicación.

Síntoma	Posibles causas	Prueba inicial
No recibe IPv4	VLAN, pool agotado, DHCP deshabilitado, relay	Captura DORA y registros DHCP
Tiene IP, pero sin red	Gateway, máscara, firewall, DNS	ipconfig/ip a y pruebas por capas
Offline en la GUI	Sin ARP reciente, segmentación, equipo inactivo	Diagnostics → ARP Table
Cambio imprevisto de IP	MAC aleatoria, caducidad, mapeo incorrecto	MAC del host y vigencia
IP duplicada	Estática manual o segundo DHCP	ARP, switch, inspección de red
HA inestable	Heartbeat, relojes, sincronización	Estado de ambos nodos, registros

66.25. Escenario empresarial A: oficina con dispositivos fijos

Una pequeña oficina utiliza una subred documental 198.51.100.0/24. Sus portátiles obtienen IP dinámicas y las impresoras tienen mapeos estables fuera del pool. El operador utiliza Search para localizar el dispositivo, verifica la MAC contra inventario, crea el mapeo y confirma DNS y accesibilidad. El procedimiento evita depender de un hostname autodeclarado.

66.26. Escenario empresarial B: red de invitados con alta rotación

Un segmento de invitados utiliza un pool amplio y leases breves según las necesidades de uso. La ocupación crece durante eventos y cae después. Se monitoriza Utilization y se revisa el comportamiento de dispositivos con MAC aleatorias. Antes de ampliar rango, se comprueban límites de VLAN, políticas de acceso, aislamiento de invitados y retención de registros.

66.27. Escenario empresarial C: clúster HA con reservas críticas

Dos nodos pfSense Plus coordinan DHCP con Kea. El administrador revisa roles y heartbeat en ambos equipos antes de realizar cualquier operación sobre las concesiones. Si un nodo entra en partner-down, primero confirma conectividad de sincronización y funcionamiento de atención a clientes; no borra la base completa para corregir un problema de HA.

66.28. Seguridad, privacidad y calidad del inventario

La tabla puede revelar MAC, nombres de dispositivos, franjas horarias y segmentación. Limitar permisos y exportaciones, usar comunicaciones cifradas para la administración, mantener trazabilidad de cambios y gestionar los registros conforme a la política corporativa. Una MAC puede ser suplantada o aleatorizada: no debe utilizarse por sí sola como mecanismo fuerte de autenticación. Combinar inventario, autenticación de red y segmentación cuando se requiera seguridad real.

RECOMENDACIÓN Mantener la consulta en modo observación por defecto; las operaciones masivas y los cambios de backend requieren planificación, respaldo y procedimiento de reversión.

66.29. Lista de comprobación operativa

Comprobación	Criterio de aceptación
Backend identificado	Kea/ISC confirmado en System → Advanced → Networking
Servicio activo	Solicitudes y respuestas correctas en un cliente de prueba
Pool suficiente	Ocupación y capacidad dentro de umbrales operativos definidos
Reservas comprobadas	Sin solapamientos ni direcciones duplicadas
ARP interpretada	No se confunde Online/Offline con estado de servicio
HA revisada si aplica	Sincronización y heartbeat correctos en ambos nodos
Evidencia preservada	Eventos, fecha y cambios documentados sin datos innecesarios

66.30. Glosario técnico

Término	Definición
Lease	Cesión temporal de parámetros DHCP a un cliente
DORA	Discover, Offer, Request, Acknowledge
ARP	Resolución entre IPv4 y MAC en un segmento
DHCP Relay	Reenvío de mensajes DHCP entre subredes
Pool	Rango configurado para asignación dinámica
Static mapping	Correspondencia administrativa predefinida por identificador
Kea / ISC	Implementaciones alternativas del servidor DHCP
Heartbeat HA	Señal de salud entre miembros de un clúster

66.31. Referencias técnicas oficiales

[1] Netgate · DHCPv4 Status

[2] Netgate · DHCPv4 Server

[3] Netgate · DHCP overview

[4] Netgate · DHCP Logs

[5] Netgate · Troubleshooting Offline DHCP Leases

[6] Netgate · Wake on LAN

[7] Netgate · Static Mappings Inside DHCP Pools

[8] Netgate · Kea Settings Tab

[9] Netgate · Troubleshooting HA DHCP Failover

[10] Netgate · Verifying Failover Functionality

[11] Netgate · Advanced Networking

[12] Netgate · DHCPv6 Status

67 Status → DHCPv6 Leases

Concesiones IPv6 · Identidad DUID/IAID · Delegación de prefijos · RA/SLAAC · Diagnóstico y alta disponibilidad

Status → DHCPv6 Leases permite inspeccionar las concesiones de direcciones IPv6 emitidas por el servidor DHCPv6, las delegaciones de prefijos registradas y el uso de sus pools. La pantalla ofrece búsqueda, filtrado, acciones sobre registros, visualización de entradas históricas y una operación global de limpieza cuyo impacto debe analizarse antes de utilizarla.

DHCPv6 no es el equivalente literal de DHCPv4: en IPv6 los anuncios de router (RA) informan sobre el encaminamiento y muchos dispositivos generan direcciones mediante SLAAC sin solicitar una concesión al servidor. Asimismo, la delegación de prefijos (IA_PD) es distinta de asignar una dirección individual (IA_NA).

PRINCIPIO DE LECTURA Una tabla vacía únicamente significa que no hay registros DHCPv6 visibles bajo los criterios actuales. No demuestra que no existan dispositivos IPv6 ni que el acceso a Internet esté caído.

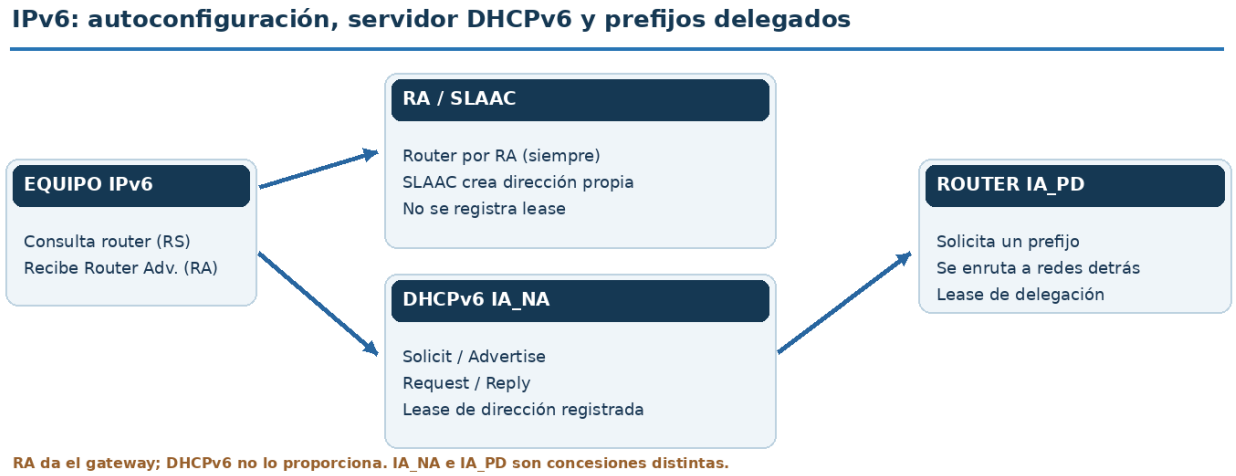


Figura 67.1. Relación entre RA, SLAAC, DHCPv6 y la delegación de prefijos.

67.1. Objetivo de la vista y ubicación en pfSense Plus

Ruta: Status → DHCPv6 Leases. Se trata de una página de observación con acciones administrativas puntuales; la configuración de los pools, los mapeos estáticos, la delegación y la selección del backend se realiza en otras pantallas. La información disponible varía con el backend Kea DHCP o ISC DHCP, la modalidad de direccionamiento y la versión instalada.

Ruta relacionada	Qué se verifica allí	Cuándo acudir
Services → DHCPv6 Server	Habilitación del servicio, rangos, reservas, PD y parámetros	Si no existen concesiones esperadas
Services → Router Advertisement	Modo RA y anuncios al enlace	Si el cliente no obtiene router o IPv6
System → Advanced → Networking	Backend DHCP seleccionado	Si los controles o el estado no coinciden con guías
Status → System Logs	Eventos de servidor DHCP y errores	Cuando el intercambio no concluye
Diagnostics → Packet Capture	DHCPv6, ICMPv6 RA/RS y NDP	Confirmar tráfico antes de cambiar opciones

Ruta relacionada	Qué se verifica allí	Cuándo acudir
Status → Interfaces	Prefijos e interfaces asignadas	Comprobar que la red tiene IPv6 correcto

67.2. Diferencias esenciales entre DHCPv4 y DHCPv6

Concepto	DHCPv4	DHCPv6
Identificador habitual	Dirección MAC / identificador de cliente	DUID + IAID
Puertos	UDP 67 (servidor), 68 (cliente)	UDP 547 (servidor), 546 (cliente)
Entrega de router	Opción de gateway DHCP	RA, no opción de gateway DHCPv6
Descubrimiento	Broadcast	Multicast y, según el escenario, unicast
Concesión	Dirección IPv4 individual	IA_NA y/o prefijos IA_PD
Autoconfiguración alternativa	APIPA no equivale a red normal	SLAAC puede operar sin lease DHCPv6
Presencia de equipo	ARP	Neighbor Discovery (NDP), no ARP

Es frecuente que una interfaz muestre direcciones link-local fe80::/10, direcciones temporales de privacidad o direcciones SLAAC y, sin embargo, la tabla DHCPv6 esté vacía. Para atribuir el origen de una dirección debe verificarse la configuración del sistema operativo y el modo RA.

67.3. Interpretación exacta del estado vacío de la pantalla

La página mostrada tiene tres bloques de resultados sin filas: «No address leases to display», «No prefix delegation leases to display» y «No leases are in use». Se observan el panel Search, los botones de visibilidad y limpieza de concesiones, y accesos en la barra superior. La ausencia de filas es el único estado que puede afirmarse con esta captura: no proporciona evidencia suficiente para diagnosticar por sí sola la causa.



Figura 67.2. Interpretación prudente de la pantalla sin concesiones.

Texto de la GUI	Lectura correcta	No implica
No address leases to display	No hay concesiones de dirección listadas	No hay hosts IPv6
No prefix delegation leases to display	No hay prefijos delegados listados	No existe un prefijo IPv6 en WAN
No leases are in use	No hay utilización mostrada para los pools	DHCPv6 está necesariamente apagado

67.4. Panel Search: campos, alcance y comportamiento

Control de la captura	Función	Consideración práctica
Search Term	Cadena de texto o expresión regular de tipo *nix	Una coincidencia puede depender del campo elegido
Lista desplegable: All	Busca en todos los campos de la concesión	Las opciones detalladas pueden variar por backend/versión
Search	Aplica el filtro introducido	No fuerza al cliente a renovar la lease
Clear	Limpia los criterios de búsqueda	No elimina la base de concesiones
Icono de contraer del bloque	Oculta o muestra el formulario de búsqueda	Solo cambia la presentación de la página

Usar una búsqueda simple por fragmento de DUID, dirección, nombre o descripción es preferible a una expresión compleja cuando se intenta localizar un equipo. Las expresiones regulares pueden ser útiles en inventarios grandes, pero deben validarse en un conjunto acotado para evitar exclusiones involuntarias.

67.5. Bloque Address Leases: campos de concesión de dirección

Columna	Interpretación y comprobación
IPv6 Address	Dirección IPv6 concedida mediante DHCPv6; verificar prefijo e interfaz antes de atribuir identidad.
DHCP Unique Identifier (DUID)	Identificador definido por el cliente; junto con IAID identifica asociaciones de identidad DHCPv6.
Hostname	Nombre declarado o conocido por el servidor; no constituye prueba criptográfica del equipo.
Description	Información administrativa asociada al registro/mapeo cuando está disponible.
Start	Inicio de validez de la concesión; revisar zona horaria del sistema.
End	Fin de la concesión registrada; renovar puede cambiar la fecha.
Actions	Botones contextuales al existir filas; disponibilidad según tipo/estado de concesión.

Si existen registros, Netgate documenta iconos de tipo de concesión (estática, activa o caducada), además de un indicador de presencia. Para IPv6, la constatación técnica de vecinos utiliza Neighbor Discovery; la documentación de la página conserva una descripción genérica de presencia basada en ARP. Esa etiqueta no debe confundirse con la prueba de disponibilidad de una aplicación.

67.6. DUID: concepto, formato y límites de identificación

El DUID (DHCP Unique Identifier) es un identificador persistente, generado por el cliente, con distintos formatos (por ejemplo DUID-LLT, DUID-EN, DUID-LL y DUID-UUID según RFC 8415). No existe una obligación de que todos los DUID tengan la misma longitud. El identificador puede mantenerse aun cuando cambie la MAC o actualizarse al reinstalar o clonar un equipo. Su valor puede contener información de hardware: se trata como dato operativo sensible.

Un ejemplo completamente sintético de DUID-LL es 00:03:00:01:02:00:00:00:00:01, utilizando una dirección MAC local ficticia. Nunca debe asumirse que dos clientes con el mismo hostname poseen el mismo DUID, ni que un DUID único impida la suplantación.

67.7. IAID, IA_NA, IA_PD y las asociaciones de identidad

IAID identifica una asociación de identidad dentro del equipo; DUID identifica al cliente. En conjunto, DUID + IAID permiten al servidor distinguir asociaciones, incluso si un cliente tiene más de una. IA_NA designa una asociación de direcciones no temporales; IA_PD representa prefijos delegados a un router descendente. Una concesión de IA_PD no equivale a una IP final que aparece en un host de una LAN.

Sigla	Significado	En la operación
DUID	DHCP Unique Identifier	Identidad de cliente
IAID	Identity Association Identifier	Distingue asociaciones de cliente
IA_NA	Identity Association for Non-temporary Addresses	Dirección IPv6 concedida
IA_PD	Identity Association for Prefix Delegation	Prefijo para redes detrás del solicitante
T1/T2	Tiempos de renovación / rebind	Temporizadores relativos al ciclo DHCPv6

67.8. Start y End: validez, renovación y caducidad

Start y End describen las ventanas de la concesión registrada, no la hora exacta de encendido o apagado de un dispositivo. Un cliente puede renovar antes del vencimiento; una entrada estática no depende de esa caducidad y puede mostrar n/a. La validez de direcciones SLAAC se maneja mediante lifetimes anunciados en RA, mecanismo diferente a estas fechas.

PRECISIÓN El tiempo de una concesión, el temporizador de RA y la duración de una entrada en Neighbor Cache no son el mismo indicador. Compararlos sin distinguir su función conduce a diagnósticos erróneos.

67.9. Indicadores de estado y acciones de las filas

Acción condicional (Netgate)	Qué realiza	Restricción importante
Añadir mapeo estático	Abre el formulario y precarga el DUID	Revisar IPv6 elegida y pool antes de guardar
Editar mapeo estático	Abre la entrada existente	No editar sin evaluar impacto sobre DNS
Crear entrada Wake-on-LAN	Prepara una entrada WOL cuando hay identificador utilizable	WOL utiliza MAC; DUID no es sustituto de MAC
Eliminar lease	Borra una entrada caducada o inactiva	No disponible para lease activa o estática

Esas acciones son documentadas por Netgate para vistas con registros; no aparecen como botones de fila en la pantalla vacía de ejemplo. De forma similar, las herramientas superiores de navegación o refresco se describen sin asignar funciones no verificadas a cada icono.

67.10. Bloque Prefix Delegation Leases: función real

Delegación de prefijos es el mecanismo por el que el servidor DHCPv6 asigna un bloque de direcciones a otro router, y pfSense lo encamina hacia él. Su uso es típico en sucursales, CPE, routers de laboratorios o subredes dependientes. Se administra y valida de forma distinta a una dirección IA_NA entregada a un equipo final.



Figura 67.3. Diferencia entre concesión IA_NA y delegación IA_PD, con direcciones de documentación.

67.11. Campos de las delegaciones de prefijos

Columna de la captura	Significado técnico
IPv6 Prefix	Bloque delegado con longitud, por ejemplo /60; comprobar que pertenece al pool autorizado.
DHCP Unique Identifier (DUID)	Identidad del solicitante; la documentación añade correlación con IAID.
Routed To	Siguiente salto IPv6 al que pfSense encamina el prefijo delegado.
Description	Descripción administrativa asociada, cuando procede.
Start / End	Vigencia de la delegación; actualizada en renovaciones.
Actions	Controles contextuales según la implementación y el estado.

Netgate documenta un campo de estado Active/Expired y correlación IAID/DUID cuando hay registros, pero dichos elementos no pueden verse en la tabla vacía de esta captura. El campo Routed To debe existir en la tabla de rutas y ser accesible por el enlace correcto para que las redes delegadas sean alcanzables.

67.12. Prefix Delegation: ejemplo de asignación a un router secundario

Un firewall de ejemplo administra 2001:db8:100::/48 y entrega 2001:db8:100:20::/60 a un router descendente. Ese router puede distribuir subredes /64 dentro del bloque delegado. Se comprueba la identidad DUID/IAID del solicitante, el prefijo asignado, la ruta de retorno hacia «Routed To», el filtrado IPv6 y el acceso desde una subred remota de prueba.

1. Confirmar que el pool de delegación está habilitado y contiene el prefijo correcto.
2. Solicitar el prefijo desde el router descendente y revisar su cliente DHCPv6-PD.
3. Verificar que aparece una nueva fila en Prefix Delegation Leases.
4. Comprobar que la ruta del prefijo apunta al «Routed To» correcto y no existe solapamiento.
5. Probar desde un host descendente tanto el siguiente salto como un destino autorizado, revisando reglas de firewall.

67.13. Bloque Address Lease Utilization y lectura de capacidad

Campo	Función visible
Interface	Interfaz que tiene configurado el pool DHCPv6.
Pool Start	Comienzo del rango de concesiones de dirección.
Pool End	Fin del rango de concesiones de dirección.
Used	Número de leases computadas para ese pool en el estado mostrado.
No leases are in use	No se muestran concesiones consumiendo los pools en este momento.

No se debe confundir el número de direcciones posibles dentro de un prefijo IPv6 con la dimensión de un pool configurado. Para capacidad y alarmas, comparar la ocupación con el rango efectivo definido y considerar también direcciones estáticas y reglas de asignación del backend.

67.14. Botón Show all Configured Leases

En su presentación normal, la página lista concesiones activas y estáticas. Show all Configured Leases muestra también registros expirados e inactivos, lo que permite investigar cambios de identidad, reciclaje de direcciones y anomalías de renovación. El control inverso, documentado por Netgate, restaura la presentación de entradas activas/estáticas. No renueva clientes y no cambia el servidor.

67.15. Botón Clear All DHCPv6 Leases: impacto y condiciones

Clear All DHCPv6 Leases detiene el daemon DHCPv6, elimina la base de concesiones dinámicas y lo inicia de nuevo. Los mapeos estáticos permanecen. En un entorno con clientes activos, pueden producirse reasignaciones, pérdida temporal de servicio, cambios en los registros de DNS, interrupciones para routers con IA_PD y efectos transitorios de alta disponibilidad.

ADVERTENCIA CRÍTICA No utilizar la limpieza masiva como primera respuesta a una tabla vacía. Confirmar impacto en clientes, delegaciones, DNS y HA; realizar copia de seguridad, establecer ventana de mantenimiento y comprobar renovación y rutas después del reinicio.

1. Identificar backend y modo de servicio, inventariar concesiones y prefijos activos y comprobar estado HA si aplica.
2. Conservar evidencias y realizar copia de la configuración conforme al procedimiento de la organización.
3. Acordar ventana y condiciones de reversión; no activar la limpieza por una sospecha no contrastada.
4. Ejecutar la operación solo cuando exista una causa técnica suficiente y autorización.
5. Confirmar que el servicio se reinicia, vuelven a producirse leases esperadas y se recuperan DNS, RA y rutas de prefijos delegados.

67.16. Barra superior, navegación y refresco de la vista

La pantalla incorpora accesos por iconos en la barra superior, junto con la miga de pan Status / DHCPv6 Leases y el control para contraer Search. Los iconos no llevan texto visible en la imagen y su semántica precisa depende de la interfaz instalada; por rigor, no se atribuye a cada uno una función no verificable únicamente por su aspecto. La búsqueda y las acciones sí están etiquetadas expresamente y quedan documentadas.

67.17. Router Advertisements: Managed, Assisted y Stateless DHCP

Modo RA	Direcciones de los hosts	Implicación para DHCPv6 Leases
Managed	DHCPv6, cuando el cliente lo admite	Se esperan IA_NA para clientes compatibles
Assisted	SLAAC y opcional DHCPv6	No todos los hosts aparecerán como leases
Stateless DHCP	SLAAC + parámetros DHCPv6	No se esperan leases IA_NA por SLAAC
Unmanaged	SLAAC sin servidor DHCPv6	La vista puede estar vacía aunque haya IPv6
Router Only	Anuncia solo router	No genera leases DHCPv6 por sí mismo

IPv6 obtiene el router por RA; no existe una opción DHCPv6 equivalente a Router/Gateway de DHCPv4. Algunos clientes, incluidos dispositivos móviles que utilizan únicamente SLAAC, pueden acceder correctamente a IPv6 sin figurar aquí. Verificar las capacidades del sistema operativo antes de cambiar el modo RA.

67.18. Kea DHCP e ISC DHCP: diferencias en presentación

Kea es el backend moderno de pfSense, mientras que ISC DHCP está deprecado. La vista y las opciones varían según backend y revisión. Netgate documenta alta disponibilidad de Kea para DHCPv4 y DHCPv6 y delegación de prefijos. Comprobar los requisitos y la disponibilidad de estas funciones en la versión instalada.

Aspecto	Kea	ISC DHCP
Evolución	Backend mantenido y en desarrollo	Backend heredado y deprecado
HA DHCPv6	Hot-standby con estado en la página cuando se configura	No asumir el mismo panel/función
PD	Soporte sujeto a versión, documentado en versiones actuales	Variaciones según versión
Acciones GUI	Pueden variar por versión instalada	Pueden variar por backend

67.19. Alta disponibilidad DHCPv6 con Kea

En configuraciones HA, Kea coordina nodos primario y standby, intercambia registros y monitoriza heartbeats. La sección High Availability puede aparecer al final de DHCPv6 Leases. Se debe revisar la salud desde ambos miembros, confirmar sincronía horaria y comprobar comunicación de HA. Una tabla vacía en un nodo aislado no basta para determinar una incidencia de failover.

En ejemplos oficiales de Netgate, el modo de alta disponibilidad es «hot-standby»; ante fallo del primario, el standby puede asumir atención a clientes según la política configurada. Los cambios en RA, CARP o rutas deben probarse por separado y el hecho de que pfsync sincronice estados de firewall no equivale a sincronizar concesiones DHCPv6.

67.20. Procedimiento: verificar por qué no hay concesiones

1. En Services → DHCPv6 Server, verificar backend, habilitación, interfaz y pool de direcciones.
2. Comprobar Status → Interfaces y que el segmento tiene un prefijo IPv6 correcto.
3. En Services → Router Advertisement, confirmar modo RA acorde a los clientes (Managed/Assisted para IA_NA).
4. Desde un cliente compatible, examinar dirección y estado de DHCPv6; comprobar si la dirección se creó mediante SLAAC.
5. Capturar UDP 546/547 y RA ICMPv6 en la interfaz correcta; correlacionar con logs de DHCP.
6. Si se esperan delegaciones, inspeccionar por separado IA_PD, Routed To y la tabla de rutas.

67.21. Procedimiento: localizar una concesión por DUID

1. Obtener el DUID del propio cliente por un método autorizado y comparar su IAID si aparece.
2. Buscar por fragmento de DUID o por dirección IPv6 utilizando Search Term.
3. Comprobar fecha, estado y prefijo de la fila; no basarse solo en hostname.
4. Si es necesario, activar Show all Configured Leases para localizar concesiones históricas.
5. Corroborar con registros DHCPv6, inventario y tabla de vecinos NDP antes de realizar acciones.

67.22. Procedimiento: crear mapeo estático de DHCPv6

1. Comprobar que el sistema está obteniendo IA_NA y que el DUID/IAID son correctos.
2. Si existe concesión, usar el control de añadir mapeo estático para precargar el DUID.
3. Introducir una dirección documental del prefijo permitido, evitando colisiones y solapamiento de pools.
4. Guardar y planificar la renovación del cliente; en DHCPv6 una dirección fijada no equivale a una reserva exclusiva global.
5. Comprobar en el cliente la nueva dirección y validar DNS, rutas y reglas IPv6.

SEGURIDAD Un mapeo estático no sustituye control de identidad: un cliente que suplante el DUID puede provocar comportamientos no deseados. Usar controles de acceso independientes para equipos críticos.

67.23. Procedimiento: comprobar delegación de prefijo a otra sede

1. Identificar el pool IA_PD configurado y la longitud de delegación prevista.
2. En el router remoto, comprobar que se solicita PD por DHCPv6 y se anuncia cada subred interior.
3. En la tabla Prefix Delegation Leases, verificar el prefijo, DUID/IAID, Routed To y vigencia.
4. Validar que pfSense conoce la ruta del prefijo delegado y que el firewall permite los flujos autorizados.
5. Desde un host detrás del router, probar alcance, DNS y tráfico entre segmentos, registrando resultados.

67.24. Procedimiento: investigación de lentitud o pérdida intermitente

Cuando un usuario informa de IPv6 irregular, las concesiones pueden seguir vigentes aunque haya problemas de MTU, RA, DNS, estados del firewall o conectividad del upstream. La pantalla de leases aporta identidad y vigencia, pero no mide calidad del enlace.

1. Revisar hora de incidencia, concesión, renovaciones y cambios de interfaz.
2. Comprobar RA y la ruta predeterminada de la estación.
3. Hacer ping6 y traceroute6 autorizados, diferenciando fallos de DNS de fallos de encaminamiento.
4. Revisar Neighbor Discovery, logs de firewall y contadores de interfaces.
5. Correlacionar los resultados con las redes delegadas y el estado de gateways si los hay.

67.25. Capturas de paquetes y comandos de comprobación

Prueba	Qué permite confirmar	Límite
Captura UDP 546/547	Intercambio cliente-servidor DHCPv6	No diagnostica RA por sí sola
Captura ICMPv6 RA/RS	Anuncios de router, flags M/O y prefijos	No muestra lease del servidor
ipconfig /all (Windows)	DUID y direcciones conocidas por el cliente	No garantiza rutas ni firewall
ip -6 addr; ip -6 route (Linux)	Direcciones, prefijos y ruta por defecto	Depende de RA y gestor de red
ping -6 / traceroute -6	Conectividad hacia un destino de prueba	ICMP puede estar filtrado
pfSense: logs DHCP	Asignación, renovación y fallos del daemon	Vista varía según backend

67.26. Matriz de diagnóstico y resolución de incidencias



Figura 67.4. Secuencia de comprobación de DHCPv6, RA, identidad y conectividad.

Síntoma	Causas plausibles	Primera comprobación
Tabla vacía con hosts IPv6	SLAAC / modo RA / filtro	Origen de dirección y filtros
Cliente sin router IPv6	RA deshabilitado, bloqueado o mal configurado	Captura ICMPv6 RA
Cliente solicita, sin Reply	Pool, servicio, VLAN, reglas locales	UDP 546/547 + logs
DUID duplicado	Clonación o reinicio de identidad	DUID/IAID de ambos clientes
Prefijo delegado sin salida	Ruta, firewall, RA downstream	Routed To + rutas + pruebas
PD cambia tras reinicio	Concesión dinámica o upstream	Registrar prefijos/renovación
HA sin sincronización	Reloj, conectividad, Kea peer	Estado y heartbeat en ambos nodos
DNS falla, IPv6 funciona	DNS no distribuido o no accesible	Resolución AAAA y RA/DHCPv6

67.27. Escenario empresarial A: estaciones y móviles

Una red documental 2001:db8:100:10::/64 utiliza RA Assisted. Los equipos de escritorio compatibles obtienen direcciones DHCPv6 y se muestran en Address Leases; varios móviles usan SLAAC y no generan concesión de dirección. El administrador distingue correctamente ambos grupos y usa Neighbor Discovery y registros de acceso si necesita evidencias de presencia.

67.28. Escenario empresarial B: delegación a router de laboratorio

Un firewall asigna un bloque /60 de documentación a un router de pruebas. El equipo descendente crea varias subredes /64 y las anuncia mediante RA. Status → DHCPv6 Leases permite inspeccionar la vigencia del prefijo y su siguiente salto, mientras que la alcanzabilidad requiere comprobar rutas y reglas, no únicamente la existencia del registro IA_PD.

67.29. Escenario empresarial C: clúster y cambios planificados

Dos equipos pfSense con Kea DHCPv6 comparten el estado de leasing para mantener disponibilidad. Antes de conmutar o limpiar registros, se revisan los heartbeats, el reloj, las concesiones y las rutas a redes delegadas. Se prueba un cliente de referencia durante la conmutación y se deja evidencia de la IP y prefijo obtenidos con identificadores ficticios en el informe general.

67.30. Buenas prácticas de seguridad y tratamiento de datos

Las direcciones IPv6, identificadores DUID, hostnames, prefijos delegados, marcas temporales y patrones de presencia pueden revelar la topología y el inventario de la organización. Restringir el acceso administrativo, registrar acciones destructivas, evitar publicar capturas operativas, limitar el tratamiento de identificadores y revisar permisos por rol. El filtrado de tráfico en IPv6 depende de reglas y segmentación; disponer de dirección IPv6 global no implica automáticamente que el servicio sea accesible desde Internet.

No modificar a ciegas RA, longitud de prefijos, backend o limpieza de leases. Un cambio de prefijo delegado puede afectar numerosas subredes aguas abajo; utilizar mantenimiento, copia de seguridad y pruebas de retorno.

67.31. Lista de control para revisión operativa

Control	Resultado aceptable
Backend conocido	Kea o ISC identificado con versión del producto
RA revisado	Modo coherente con clientes y SLAAC/DHCPv6
DUID/IAID validados	Sin inconsistencias de identidad relevantes
IA_NA e IA_PD separados	Se distinguen direcciones individuales y prefijos
Rutas y DNS verificados	Conectividad comprobada desde cliente final
Acciones destructivas controladas	Borrado masivo solo mediante autorización
HA revisada cuando aplica	Nodos y heartbeat correctos
Información protegida	Sin exposición de datos operativos en informes

67.32. Glosario

Término	Definición
DHCPv6	Protocolo de configuración dinámica para IPv6.
DUID	Identificador del cliente DHCPv6.
IAID	Identificador de asociación dentro de un mismo cliente.
IA_NA	Asociación de direcciones IPv6 no temporales.
IA_PD	Asociación de prefijos IPv6 delegados.
SLAAC	Autoconfiguración de direcciones sin estado.
RA / RS	Router Advertisement / Router Solicitation.
NDP	Neighbor Discovery Protocol; descubrimiento de vecinos y routers.
Kea	Backend de servidor DHCP moderno.
PD	Prefix Delegation para routers descendentes.
Renew / Rebind	Operaciones de renovación DHCPv6 del cliente.

67.33. Referencias técnicas oficiales

[1] Netgate · DHCPv6 Status	**[2] Netgate · DHCPv6 Server**
[3] Netgate · IPv6 Router Advertisements	[4] Netgate · DHCP Overview
[5] Netgate · Kea Settings Tab	[6] Netgate · Advanced Networking
[7] Netgate · High Availability Test	[8] Netgate · Troubleshooting HA DHCP Failover
[9] Netgate · High Availability Cluster Example	[10] Netgate · pfSense Plus 26.03 release notes
[11] Netgate · DHCPv4 Status (contrast)	[12] IETF · RFC 8415 DHCP for IPv6
[13] IETF · RFC 4861 Neighbor Discovery	[14] IETF · RFC 4862 SLAAC

68 Status → DNS Resolver

Caché de infraestructura de Unbound · Latencia y timeouts · EDNS · Servidores lame · Diagnóstico operativo

La vista Status → DNS Resolver de pfSense Plus permite inspeccionar la memoria operativa que Unbound mantiene sobre servidores DNS consultados. Su propósito no es listar las respuestas DNS de los usuarios, sino mostrar información de servidores: tiempos de respuesta, temporizadores de reintento, compatibilidad EDNS y señales de falta de autoridad.

La vista presenta DNS Resolver Infrastructure Cache Speed y DNS Resolver Infrastructure Cache Stats. Una tabla vacía no equivale por sí sola a una avería de resolución. Combinar esta información con consultas reproducibles, registros y comprobaciones de conectividad.

CLAVE OPERATIVA «No Data» describe el contenido visible de la caché de infraestructura en ese instante. No demuestra, por sí solo, que Unbound esté detenido o que la resolución DNS falle.

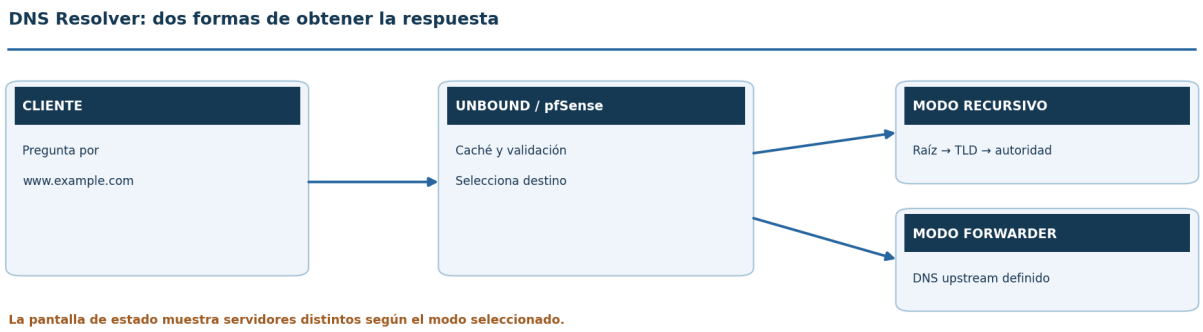


Figura 68.1. Diferencia entre resolución recursiva y reenvío a servidores upstream.

68.1. Objetivo y ruta exacta de la pantalla

Ruta de navegación: Status → DNS Resolver. Se trata de una vista de estado, no de la pantalla donde se habilita, se deshabilita o se parametriza el servicio. La configuración del demonio reside en Services → DNS Resolver y la supervisión del proceso en Status → Services. Los registros se consultan en Status → System Logs, sección DNS Resolver.

Pantalla relacionada	Función principal	Cuándo consultarla
Services → DNS Resolver	Modo recursivo o forwarding, escucha, ACL, DNSSEC y parámetros avanzados	Revisar configuración efectiva
Status → DNS Resolver	Caché de infraestructura de servidores que conoce Unbound	Analizar selección y fallos upstream
Status → Services	Verificar unbound Running/Stopped; reinicio controlado	Comprobar disponibilidad del proceso
Diagnostics → DNS Lookup	Emitir consultas y observar respuestas/tiempos	Validar funcionalidad DNS
Status → System Logs → DNS Resolver	Mensajes de Unbound y otros procesos DNS	Investigar errores y validación

68.2. Qué es Unbound y por qué mantiene una caché de infraestructura

Unbound es el resolutor DNS recursivo, caché y validador DNSSEC utilizado por pfSense. Recibe preguntas de clientes autorizados y, según su modo, contacta directamente con jerarquías DNS públicas o transfiere consultas a servidores configurados. Para elegir a cuál consultar conserva datos de experiencia reciente acerca de cada servidor y zona.

Esta información reside en una caché especial —infrastructure cache o infra-cache—, independiente de los registros de respuesta. En ella Unbound puede conservar latencia, dispersión de tiempos, eventos de

timeout, EDNS soportado y señales de servidores sin autoridad adecuada. Los valores se actualizan con el tráfico real y caducan según un TTL propio.



Figura 68.2. El estado de infraestructura no equivale a la caché de RRsets o mensajes DNS.

68.3. Cómo cambia la vista según el modo de operación

Modo	Servidores esperables	Consecuencia de lectura
Resolver / recursivo	Servidores raíz, TLD y autoritativos de zonas solicitadas	Puede haber muchas IP y zonas diferentes
Forwarding	Servidores reenviadores de System → General Setup, fuentes WAN y overrides	Comparar su capacidad de respuesta y ruta WAN
Sin actividad o tras reinicio	Ninguno o muy pocos hasta que se realicen consultas upstream	«No Data» puede ser completamente normal

En modo resolver, consultar repetidamente un nombre ya cacheado no obliga necesariamente a contactar nuevos servidores autoritativos. En forwarding, una respuesta también puede satisfacerse desde caché. Por ello la población de las tablas depende de la demanda, antigüedad de registros, modo y estado del demonio.

68.4. Lectura fiel de la pantalla sin entradas

La página incluye encabezado Status / DNS Resolver, una barra de accesos rápidos y dos paneles con el resultado «No Data». No presenta campo de búsqueda, controles de alta ni un botón de modificación de filas. Los encabezados sí indican qué columnas aparecen cuando Unbound tiene datos.

INTERPRETACIÓN El dato negativo es exclusivamente «no hay filas en estas tablas». Antes de concluir que hay un problema se debe comprobar si las consultas DNS funcionaron, si hay tráfico hacia servidores upstream y si la página está mostrando datos recientes.

68.5. Iconos de la barra superior: finalidad y precauciones

Icono visible	Acción documentada	Observaciones
Flecha circular	Reiniciar el servicio asociado	Puede vaciar cachés o provocar un corte breve de resolución
Círculo con cuadrado	Detener el servicio activo	Puede interrumpir DNS a los clientes que dependen del firewall
Controles deslizantes	Abrir la configuración del DNS Resolver	No aplica automáticamente cambios
Símbolo gráfico	Acceso relacionado con estado/monitorización	El destino depende de los accesos disponibles en esa versión
Listado rectangular	Abrir registros relacionados	Ayuda a correlacionar eventos con las tablas
Interrogación	Ayuda contextual de la página	No altera el servicio

Los accesos rápidos que Netgate documenta incluyen Restart Service, Stop Service, Related Settings, Status Page Link, Log Page Link y Help Link. La presencia y el destino concreto pueden cambiar según los servicios activos y la versión. No confundir reiniciar el demonio con refrescar el navegador: son operaciones distintas.

ADVERTENCIA No utilizar Restart ni Stop para «hacer aparecer» filas sin comprobar primero el funcionamiento DNS. Reiniciar Unbound puede borrar sus cachés y crear una avalancha temporal de consultas externas.

68.6. Primera tabla: DNS Resolver Infrastructure Cache Speed

Este panel reúne métricas de rapidez y fiabilidad estimadas por Unbound para servidores y zonas. No es un monitor ICMP, ni presenta porcentajes de pérdida equivalentes a los de un gateway; constituye el estado de los temporizadores y observaciones internas del algoritmo de selección de servidores.

Campo exacto	Significado operativo	Qué no debe suponerse
Server	IP del servidor DNS evaluado en la infra-cache.	No identifica necesariamente al DNS configurado por un cliente final.
Zone	Zona DNS para la que se usó o evaluó el servidor.	No siempre representa el FQDN completo solicitado.
TTL	Vida restante del elemento de infraestructura.	No es el TTL del registro A o AAAA solicitado.
Ping	Estimación suavizada del tiempo de respuesta DNS, en ms.	No implica que se haya ejecutado ping ICMP.
Var	Variación estimada de los tiempos de respuesta, en ms.	No es la desviación RTTsd de un gateway.
RTT	Temporizador de espera de ida y vuelta sin el retroceso exponencial, en ms.	No es necesariamente la latencia bruta de una muestra.
RTO	Timeout efectivo con backoff cuando se producen fallos, en ms.	No equivale a la latencia de una respuesta exitosa.
Timeout A	Contador interno de timeouts en consultas tipo A.	No es un fallo general de toda la conexión IPv4.
Timeout AAAA	Contador interno de timeouts en consultas tipo AAAA.	No implica ausencia de conectividad IPv6 por sí solo.
Timeout Other	Contador de timeouts para otros tipos de consulta.	No es una lista de errores de DNSSEC.

68.7. Server y Zone: relación entre dirección y autoridad

La columna Server identifica el destino de la consulta, mientras Zone refleja la autoridad DNS asociada. El mismo servidor puede estar asociado a varias zonas y una zona disponer de múltiples servidores, por lo que no basta con comparar una sola fila. En resolución recursiva se pueden observar raíces, dominios de primer nivel y autoridades específicas; en forwarding predominan los reenviadores que constituyen el destino upstream.

Un servidor responde autoritativamente cuando corresponde a la zona solicitada y proporciona el tipo de respuesta previsto. Si un servidor declara no ser autoridad o responde de manera incompatible, la infra-cache puede conservar esa señal para que el algoritmo evite rutas de consulta deficientes.

68.8. TTL: temporizador de la caché de infraestructura

En la configuración avanzada de pfSense, TTL for Host Cache Entries controla cuánto persisten estas observaciones; la documentación de Netgate establece 15 minutos como valor predeterminado. Este TTL no es el TTL de un RRset de dominio. Al caducar, Unbound puede reevaluar al servidor si nuevas consultas lo requieren.

Modificar este parámetro tiene compromisos: valores muy cortos pierden aprendizaje y elevan sondeos; valores largos prolongan estados observados durante fallos transitorios. No alterar el valor predeterminado como respuesta automática a una tabla vacía o a una única medida elevada.

68.9. Ping, Var, RTT y RTO: distinguir medición y control de reintentos

Ping representa el tiempo suavizado de respuesta DNS observado en el algoritmo de Unbound. Var es la variabilidad también suavizada. RTT representa el timeout calculado antes de aplicar retroceso

exponencial; RTO incorpora ese backoff cuando un servidor no contesta. La combinación orienta la selección de servidores y evita perseguir una dirección de la que se conocen reiterados fallos.

Ejemplo estrictamente didáctico: una autoridad que responde de forma estable podría mantener un tiempo de espera reducido; ante varias consultas perdidas, el valor RTO crecerá y otras autoridades válidas serán candidatas preferibles. En ciertas versiones/configuraciones un RTO de 120 000 ms identifica un destino considerado temporalmente no útil, pero debe corroborarse con consultas, registros y conectividad.

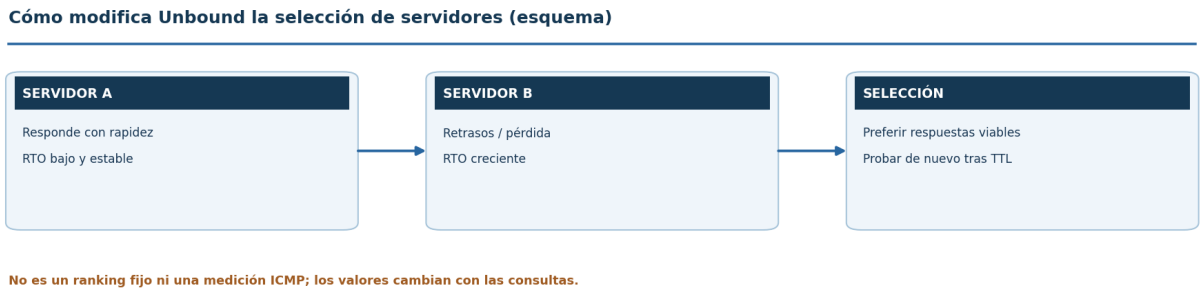


Figura 68.3. La elección de servidores depende de tiempos observados, backoff y disponibilidad.

68.10. Timeout A, Timeout AAAA y Timeout Other

Estas tres columnas separan los contadores de expiración por familia de tipo de pregunta. A solicita direcciones IPv4; AAAA solicita IPv6. Other comprende tipos distintos, entre ellos consultas que participan en delegación o validación. Un timeout de tipo AAAA no significa necesariamente que la WAN IPv6 haya caído: puede deberse al servidor consultado, ruta, filtrado, UDP fragmentado o problema específico de ese tipo de intercambio.

La observación debe realizarse a lo largo del tiempo. Un valor puntual no es una tasa por segundo ni una prueba de pérdida total. Es útil correlacionar con la zona, la IP del servidor, RTO y el resultado de una consulta específica de ese tipo.

68.11. Segunda tabla: DNS Resolver Infrastructure Cache Stats

Esta sección recoge capacidades EDNS y las señales de lameness —falta de autoridad, incapacidad de responder como se espera o comportamiento DNSSEC incompatible—. La cabecera de la captura contiene Server, Zone, eDNS Lame Known, eDNS Version, Probe Delay, Lame DNSSEC, Lame Rec, Lame A y Lame Other.

Campo exacto	Interpretación técnica	Criterio de prudencia
Server	Servidor al que corresponden los indicadores.	Comparar con el campo Zone.
Zone	Zona para la que se registraron los indicadores.	Evitar conclusiones globales sobre el dominio.
eDNS Lame Known	Se conoce si el destino presenta comportamiento EDNS problemático.	No es por sí solo una prueba de fallo en todos los tipos DNS.
eDNS Version	Versión EDNS que el servidor ha demostrado soportar (o desconocida/no compatible).	No es la versión del software Unbound.
Probe Delay	Plazo o espera antes de nuevas sondas sobre un destino problemático.	No equivale al TTL de una respuesta DNS.
Lame DNSSEC	Señal de comportamiento de servidor «lame» en consultas relativas a DNSSEC.	Corroborar el fallo DNSSEC de la zona y cadena de confianza.
Lame Rec	Señal relacionada con comportamiento recursivo donde se esperaba autoridad.	No confundir con modo forwarding de pfSense.

Campo exacto	Interpretación técnica	Criterio de prudencia
Lame A	Señal de falta de autoridad/validez para consultas de tipo A.	Puede ser limitada a la zona y tipo.
Lame Other	Señal de falta de autoridad en otros tipos de consulta.	Correlacionar con log y consulta concreta.

68.12. EDNS: Extended DNS y su papel en DNSSEC

EDNS (Extension Mechanisms for DNS) amplía funciones del protocolo DNS, entre ellas la negociación del tamaño de mensajes UDP y elementos necesarios para transportar respuestas DNSSEC. La detección de soporte EDNS permite a Unbound ajustar su comunicación con distintas autoridades. Un elemento marcado como «eDNS Lame Known» indica que se dispone de conocimiento sobre un comportamiento de EDNS defectuoso o no fiable; no autoriza a deshabilitar DNSSEC en todo el firewall.

En pfSense, EDNS Buffer Size es un parámetro de Services → DNS Resolver → Advanced Settings. Netgate documenta un modo automático según MTU y otros valores seleccionables. Si hay fallos por fragmentación, deben verificarse capturas y transporte antes de cambiar buffers: una cifra aparentemente menor puede aumentar la necesidad de TCP como mecanismo de reserva.

68.13. Lame DNSSEC, Lame Rec, Lame A y Lame Other

En terminología DNS, un servidor lame no proporciona la autoridad o el comportamiento esperado para la zona/tipo consultado. Una delegación rota, un servidor mal declarado, una autoridad que responde como recursor o respuestas DNSSEC deficientes pueden originar señales relacionadas. Es una propiedad observada en un contexto determinado y no una condena definitiva de toda la dirección IP.

Cuando una misma zona muestra numerosas señales lame, revisar primero la coherencia entre NS, glue, DNSSEC, registros y rutas. En redes empresariales con DNS interno, verificar además que la configuración de Domain Overrides dirija las zonas privadas al servidor adecuado. Un override mal dirigido puede crear un problema de resolución muy distinto a una autoridad pública defectuosa.

68.14. Probe Delay y recuperación tras un servidor no disponible

Unbound limita los intentos hacia servidores que presentan fallos persistentes, para no agotar puertos, sockets y tiempo de procesamiento. La infra-cache conserva esperas y ventanas de prueba: al expirar esa condición, nuevas consultas pueden desencadenar un nuevo sondeo. La caducidad del estado no garantiza que el servidor se haya recuperado, únicamente que podrá reevaluarse.

La documentación de NLnet Labs describe regímenes de operación normal, sondeo y bloqueo temporal, incluido el incremento exponencial de los timeouts. No usar Probe Delay como un temporizador de failover WAN ni interpretar un RTO alto como prueba de que el router upstream haya perdido enlace físico.

68.15. Por qué puede aparecer «No Data»: causas posibles

Hipótesis	Verificación sin modificar el sistema	Resultado esperado
Unbound no está iniciado	Status → Services	Servicio detenido o ausente
No se han realizado consultas upstream recientes	Diagnostics → DNS Lookup + repetir vista	La consulta funciona; quizá se puebla infra-cache
Las consultas proceden de caché o hosts locales	Probar un nombre que exija salida, de forma controlada	Puede existir respuesta sin nueva consulta autoritativa
Servicio reiniciado o caché vaciada	Últimos eventos en System Logs	Estado vacío tras recreación del proceso
Otro servicio DNS atiende el puerto	Services → DNS Resolver / DNS Forwarder	Unbound puede estar deshabilitado
Problema de salida, ACL o ruta	Diagnóstico de WAN y captura de puerto 53 / 853 según modo	Se observan consultas fallidas o sin retorno
Visualización momentánea o versión concreta	Recargar vista; examinar versión y logs	No confundir UI con fallo del proceso

68.16. Procedimiento 1: comprobar el servicio y la resolución sin riesgo

01 Abrir Status → Services y comprobar el estado del proceso unbound; anotar cualquier aviso.

02 Confirmar en Services → DNS Resolver si está habilitado y si utiliza resolver mode o forwarding mode.

03 Ejecutar Diagnostics → DNS Lookup sobre example.com y registrar respuesta, tipo de registro y tiempos.

04 Volver a Status → DNS Resolver y comparar ambas tablas antes y después de la consulta.

05 Revisar Status → System Logs → DNS Resolver si el resultado no es correcto o la vista permanece vacía.

06 Si la resolución funciona, evitar reinicios únicamente para conseguir filas en las tablas.

LECTURA REPRODUCIBLE Diagnostics → DNS Lookup puede consultar el resolver local y otros DNS configurados en System → General Setup. Anotar qué servidor respondió; no extrapolar el resultado de un DNS externo al funcionamiento interno de Unbound.

68.17. Procedimiento 2: inspección mediante comandos de Unbound

Cuando la GUI no muestra suficiente información, el comando oficial unbound-control permite observar la infra-cache. Ejecutar únicamente con permisos administrativos autorizados, preferentemente en ventana de diagnóstico y sin modificar parámetros.

```
unbound-control -c /var/unbound/unbound.conf lookup example.com
unbound-control -c /var/unbound/unbound.conf dump_infra
unbound-control -c /var/unbound/unbound.conf dump_cache
```

lookup muestra los servidores asociados a la resolución de una zona; dump_infra lista la caché de infraestructura, que es el dato relacionado con esta pantalla. dump_cache, en cambio, trata de los registros y mensajes cacheados. No pegar salidas reales en informes distribuidos sin revisar previamente direcciones internas, dominios y topología.

68.18. Diferencia entre vaciar una respuesta DNS y vaciar la infraestructura

Acción	Afecta a	Riesgo / consecuencia
flush example.com	Registros cacheados del nombre consultado	Volverá a consultarse; no corrige rutas ni autoridad
flush_infra all	Infraestructura de latencias, EDNS y lameness	Pierde aprendizaje de servidores; uso solo justificado
reload	Recarga Unbound y limpia cachés según documentación	Cambia estado operativo y carga de consultas
Restart en Status → Services	Proceso unbound y cachés del demonio	Interrupción temporal para clientes
Actualizar página del navegador	Sólo interfaz de consulta de estado	No debería alterar cachés DNS

Netgate documenta flush <nombre>, reload y reinicio como operaciones distintas. NLnet Labs documenta flush_infra all para el estado de infraestructura. No programar vaciados periódicos como sustituto de investigar fallos; ocultarían señales de latencia y harían la resolución menos eficiente.

68.19. Procedimiento 3: investigar un RTO elevado o repetidos timeouts

01 Identificar Server y Zone concretos, sin interpretar el conjunto de la tabla como un único servidor DNS.

02 Anotar Ping, Var, RTT, RTO y contadores de timeout; repetir la observación tras nuevas consultas controladas.

03 Confirmar gateway, interfaz de salida y ruta efectiva para ese destino, especialmente en Multi-WAN.

04 Usar Diagnostics → DNS Lookup y, si es posible, captura de paquetes DNS en la WAN adecuada.

05 Buscar errores en los registros y comparar autoridades alternativas o forwarders configurados.

06 Corregir primero la causa demostrada; verificar después recuperación y tiempos, evitando cambios simultáneos.

68.20. Multi-WAN y elección de servidores DNS

En modo resolver, los servidores autoritativos no se conocen de antemano y el camino habitual depende de la ruta por defecto del firewall. En forwarding, los servidores upstream pueden asociarse a gateways distintos, lo que facilita rutas de consulta adecuadas en entornos Multi-WAN. Un forwarder conectado por una WAN caída puede acumular timeouts y resultar menos preferido, pero esta vista no sustituye Status → Gateways ni pruebas de ruta.

La secuencia de comprobación consiste en revisar el estado de los gateways, DNS Servers de System → General Setup, reglas de salida y NAT cuando apliquen, y las capturas de red. La selección adaptativa de Unbound tampoco equivale a un balanceador empresarial con SLA garantizado; es un mecanismo interno de resolución.

68.21. DNSSEC, reloj del sistema y fallos de validación

DNSSEC protege la autenticidad e integridad de respuestas mediante firmas y cadena de confianza. Los errores DNSSEC pueden producir SERVFAIL aunque la conectividad IP sea correcta. Antes de deshabilitar la validación por diagnóstico, revisar la hora del firewall, la sincronización NTP, la respuesta de las autoridades y los registros. Si se prueba una modificación temporal en un entorno controlado, documentar y revertir el cambio inmediatamente.

No equiparar Lame DNSSEC a un certificado TLS caducado; pertenecen a tecnologías distintas. DNSSEC valida datos DNS, mientras que DNS over TLS protege un canal cifrado de transporte a un forwarder compatible, normalmente en TCP/853. Unbound puede utilizar DNSSEC incluso sin DoT.

68.22. Firewall, NAT, ACL y puertos relevantes

Flujo	Puerto habitual	Observaciones
Clientes → DNS Resolver	UDP/53 y TCP/53	La interfaz de escucha y las ACL determinan si se atiende al cliente.
Resolver → autoridades / forwarders	UDP/53 y TCP/53	Se requiere ruta válida y permiso de salida/retorno.
Forwarding con DNS over TLS	TCP/853	El upstream debe ofrecer DoT y negociar TLS correctamente.
DNSSEC con respuestas grandes	DNS UDP/TCP según negociación	Fragmentación, EDNS y fallback TCP pueden ser relevantes.
Consultas de prueba	Según destino configurado	DNS Lookup no siempre comprueba el mismo endpoint que usa una aplicación.

68.23. Escenario empresarial A: respuesta DNS lenta para un dominio

Una delegación externa presenta respuestas intermitentes. En Status → DNS Resolver aparecen valores RTO elevados para una autoridad concreta y aumento de Timeout A o Timeout Other. Se confirma el mismo patrón mediante consultas directas y captura de paquetes; otros dominios responden con normalidad. La actuación correcta es revisar autoridad, DNSSEC y camino hacia ese destino, no reiniciar pfSense ni sustituir todos los DNS de los clientes.

68.24. Escenario empresarial B: red con dos salidas a Internet

Un firewall utiliza dos WAN con servidores forwarder asociados a rutas diferentes. Tras un fallo parcial, la tabla de infraestructura puede acumular tiempos de espera para el reenviador no alcanzable. El administrador contrasta Status → Gateways, encaminamiento, respuesta de los DNS upstream y consultas hechas contra el propio firewall. La decisión de migrar el forwarder o ajustar gateway requiere evaluación de impacto y no se deduce solo de una fila RTT.

68.25. Escenario empresarial C: DNS interno de una zona privada

Una organización delega la resolución de una zona privada ficticia como corp.example.com en un DNS interno. Una modificación de Domain Overrides puede hacer que las consultas se envíen a un servidor no autoritativo, produciendo respuestas erróneas o timeouts. Diagnosticar diferenciando autoridad, ACL, host

override y conectividad VPN. Al documentar pruebas, utilizar dominios reservados de ejemplo, nunca nombres reales de instalaciones.

68.26. Matriz de incidencias: síntoma, causa probable y primera prueba

Síntoma	Hipótesis razonables	Comprobación prioritaria
«No Data» con consultas correctas	Sin entradas recientes; caché recreada; respuesta local	Verificar unbound y repetir consulta controlada
SERVFAIL de una sola zona	DNSSEC, delegación, autoridad lame o ruta	Logs + lookup de la zona
RTT/RTO altos en un solo servidor	Pérdida, congestión, ICMP irrelevante o timeout DNS	Captura de DNS y rutas
Muchos Timeout AAAA	Servidor específico, IPv6 o filtrado upstream	Prueba A/AAAA separada
Errores de DNSSEC	Reloj, cadena de confianza, fragmentación	NTP + logs DNSSEC
Resuelve en pfSense, falla en equipos	ACL de escucha, DNS cliente, firewall, caché cliente	Consulta desde equipo + registro
Solo falla en Multi-WAN	Gateway, DNS upstream o ruta de regreso	Status → Gateways + prueba por WAN

68.27. Registros y correlación temporal

Status → System Logs → DNS Resolver contiene eventos del demonio Unbound y otros procesos DNS. Para un incidente se recomienda anotar momento, zona afectada, tipo de consulta, IP de origen de prueba (si se puede anonimizar), gateway de salida y respuesta observada. Una captura de paquetes registra pruebas de red, pero puede contener nombres sensibles y datos sobre equipos: aplicar controles de acceso y medidas de anonimización antes de compartirla.

Un volumen elevado de logs en nivel debug puede consumir recursos y exponer dominios consultados. El ajuste de Log Level y el registro de todas las consultas deben reservarse para ventanas acotadas, con una política de conservación y revisión apropiadas.

68.28. Buenas prácticas de seguridad y rendimiento

Medida	Motivo técnico
Permitir DNS solo desde redes autorizadas	Evitar ofrecer un resolutor abierto o utilizable para abuso.
Mantener DNSSEC salvo incompatibilidad acreditada	Reduce la aceptación de respuestas manipuladas.
Usar cachés y TTL predeterminados como punto de partida	Preserva aprendizaje y evita carga de consulta innecesaria.
Evitar reinicios como técnica rutinaria de troubleshooting	Interrumpe servicio y elimina evidencia temporal útil.
Mantener hora NTP correcta	Clave para validación de firmas, certificados y registros.
Supervisar también WAN, gateway y estado de servicio	Una tabla de DNS no sustituye el resto de observabilidad.
Anonimizar capturas y logs al documentar	Puede revelar dominios, clientes y estructura de red.

68.29. Procedimiento seguro de recuperación y plan de reversión

01 Definir síntoma objetivo y alcance: dominio, usuarios, interfaces y momento de fallo.

02 Guardar evidencia: estado del servicio, consulta reproducible, extractos de logs depurados y rutas.

03 Aplicar una sola corrección sustentada por pruebas (ruta, ACL, forwarder o autoridad).

04 Comprobar resolución desde firewall y cliente representativo; verificar retorno de servicios dependientes.

05 Si no mejora, revertir exactamente el parámetro modificado y revisar efectos del cambio.

06 Anotar causa raíz, evidencia y seguimiento sin incluir información operativa identificativa en publicaciones.

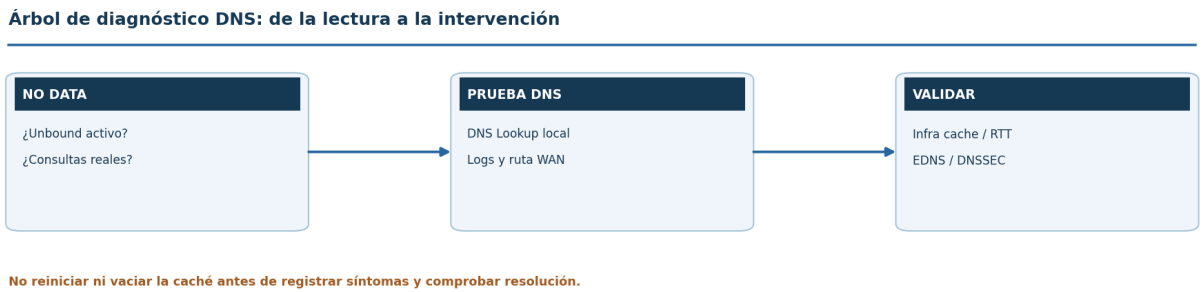


Figura 68.4. Diagnóstico ordenado antes de reiniciar o alterar la configuración DNS.

68.30. Glosario esencial

Término	Definición breve
Unbound	Servicio de resolución DNS de pfSense, con caché y validación DNSSEC.
Infra-cache	Memoria de comportamiento de servidores DNS (latencia, EDNS y señales lame).
RRset	Conjunto de registros DNS del mismo nombre, clase y tipo.
RTT / RTO	Tiempo estimado de espera y timeout efectivo con backoff.
Backoff exponencial	Incremento progresivo del tiempo de espera tras reintentos fallidos.
EDNS	Extensiones de DNS para capacidades adicionales y negociación de transporte.
Lame server	Servidor que no ofrece la autoridad o respuesta esperadas para una zona.
DNSSEC	Extensiones de seguridad para validar autenticidad/integridad de datos DNS.
DoT	DNS over TLS: cifrado de transporte hacia servidor compatible.
SERVFAIL	Código DNS de error en el procesamiento o resolución de una consulta.

68.31. Lista de comprobación para auditoría DNS

Antes de cerrar un incidente o de trasladar el sistema a producción, el administrador puede aplicar esta lista de verificación. Los resultados deben anotarse con fecha y sin exponer datos internos en documentación compartida.

Comprobación	Criterio de aceptación
Servicio	Unbound activo, sin eventos críticos recientes.
Resolución local	DNS Lookup devuelve una respuesta válida en tiempo razonable.
Configuración	Modo resolver/forwarding y DNS upstream documentados.
Infraestructura	No hay servidores persistentemente inutilizables sin explicación.
Seguridad	DNSSEC, reglas de acceso y hora del equipo revisados.

Comprobación	Criterio de aceptación
Salida WAN	Rutas, gateway y conectividad al DNS upstream verificados.
Evidencia	Capturas, resultados y logs protegidos y anonimizados.

68.32. Referencias oficiales y material normativo

Netgate · DNS Resolver Status

Netgate · DNS Resolver Mode

Netgate · DNS Resolver Configuration

Netgate · DNS Resolver Advanced Options

Netgate · CLI Commands

Netgate · Troubleshooting DNS Resolution

Netgate · Troubleshooting DNS Cache

Netgate · DNS Lookup

Netgate · Resolver Logs

Netgate · GUI Shortcut Icons

NLnet Labs · Unbound Timeout Information

NLnet Labs · Unbound Control Manual

NLnet Labs · Infrastructure Cache Data Structures

Las opciones avanzadas y el comportamiento de Unbound pueden variar según la versión de pfSense Plus y del servicio; debe consultarse la ayuda y la documentación vigentes del sistema administrado.

69 Status → Filter Reload

Recarga del filtro PF · NAT y estados · Seguimiento de errores · Sincronización HA · Recuperación segura

La pantalla Status → Filter Reload concentra dos tareas operativas: iniciar una recarga manual del conjunto de reglas del cortafuegos y observar su progreso. En entornos de alta disponibilidad puede mostrar, además, un control separado para forzar la sincronización XMLRPC de la configuración.

El panel no sustituye a Firewall → Rules, Firewall → NAT ni Diagnostics → States: no se editan reglas ni se eliminan directamente estados desde esta vista. La función es aplicar y diagnosticar, no definir la política de seguridad.

PRINCIPIO DE ADMINISTRACIÓN Una recarga correcta indica que terminó el proceso de carga, pero no demuestra por sí sola que el tráfico previsto esté pasando, que las rutas sean correctas o que las sesiones antiguas hayan desaparecido.

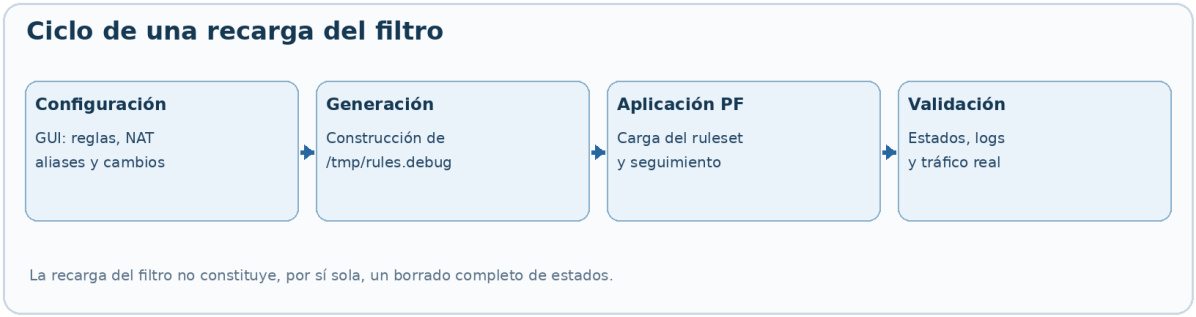


Figura 69.1. Del cambio de configuración al control del tráfico, con verificación posterior.

69.1. Objetivo operativo y ruta de acceso

Ruta: Status → Filter Reload. Es una pantalla de estado y acción administrativa puntual. Los cambios de firewall y NAT se realizan en las secciones correspondientes y, cuando la GUI lo solicita, se aplican mediante Apply Changes. Desde ese aviso puede accederse a la página de progreso de recarga.

Elemento	Función	Alcance
Reload Filter	Inicia una recarga manual del filtro	Modifica el ruleset activo; no reinicia el dispositivo
Reload status	Muestra mensajes emitidos durante la operación	Seguimiento, no edición de políticas
Force Config Sync (condicional)	Fuerza sincronización XMLRPC hacia el nodo configurado	Solo HA con XMLRPC activado
Accesos del encabezado	Atajos contextuales y ayuda	Los destinos se verifican con tooltip en la GUI

69.2. Lectura exacta de la pantalla mostrada

La captura presenta la ruta Status / Filter Reload y un bloque titulado Filter Reload con botón verde «Reload Filter» e icono de flechas circulares. Debajo aparece el panel «Reload status», sin mensajes visibles en ese instante. No se muestran campos de texto, selector de interfaces ni opción para elegir qué reglas recargar.

Los pequeños iconos del encabezado pertenecen a la navegación contextual de la interfaz. Su destino concreto puede depender del tema y de la versión: en administración se debe consultar el tooltip antes de atribuir a cada icono una acción específica. No son controles individuales de recarga dentro del formulario.

INTERPRETACIÓN Un panel Reload status vacío no permite diagnosticar por sí mismo un problema: puede no existir una operación visible en curso. Es necesario lanzar la recarga cuando proceda y esperar los mensajes de finalización.

69.3. Qué significa recargar el filtro en pfSense Plus

pfSense traduce los objetos definidos en la GUI —reglas de interfaz y flotantes, NAT, aliases y políticas relacionadas— a un ruleset interpretable por Packet Filter (PF). El archivo generado /tmp/rules.debug permite inspeccionar el resultado; es un producto de la configuración, no la fuente persistente de la política.

Durante la recarga, pfSense vuelve a generar y aplicar la configuración del filtro. El proceso puede incorporar reglas y anchors construidos por otras funciones y paquetes. El archivo /tmp/rules.debug puede ser sobrescrito en una recarga posterior: editarlo manualmente no constituye una modificación permanente.

Capa	Qué representa	Qué revisar
Configuración GUI	Política declarativa de reglas, NAT y aliases	Que el cambio esté guardado y aplicado
Archivo generado	/tmp/rules.debug producido por pfSense	Sintaxis y presencia de la regla esperada
Ruleset cargado	Reglas interpretadas por PF	pfctl -sr, pfctl -sn, anchors
Tabla de estados	Conexiones y traducciones existentes	Diagnostics → States
Tráfico real	Paquetes, decisiones y rutas efectivas	Firewall logs y capturas

69.4. Cuándo utilizar Reload Filter y cuándo no

Se utiliza cuando se necesita forzar una aplicación del filtro, comprobar si un conjunto de reglas ha quedado operativo o reproducir el proceso para diagnosticar una anomalía. La propia documentación Netgate lo recomienda al investigar reglas nuevas que no parecen haberse aplicado.

Situación	¿Recargar?	Justificación
Cambio de reglas pendiente de Apply Changes	Primero Apply Changes	No confundir guardar, aplicar y recargar
La regla no aparece en PF, sin error conocido	Sí, controladamente	Repetir carga y consultar mensajes
Conexión antigua sigue pasando tras bloqueo	No es suficiente	Puede persistir un estado ya creado
DNS o gateway fuera de servicio	No como primera acción	Comprobar el subsistema afectado
Error por paquete que inserta reglas	Con diagnóstico y plan de recuperación	La recarga puede detenerse en ese componente
Sincronizar secundaria HA	Force Config Sync, si procede	Es una función distinta

69.5. Botón Reload Filter: secuencia de operación segura

1. Confirmar el propósito del cambio y registrar qué política se espera observar después.
2. En un entorno crítico, garantizar una vía de administración independiente (consola, gestión fuera de banda o acceso local) y conservar copia de configuración.
3. Entrar en Status → Filter Reload y pulsar «Reload Filter» una sola vez.
4. Esperar la actualización de «Reload status»; el proceso puede finalizar muy rápidamente.
5. Desplazarse al final del panel: allí aparecen los mensajes más recientes.
6. Buscar «Done.» como finalización normal; si se detiene o muestra errores, anotarlos y seguir el diagnóstico, sin pulsar repetidamente.
7. Comprobar reglas y NAT cargadas, después probar conectividad nueva y revisar la tabla de estados.

OPERACIÓN CON IMPACTO No se recomienda recargar de manera repetitiva durante una incidencia sin antes observar el resultado de la primera ejecución. Se pueden enmascarar errores, alterar contadores y agravar una configuración incorrecta.

69.6. Reload status: progreso, orden de mensajes y diagnóstico

Netgate indica que el estado se actualiza automáticamente. Los mensajes nuevos se colocan en la parte inferior y, en instalaciones pequeñas, a menudo solo se aprecia «Done.»: puede ser una ejecución normal sin cambios pendientes. En sistemas con muchas reglas o paquetes, el proceso puede tardar más.

Salida observada	Interpretación prudente	Siguiente comprobación
Done.	Proceso finalizado según la vista	Prueba efectiva del flujo y PF
Mensajes intermedios y avance	Recarga en curso	Esperar y leer el final
Error de sintaxis o carga	Ruleset no aplicado como se esperaba	Identificar regla, alias o paquete causante
Se detiene en un paquete	Posible bloqueo en componente concreto	Revisar paquete y registros asociados
Sin información visible	Insuficiente para concluir éxito o fallo	Realizar operación controlada y observar

69.7. PF: recarga de reglas frente a reinicio del firewall

Un filtro puede ser recargado sin reiniciar FreeBSD ni reiniciar todos los servicios. Por el contrario, un reinicio de sistema afecta a procesos, interfaces y disponibilidad general. Tampoco equivale Reload Filter a detener el firewall mediante pfctl -d: esta última orden desactiva el filtrado y también NAT, con repercusiones severas de seguridad y conectividad.

Operación	Cambio principal	Riesgo y uso
Reload Filter	Regenera / vuelve a cargar reglas PF	Puede alterar tratamiento de conexiones nuevas
Reset States	Elimina estados seleccionados o tabla completa	Puede cortar sesiones establecidas
Reboot System	Reinicia el sistema operativo y servicios	Interrupción general; no es diagnóstico inicial
pfctl -d	Deshabilita PF y NAT	Recuperación excepcional con consola y control

69.8. Sesiones existentes y nuevas: por qué no siempre cambia el tráfico

PF es un cortafuegos con seguimiento de estado: al permitir una conexión, registra información que puede ser utilizada para el tráfico posterior. Una nueva regla de bloqueo no tiene por qué cortar una conexión que ya dispone de un estado válido. Esta distinción explica muchos falsos fallos de recarga.

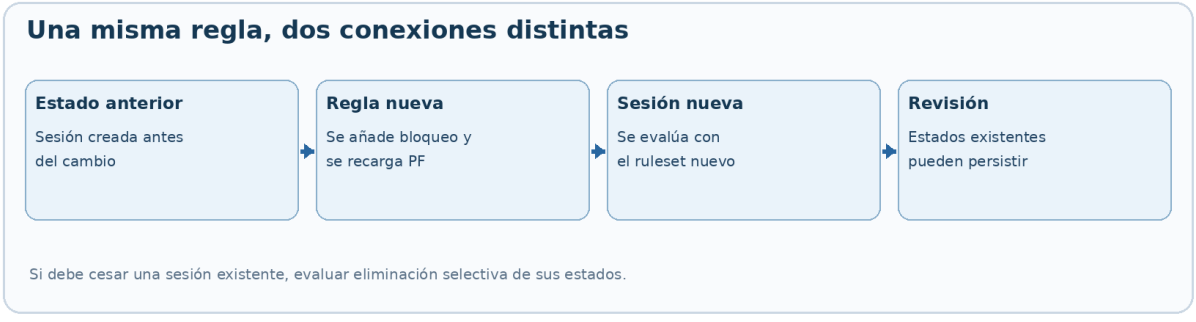


Figura 69.2. Efecto de una regla nueva sobre tráfico previamente autorizado y nuevas conexiones.

Cuando una modificación de NAT, bloqueo o shaping debe imponerse de inmediato a sesiones ya activas, Netgate documenta Diagnostics → States → Reset States. Esa operación es separada y disruptiva; es preferible inspeccionar primero el estado afectado y, si la función disponible lo permite, eliminar únicamente los estados relevantes.

ADVERTENCIA Borrar todos los estados puede interrumpir VPN, conexiones de base de datos, sesiones de usuario y administración web. No es una consecuencia automática ni necesaria de pulsar Reload Filter.

69.9. NAT, port forwards, aliases y reglas dinámicas

En PF conviven reglas de filtrado y traducciones NAT. Para diagnosticar, comprobar tanto la política visible en Firewall → Rules como las reglas realmente cargadas de traducción. Algunas funciones crean anchors adicionales que no se aprecian en una lectura superficial del listado principal: por ejemplo, paquetes o servicios que añaden reglas dinámicas.

Un cambio de alias basado en FQDN puede depender también de la resolución periódica de nombres; recargar PF no corrige por sí mismo una dirección DNS errónea ni arregla un enlace de salida sin conectividad. El tráfico que no atraviesa el firewall, como dos hosts en la misma VLAN conectados al mismo switch, tampoco se controla con estas reglas L3.

69.10. Comandos de inspección: lectura frente a modificación

Comando / herramienta	Qué proporciona	Precaución
pfctl -sr	Reglas de filtrado activas	Lectura; puede incluir reglas extensas
pfctl -sn	Reglas NAT activas	Lectura; cotejar con objetivos
pfctl -vvsr	Reglas y contadores ampliados	Lectura; contadores pueden cambiar tras recargas
pfctl -sa	Información global del motor PF	Lectura; salida voluminosa
pfSsh.php playback pfanchordrill	Detalle de anchors de PF	Lectura; paquetes pueden aportar reglas
pfctl -f /tmp/rules.debug	Reaplica manualmente reglas generadas	Modifica estado PF; usar solo con justificación técnica

Para ejecutar comandos, utilizar acceso de consola o Diagnostics → Command Prompt cuando la política lo permita. El último comando anterior no es una prueba de solo lectura: Netgate lo cita para verificar posibles errores de carga, pero debe ejecutarse únicamente después de revisar el contexto y disponer de un camino de recuperación.

69.11. El panel y el flujo del cortafuegos: qué observar en los logs

La pestaña Firewall dentro de Status → System Logs es el primer punto de diagnóstico cuando se sospecha que un flujo es bloqueado. Por defecto se registran los bloqueos habituales, mientras que el tráfico permitido no necesariamente se registra salvo que se active logging en la regla correspondiente. Conviene correlacionar hora, interfaz, IP, puerto, protocolo y estado de conexión.

Cuando se prueba una regla, lanzar tráfico desde un equipo de origen conocido, verificar que la conexión atraviesa la interfaz prevista y revisar inmediatamente Diagnostics → States. Una entrada de estado demuestra que el tráfico fue permitido al crear la sesión, pero no acredita que la aplicación remota responda correctamente.

69.12. Verificación de una regla de permiso: caso guiado

1. Crear o revisar la regla de paso que deba permitir tráfico desde un host de laboratorio 192.0.2.10 hacia un destino documentado 198.51.100.20.
2. Guardar y aplicar en Firewall → Rules, comprobar el aviso y el estado de carga.
3. Si la regla sigue sin actuar, visitar Filter Reload y ejecutar una recarga manual observada.
4. Comprobar el ruleset con pfctl -sr y la traducción, si aplica, con pfctl -sn.
5. Generar una conexión NUEVA de prueba, inspeccionar logs y buscar el estado asociado.
6. Si PF permite el flujo pero el servicio no contesta, estudiar DNS, retorno, gateway, MTU y extremo remoto.

69.13. Verificación de una regla de bloqueo: evitar pruebas engañosas

Para validar una política de bloqueo, repetir la prueba mediante una conexión nueva. Si el host sigue enviando datos por una sesión previamente establecida, localizarla en Diagnostics → States antes de concluir que la recarga falló. Evitar usar una sesión de administración activa como primera prueba.

1. Anotar IP de origen y destino, protocolo y puerto de la conexión afectada.
2. Comprobar reglas, orden, floating rules y si la política está guardada y aplicada.
3. Consultar Filter Reload para detectar problemas de carga y comprobar «Done.».
4. Realizar una conexión nueva o evaluar, con autorización, eliminar solo el estado anterior correspondiente.
5. Revisar bloqueos en Firewall Logs y confirmar la ausencia de estados nuevos autorizados.

69.14. Alta disponibilidad: aparición condicional de Force Config Sync

Cuando el firewall participa en un clúster HA y tiene sincronización de configuración XMLRPC habilitada, Netgate documenta la aparición del botón «Force Config Sync» en esta misma página. La pulsación solicita replicar la configuración hacia el nodo definido en la sincronización. No debe confundirse con recargar las reglas locales ni con conmutar el nodo CARP.

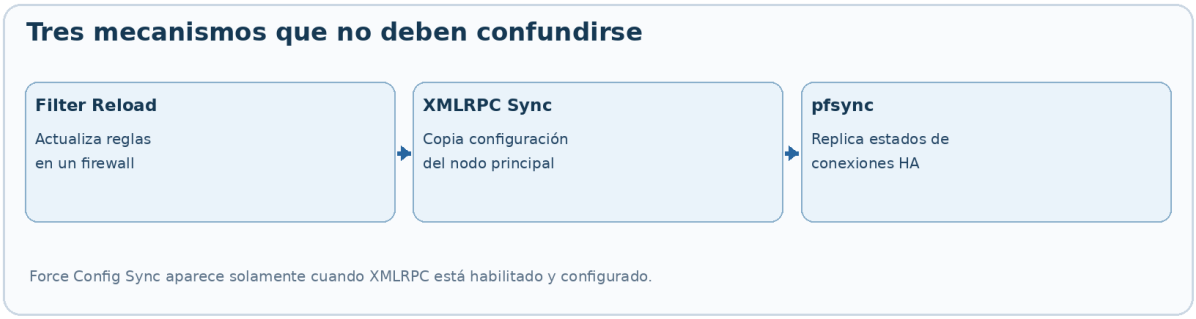


Figura 69.3. Recarga del filtro local, sincronización de configuración y replicación de estados.

Mecanismo	Objetivo	Qué no hace
Reload Filter	Aplica reglas PF en el equipo desde el que se ejecuta	No cambia el rol CARP por sí solo
Force Config Sync / XMLRPC	Envía ajustes compatibles al nodo secundario configurado	No replica estados de sesiones existentes
pfsync	Sincroniza estados entre nodos HA	No reemplaza reglas, NAT ni certificados
CARP	Gestiona propiedad de direcciones VIP compartidas	No reescribe reglas PF por sí mismo

HA XMLRPC debe configurarse solo en el nodo principal. Antes de forzar sincronización, comprobar coincidencia del orden de interfaces, transporte de la GUI, credenciales, permisos y qué apartados están incluidos. Una asociación errónea puede aplicar reglas a interfaces incorrectas.

69.15. Multi-WAN y rutas: limitaciones de la recarga

La recarga puede activar cambios de reglas que incluyen selección de gateway o políticas de encaminamiento. No obstante, un gateway caído, una ruta incorrecta, un retorno asimétrico o un grupo de gateways mal dimensionado requieren diagnóstico específico en Status → Gateways, Diagnostics → Routes y tablas de estados. No usar la recarga como sustituto de comprobar enlaces y rutas.

Si se modificó una política de salida sobre conexiones ya establecidas, los estados asociados pueden conservar comportamiento anterior. Registrar si la validación usa una sesión nueva o antigua, especialmente en aplicaciones de larga duración y conexiones UDP.

69.16. Paquetes y reglas añadidas mediante anchors

Cuando el proceso se detiene al procesar un paquete, no conviene insistir sin diagnóstico. Algunos paquetes instalan sus propias reglas en anchors PF. La herramienta pfanchordrill ayuda a inspeccionarlas y los logs permiten identificar el servicio o paquete implicado. Resolver el error del componente y repetir el proceso una sola vez en una ventana controlada.

69.17. Plan de diagnóstico reproducible si el resultado es anómalo



Figura 69.4. Orden recomendado para aislar problemas después de una recarga.

Síntoma	Hipótesis inicial	Prueba segura
La regla nueva no tiene efecto	Recarga fallida o sesión antigua	Reload status + Diagnostics → States
El proceso no termina	Error de configuración o paquete	Leer último mensaje y logs de sistema
Se pierde la administración	Bloqueo del propio acceso o ruta	Consola local / vía fuera de banda
NAT parece no cambiar	Estado previo mantiene traducción	pfctl -sn y prueba con sesión nueva
Reglas distintas en HA	XMLRPC pendiente o fallida	Comparar nodos y revisar ajustes HA
Una VPN se corta	Dependencia de ruta, NAT o política	Correlacionar logs VPN y gateways

69.18. Recuperación segura cuando la recarga corta acceso

Una política mal definida puede bloquear la administración del propio firewall. El plan de recuperación debe existir ANTES de aplicar cambios que afecten a la interfaz de gestión. Netgate documenta procedimientos de recuperación por consola. Desactivar PF mediante pfctl -d también desactiva NAT y expone de forma transitoria rutas antes protegidas, por lo que no es una maniobra ordinaria.

1. Usar la consola o el acceso fuera de banda preestablecido y confirmar que el equipo sigue operativo.
2. Revisar la configuración y determinar qué regla o alias causó el bloqueo; evitar borrar la configuración completa.
3. Restaurar una política conocida o una versión anterior mediante Config History, según proceda.
4. Aplicar de nuevo la sección afectada y verificar acceso LAN y administración remota autorizada.
5. Documentar cronología, reglas, impacto y evidencia de las pruebas posteriores.

69.19. Procedimiento empresarial: publicación de servicio con NAT

Escenario didáctico: un servicio publicado sobre 203.0.113.50 debe redirigir tráfico TCP 443 hacia 192.0.2.20, con autorización explícita y segmentación interna. Son IP reservadas para documentación, no ejemplos de configuración operativa pública. Antes de cambiar NAT se comprueban los filtros de entrada, el estado actual de la publicación y las sesiones que podrían depender de ella.

1. Revisar Firewall → NAT y Firewall → Rules, identificando la regla relacionada.
2. Realizar respaldo de configuración y disponer de una prueba remota independiente.
3. Guardar y aplicar cambios, observando Status → Filter Reload.
4. Validar NAT cargado, logs de la interfaz externa y conexión nueva desde una red de prueba.

5. Si la sesión antigua persiste con traducción previa, evaluar eliminación selectiva de estados en ventana autorizada.

69.20. Procedimiento empresarial: nueva regla restrictiva sin corte de administración

En una segmentación de VLAN se quiere restringir comunicación entre una red de usuarios y otra de servidores, sin afectar el acceso de gestión. La norma es comprobar primero el trayecto de la administración, la posición de la regla y posibles conexiones creadas previamente. La recarga es la última parte de aplicar el cambio, seguida de una prueba de puerto y un plan de reversión.

69.21. Procedimiento empresarial: dos nodos pfSense Plus en HA

Con un clúster CARP funcional y pfsync activo, un cambio de políticas en el nodo principal puede sincronizarse mediante XMLRPC con el secundario si la opción correspondiente está habilitada. El operador debe verificar que ambos tienen la misma asignación lógica de interfaces y que el secundario ha recibido las reglas esperadas. Solo si se detecta un problema y se ha revisado la configuración, se usa Force Config Sync en el principal.

69.22. Ventana de mantenimiento, observabilidad y evidencias

Antes	Durante	Después
Respaldo de config.xml	Registrar hora y operador	Comprobar acceso de administración
Vía alternativa de acceso	Capturar Reload status final	Probar flujo permitido y bloqueado
Lista de sesiones críticas	Evitar varias recargas superpuestas	Comparar PF y NAT efectivos
Plan de reversión acordado	Observar VPN y gateways	Guardar logs y documentar incidencia

Para auditoría, resulta más útil un registro con cambio exacto, hora, línea de finalización, prueba realizada, resultado y responsable que una captura aislada de «Done.». La GUI no ofrece en esta vista una herramienta de validación extremo a extremo.

69.23. Rendimiento, efectos secundarios y precauciones

Las recargas pueden producir variación de contadores y picos de actividad, especialmente con reglas numerosas, aliases extensos o paquetes que añaden anchors. Evitar ciclos de recarga repetidos en horario de máxima carga. La carga correcta del filtro no garantiza que los servicios enlazados hayan reiniciado ni que una modificación en otra sección que requiera reinicio propio se haya aplicado.

69.24. Errores comunes que conviene prevenir

Confundir «Done.» con conectividad verificada y omitir una prueba real desde el cliente.

Olvidar que estados creados con reglas antiguas pueden seguir permitiendo tráfico.

Recargar PF para intentar resolver problemas de DNS, WAN o rutas no relacionadas.

Borrar todos los estados cuando bastaría validar con una conexión nueva.

Usar Force Config Sync en el secundario o sin comprobar asociación de interfaces.

Editar /tmp/rules.debug esperando que el cambio permanezca tras la siguiente recarga.

Ejecutar comandos con efectos sobre PF sin disponer de acceso de recuperación.

69.25. Glosario esencial

Término	Significado
PF	Packet Filter, motor de filtrado stateful utilizado por pfSense
Ruleset	Conjunto de reglas de filtrado y NAT cargado en el motor

Término	Significado
Estado / state	Registro de una conexión ya autorizada y sus atributos
Anchor	Subconjunto de reglas gestionado dentro de la estructura PF
XMLRPC	Mecanismo de sincronización de configuraciones en HA
pfsync	Mecanismo de sincronización de estados entre nodos
CARP	Protocolo de redundancia de direcciones IP virtuales
NAT	Traducción de direcciones y/o puertos entre redes

69.26. Lista final de comprobación del administrador

La modificación prevista está guardada y aplicada en su sección.

La recarga terminó; la última salida contiene «Done.» sin errores no resueltos.

La regla esperada aparece en PF; NAT y anchors se han contrastado si son relevantes.

Las pruebas han diferenciado sesiones nuevas de estados previos.

Los logs no muestran bloqueos inesperados para tráfico crítico.

La administración, VPN, gateways y rutas siguen funcionando.

En HA, se ha comprobado qué sincronizó XMLRPC y cuál es el rol CARP.

Existe registro de cambio y procedimiento de reversión.

69.27. Referencias oficiales y lectura complementaria

Netgate — Filter Reload Status	**Netgate — Troubleshooting Firewall Rules**
Netgate — Viewing the PF ruleset	Netgate — Firewall Fundamentals
Netgate — Reset State Table	Netgate — Viewing Firewall States
Netgate — High Availability Synchronization Settings	Netgate — XMLRPC Configuration Synchronization
Netgate — Troubleshooting High Availability	Netgate — Troubleshooting Access when Locked Out
Netgate — Backup and Restore	Netgate — Working with Log Files
Netgate — pfInfo	Netgate — High Availability Testing

70 Status → Gateways

Supervisión dpinger · Latencia y pérdida · Grupos Multi-WAN · Estados PF · Failover y diagnóstico

Las puertas de enlace determinan por dónde puede salir el tráfico y cómo se selecciona una ruta ante cambios de disponibilidad. Status → Gateways combina información operativa de las rutas supervisadas con una segunda pestaña dedicada al estado de los grupos de gateways.

La página de estado no crea puertas de enlace, no modifica sus umbrales y no configura grupos. Esos cambios se realizan en System → Routing y se ponen en uso mediante las funciones compatibles y las políticas de firewall que correspondan.

PRINCIPIO DE SUPERVISIÓN Una flecha o estado Online en una interfaz no demuestra por sí sola acceso a Internet; una respuesta positiva del monitor tampoco garantiza conectividad hacia todos los destinos.

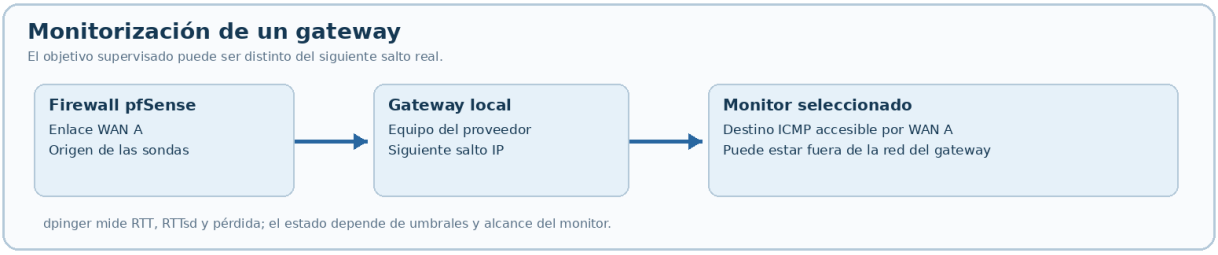


Figura 70.1. Origen de sondas, puerta de enlace y objetivo de supervisión como tres conceptos distintos.

70.1. Propósito, ruta y alcance operativo

Ruta exacta: Status → Gateways. Pestañas: Gateways y Gateway Groups. Esta vista reúne tanto gateways definidos manualmente como los creados por interfaces dinámicas. Un gateway puede aparecer como predeterminado para IPv4 o IPv6, pero esa condición no equivale a ser el único camino disponible.

Vista	Presenta	No sustituye
Gateways	Direcciones de gateway/monitor, tiempos, pérdida, estados y controles sobre estados de firewall.	System → Routing → Gateways y Diagnostics → States.
Gateway Groups	Miembros por tiers y comportamiento esperado de grupos previamente definidos.	System → Routing → Gateway Groups y Firewall → Rules.

70.2. Lectura editorial de las pantallas

La primera pestaña presenta una tabla con columnas Name, Gateway, Monitor, RTT, RTTsd, Loss, Status, Description y Action. En un mismo listado pueden coexistir enlaces de familias IP diferentes y otros todavía sin mediciones consolidadas. La segunda pestaña muestra las columnas Group Name, Gateways, Description y Action; una lista sin filas indica que no hay grupos mostrados en esa vista, no que el servicio de monitoreo haya fallado.

Las herramientas de navegación del encabezado —actualizar, detener la actualización, ajustes y accesos gráficos o de lista según versión/tema— deben verificarse por su descripción contextual antes de atribuirles una operación. No forman parte de los botones de eliminación selectiva de estados que aparecen dentro de cada fila.

70.3. Columnas de Gateways: identidad y direccionamiento

Campo	Interpretación	Precaución
Name	Nombre lógico del gateway; “(default)” identifica el predeterminado de su familia.	El nombre no tiene por qué coincidir con interfaz ni monitor.

Campo	Interpretación	Precaución
Gateway	Dirección IP del siguiente salto.	Puede ser privada detrás del equipo de un operador; no implica IP pública.
Monitor	Objetivo ICMP usado para calcular calidad.	Puede ser distinto del gateway físico; “(unmonitored)” indica monitorización deshabilitada.
Description	Texto administrativo del gateway.	En gateways dinámicos puede proceder de una descripción generada.

70.4. RTT: tiempo de ida y vuelta

RTT (Round Trip Time) estima la latencia de las sondas hacia el destino de monitorización, normalmente en milisegundos. La interpretación depende de la distancia física, tecnología del enlace y congestión. Una latencia reducida hacia el router del proveedor puede coexistir con problemas aguas arriba; para medir disponibilidad de Internet debe escogerse cuidadosamente el objetivo.

70.5. RTTsd: variación de latencia

RTTsd representa la desviación estándar de las últimas observaciones de RTT. Un valor alto significa variabilidad y puede anticipar jitter perceptible en VoIP, videollamadas o aplicaciones sensibles a temporización. No es un ancho de banda ni una medida de pérdida de paquetes: complementa a RTT y Loss.

70.6. Loss: pérdidas durante el sondeo

Loss cuantifica el porcentaje de sondas de monitorización que no obtuvieron respuesta en la ventana del daemon dpinger. Una pérdida sostenida puede sugerir fallo de circuito o de ruta, pero algunos hosts limitan o descartan ICMP sin afectar al tráfico real. Nunca atribuir automáticamente toda pérdida a la línea contratada sin revisar el destino de monitorización y el comportamiento de aplicaciones.

70.7. Status: estados y datos todavía no consolidados

Estado visual	Significado operativo	Comprobación recomendada
Online	El destino de monitorización responde dentro de condiciones válidas.	Cruzar con DNS, rutas y aplicaciones reales.
Warning	Alerta de latencia o pérdida según umbrales del gateway.	Revisar tendencia de RTT/RTTsd, Loss y logs.
Offline / Down	El gateway supera una condición grave de monitorización o falla su acceso.	Verificar capa física, monitor, rutas y upstream.
Pending / Gathering Data	Estado transitorio o sin resultados suficientes; texto variable según versión.	Esperar muestra y revisar si interfaz está configurada/en servicio.
(unmonitored)	Supervisión desactivada; no hay evaluación de calidad por dpinger.	No confiar en ello para detectar failover automáticamente.

DISTINCIÓN TÉCNICA La documentación general enumera Online, Offline y Warning; las interfaces y widgets de distintas versiones pueden mostrar Pending, Unknown o Gathering Data antes de tener información útil. No se deben equiparar automáticamente a una avería.



Figura 70.2. Estados informativos y advertencias: clasificación conceptual para la operación diaria.

70.8. Colores, iconos y accesos de la página

Las celdas de estado usan colores para facilitar la lectura, pero los nombres de estado y las medidas son más fiables que el color, que puede variar por tema o versión. La indicación de gateway predeterminado se expresa al lado del nombre. Los iconos de la columna Action están orientados a administrar estados de conexiones existentes y deben tratarse como acciones de impacto.

70.9. Tres acciones diferentes de la columna Action

Icono / alcance	Estados que puede eliminar	Limitación o riesgo
Cruz circular por nombre	Estados creados por reglas con policy routing al gateway concreto por su nombre.	No comprende estados que usaron ese gateway como miembro de un grupo.
Cruz circular por IP	Estados asociados al gateway por su IP en policy routing directo, grupo o reply-to WAN.	Puede afectar sesiones de varias políticas o interfaces.
Cruz simple (default)	Estados cuyo gateway de salida es el predeterminado de IPv4/IPv6.	Puede afectar conexiones de gestión, VPN y tráfico interno; impacto amplio.

PELIGRO: PÉRDIDA DE SESIONES No utilizar estos iconos para “probar si mejora” una incidencia. Su efecto es eliminar estados del filtro PF, no corregir la conectividad del proveedor. Preparar siempre un canal administrativo alternativo.

70.10. Gateway Groups: interpretación de la segunda pestaña

Status → Gateways → Gateway Groups muestra grupos creados previamente. Group Name identifica el objeto; Gateways presenta los miembros agrupados por tiers; Description ofrece su finalidad; Action permite eliminar selectivamente estados de policy routing asociados al nombre de ese grupo. Una tabla vacía se resuelve, si se necesita la función, creando el grupo en System → Routing → Gateway Groups y aplicándolo donde proceda.

70.11. Tier y prioridad: conmutación frente a balanceo

Tier 1 tiene preferencia sobre Tier 2; si todos los miembros del tier preferido dejan de estar disponibles, se pasa al siguiente tier viable. Cuando dos enlaces comparten el mismo tier, el firewall puede repartir conexiones nuevas entre ellos, si el consumidor del grupo permite balanceo. No reparte cada paquete de forma independiente ni garantiza distribución proporcional al caudal real.



Figura 70.3. Dos asignaciones de tiers habituales; el grupo exige configuración y asociación a una política.

70.12. El grupo no hace nada hasta que se utiliza

Netgate indica expresamente que un grupo creado no inicia acciones por sí mismo. Debe seleccionarse, por ejemplo, en el campo Gateway de una regla de Firewall → Rules para policy routing, o como gateway predeterminado del propio firewall cuando se trate de un grupo de failover compatible. No todas las funciones permiten balanceo: el gateway predeterminado y ciertos endpoints VPN exigen un gateway por tier.

70.13. Parámetros de creación de grupos y dónde se modifican

Opción en System → Routing	Uso	Consecuencia administrativa
Gateway Priority / Tier	Define miembros y prioridad (Tier 1–5, Never).	Mismo tier: reparto por conexiones; distinto tier: respaldo.
Trigger Level	Member Down, Packet Loss, High Latency o ambos.	Decide cuándo se excluye un miembro para el grupo.
Keep Failover States	Control de estados al recuperarse gateway preferido.	Puede conservar sesiones por respaldo o forzar su recreación.
Virtual IP	Dirección a emplear cuando una función exige vínculo específico.	Solo para configuraciones que lo requieren, como algunos escenarios de HA/VPN.

70.14. Trigger Level y umbrales: reglas de alarma

Member Down responde a fallos graves; Packet Loss responde al umbral inferior de pérdida; High Latency al de latencia; Packet Loss or High Latency a cualquiera de ambos. El nivel elegido determina la sensibilidad de failover, no modifica los valores de umbrales medidos por dpinger.

70.15. dpinger: mecanismo de medida y registro

pfSense emplea el daemon dpinger para enviar sondas ICMP desde la interfaz apropiada, acumular muestras, calcular latencia y pérdida, y emitir alarmas o recuperación. La vista de estado es una síntesis del proceso; para explicar una transición se consulta Status → System Logs → System / Gateways. Las líneas de arranque de dpinger no indican necesariamente error, mientras que Alarm y Clear permiten localizar degradaciones y restablecimientos.

70.16. Umbrales y temporizadores avanzados de monitorización

Estos valores pertenecen a System → Routing → Gateways, opciones avanzadas; son valores documentados por Netgate para configuraciones habituales, no recomendaciones universales. Se deben validar frente al SLA y a una línea base real, especialmente en enlaces móviles, satélite o radio.

Parámetro	Valor documentado	Efecto de modificarlo
Latency From / To	200 / 500 ms	Umbrales de aviso y caída por latencia; aumentarlos reduce sensibilidad.
Packet Loss From / To	10 % / 20 %	Aviso y caída por pérdida; subirlos puede ocultar degradación.
Probe Interval	500 ms	Frecuencia de sondeo; menos frecuente retrasa detección.
Loss Interval	2.000 ms	Plazo para declarar sonda perdida; debe ser >= umbral alto de latencia.
Time Period	60.000 ms	Ventana de promedio; más larga suaviza picos y retrasa alarmas.
Alert Interval	1.000 ms	Periodicidad de evaluación; debe ser >= Probe Interval.

CAMBIO CONTROLADO Ajustar umbrales puede reducir falsos positivos, pero también impedir que se detecte una incidencia real. Registrar la línea base, modificar un parámetro y contrastar durante una ventana representativa.

70.17. Selección correcta de Monitor IP

Una dirección del router del operador mide, ante todo, el tramo firewall–router; si la caída ocurre después del router, el monitor puede permanecer Online. Un objetivo externo estable, alcanzable por la WAN evaluada, facilita detectar fallos aguas arriba. Netgate recomienda un destino distinto por gateway y recuerda que pfSense suele instalar rutas específicas para que cada monitor se compruebe por la WAN correcta.

Para redes con CGNAT, enlaces móviles y dobles NAT, distinguir la IP del gateway local y una IP alcanzable en Internet. No utilizar una dirección interna de otra sede como objetivo si su disponibilidad depende de una VPN cuya ruta se está diagnosticando, salvo que esa dependencia sea exactamente lo que se desea medir.

70.18. Monitorización desactivada y supresión de acciones

Disable Gateway Monitoring impide disponer de mediciones fiables y puede desactivar la lógica de detección de fallos de Multi-WAN. Disable Gateway Monitoring Action conserva las mediciones, pero suprime las actuaciones automáticas ante cambios de estado. Son controles distintos y deben tratarse de manera explícita en la documentación de explotación.

70.19. Default gateway, policy routing y tráfico originado por el firewall

El tráfico iniciado por el firewall utiliza normalmente su ruta predeterminada, salvo rutas específicas o servicios vinculados a otra interfaz. En cambio, una regla de firewall puede forzar un gateway o grupo para tráfico que atraviesa el equipo. Una WAN Online no asegura que un proceso del propio firewall esté usando esa WAN; comparar System → Routing → Gateways, Diagnostics → Routes y la regla que procesa el flujo.

70.20. NAT y reply-to en entornos Multi-WAN

Las conexiones entrantes por interfaces de tipo WAN suelen usar reply-to para devolver respuestas por la misma WAN. Un estado asociado por reply-to puede aparecer en el alcance de eliminación por IP del gateway. Para tráfico LAN, las reglas con Gateway generan policy routing; si se utiliza una ruta alternativa, comprobar también Outbound NAT y el retorno por la interfaz correcta.

70.21. Sesiones existentes durante un failover

El failover generalmente afecta a nuevas conexiones y a conexiones que se recrean. Las sesiones existentes pueden permanecer en la tabla de estados aunque el camino original haya fallado; por eso existen políticas opcionales de eliminación de estados. Borrar estados indiscriminadamente puede interrumpir servicios estables, y el retorno de la WAN primaria puede no mover por sí mismo todas las sesiones existentes.

70.22. Opciones de eliminación automática de estados

Ajuste global	Comportamiento	Impacto
Do not kill states (predeterminado)	No elimina automáticamente los estados durante fallo del gateway.	Menos disruptivo; algunas sesiones tardarán en reconectar.
Kill states for all gateways which are down	Elimina estados selectivos con información de policy routing.	No cubre todos los estados de cambio de gateway predeterminado.
Flush all states on gateway failure	Vacía toda la tabla ante fallo de cualquier gateway.	Muy disruptivo; considerar solo en casos diseñados y probados.

Las opciones avanzadas en System → Advanced → Miscellaneous y algunas opciones por gateway/grupo pueden sustituir el comportamiento global. “Keep Failover States” del grupo también interviene al recuperar la WAN preferida. Documentar tanto el fallo como la recuperación: no son simétricos.

70.23. IPv4, IPv6 y enlaces pendientes

Cada familia IP tiene su tabla de rutas, gateway por defecto y objetivos de comprobación. Un enlace IPv4 funcional no presupone conectividad IPv6; a su vez, una entrada IPv6 en Pending no confirma interrupción general de salida. En enlaces opcionales, desconectados o sin direccionamiento válido, las mediciones pueden permanecer sin consolidar. Comprobar la configuración real de cada interfaz antes de intervenir.

70.24. Procedimiento 1: revisión diaria y línea base

1. Entrar en Status → Gateways y registrar fecha, nombre lógico, familia IP, RTT, RTTsd, Loss y Status sin copiar identificadores de usuarios o sedes.
2. Identificar qué gateway figura como predeterminado; contrastar con Diagnostics → Routes.
3. Examinar la pestaña Gateway Groups; confirmar tiers y grupos aplicados realmente a reglas.
4. Correlacionar mediciones con Status → Monitoring y el registro System / Gateways.
5. Validar un servicio DNS, un destino externo y, cuando proceda, las aplicaciones críticas; archivar los resultados de forma segura.

70.25. Procedimiento 2: configurar un failover mínimo y verificarlo

1. Preparar respaldo de configuración y acceso fuera de banda; confirmar que ambas WAN tienen gateway y monitor fiables.
2. En System → Routing → Gateway Groups crear un grupo con WAN_A en Tier 1 y WAN_B en Tier 2, definiendo Trigger Level de acuerdo con el objetivo de disponibilidad.
3. Aplicar el grupo en la regla pertinente de Firewall → Rules y verificar NAT de salida para ambas WAN; para tráfico del firewall, configurar un grupo de failover compatible como default si procede.
4. Comprobar en Status → Gateways que ambos enlaces están Online antes de realizar ensayos de caída.
5. Simular por separado la caída Ethernet, fallo del CPE y pérdida aguas arriba en una ventana controlada; observar logs y flujos nuevos.
6. Restaurar el enlace, comprobar recuperación y documentar el efecto sobre conexiones existentes y servicios internos.

70.26. Procedimiento 3: validar balanceo sin confundirlo con caudal

1. Crear un grupo con al menos dos gateways en el mismo tier y utilizarlo en una regla de policy routing apta.
2. Confirmar NAT, monitorización y que no exista una regla de mayor prioridad que capture el tráfico antes de la regla Multi-WAN.
3. Desde estaciones de prueba, iniciar múltiples conexiones nuevas hacia destinos externos; evitar decidir por una única pestaña de navegador con sesiones persistentes.
4. Comparar IP pública de salida, estados de firewall y gráficas de las WAN; revisar si el reparto es por conexiones, no por bytes.
5. Comprobar el comportamiento al fallar uno de los miembros y verificar que se retira del conjunto elegible.

70.27. Procedimiento 4: diagnóstico de Pending, pérdida o alarma



Figura 70.4. Secuencia de diagnóstico progresivo antes de modificar gateways o eliminar estados.

1. Comprobar link físico, dirección asignada, DHCP/PPPoE si aplica, y si el gateway tiene IP válida.
2. Verificar la ruta al Monitor IP y hacer pruebas desde la WAN correcta; no utilizar exclusivamente ping desde un equipo LAN.
3. Leer Status → System Logs → System / Gateways buscando Alarm, Clear y errores de dpinger.

4. Comparar el RTT, la pérdida y la disponibilidad de servicios; diferenciar caída real de limitación ICMP.
5. Revisar las reglas de policy routing, NAT y configuración de grupos; no tocar umbrales hasta confirmar línea base.
6. Si se requiere un cambio disruptivo, mantener sesión de consola o gestión fuera de banda y un plan de reversión.

70.28. Matriz de diagnóstico y acciones correctivas

Síntoma	Causa plausible	Comprobación prioritaria
Gateway Online, sin Internet	Monitor solo mide módem/CPE; DNS o ruta errónea.	Monitor externo, Diagnostics → Routes, DNS y pruebas de aplicación.
Warning por pérdida	Congestión, Wi-Fi upstream o ICMP limitado.	dpinger, calidad del enlace y otro objetivo monitor.
Pending indefinido	Interfaz sin IP, monitor no iniciado o gateway no operativo.	Interface Status, rutas, evento de arranque dpinger.
Failover no conmuta	Monitor del módem permanece Online; grupo no usado.	Simular avería real aguas arriba y revisar rules/tiers.
Balanceo no se aprecia	Conexiones persistentes, reglas o NAT incompletas.	Sesiones nuevas y tráfico en cada WAN.
Corte al eliminar states	Se seleccionó acción por IP/default de alcance amplio.	Revisión de estados y plan de continuidad.

70.29. Comandos y herramientas de inspección (lectura)

En Diagnostics → Ping elegir interfaz/source adecuados para probar el objetivo; en Diagnostics → Routes inspeccionar rutas; en Status → Monitoring observar histórico; en Status → System Logs → System / Gateways inspeccionar eventos. Para operadores con consola y autorización técnica, pueden resultar útiles comandos de solo lectura como `netstat -rn`, `route -n get 198.51.100.1` o `pfctl -ss` (la salida puede incluir datos sensibles). Evitar comandos de eliminación o reinicio como primera medida.

70.30. Escenarios empresariales razonados

Escenario	Diseño y objetivo	Validación mínima
Oficina con fibra + 4G	Tier 1 fibra, Tier 2 móvil; objetivo externo por WAN; coste de datos del backup controlado.	Avería del proveedor sin caída de enlace Ethernet; sesión nueva por 4G.
Dos proveedores similares	Balanceo de conexiones en mismo tier para tráfico adecuado y failover conjunto.	Salidas públicas distintas y desactivación de miembro fallido.
Sede con túneles VPN	Rutas y NAT diferenciadas; comprobar endpoints y retorno de túneles cuando cambia WAN.	Reestablecimiento de VPN, DNS y acceso a aplicaciones tras conmutación.

70.31. Riesgos, seguridad y recomendaciones de administración

No almacenar volcados de estados ni registros con direcciones de clientes en repositorios públicos. Limitar la administración de pfSense a personal autorizado; conservar copia de configuración; definir procedimiento de emergencia con consola independiente; evaluar impacto de loss/recovery sobre VPN, telefonía IP y sesiones persistentes; revisar los gráficos con ventana temporal suficiente y documentar modificaciones de umbrales y monitor.

Las alertas aisladas no justifican cambios radicales. En Multi-WAN, las pruebas deben reproducir fallos del enlace físico y del upstream; el estado Online del CPE no equivale a disponibilidad del operador más allá de él. Tampoco debe confundirse el ajuste de Trigger Level de un grupo con la modificación de la monitorización de un gateway.

70.32. Glosario técnico

Concepto	Definición práctica
Gateway	Siguiente salto utilizado por una ruta o política de encaminamiento.
dpinger	Daemon de pfSense que envía sondas ICMP y calcula salud de gateways.
RTT / RTTsd	Tiempo de ida y vuelta / desviación estándar de ese tiempo.
Monitor IP	Destino sobre el que se realiza la medición de salud.
Gateway Group / Tier	Objeto de gateways y nivel de prioridad o balanceo.
Policy routing / reply-to	Selección de salida por regla / retorno por la WAN de entrada.
PF state	Registro de una conexión autorizada que puede conservar la ruta original.

70.33. Referencias oficiales y ampliación de consulta

01. Gateway Status — https://docs.netgate.com/pfsense/en/latest/monitoring/status/gateways.html

02. Gateway Groups — https://docs.netgate.com/pfsense/en/latest/routing/gateway-groups.html

03. Gateway Settings — https://docs.netgate.com/pfsense/en/latest/routing/gateway-configure.html

04. Gateway Logs — https://docs.netgate.com/pfsense/en/latest/monitoring/logs/gateway.html

05. Multi-WAN: Load Balancing and Failover — https://docs.netgate.com/pfsense/en/latest/multiwan/load-balance-and-failover.html

06. Multi-WAN: Verifying Functionality — https://docs.netgate.com/pfsense/en/latest/multiwan/test.html

07. Multi-WAN: Troubleshooting — https://docs.netgate.com/pfsense/en/latest/troubleshooting/multi-wan.html

08. Advanced Miscellaneous: Gateway Monitoring — https://docs.netgate.com/pfsense/en/latest/config/advanced-misc.html

09. Default Gateway Management — https://docs.netgate.com/pfsense/en/latest/routing/gateways.html

10. Policy Routing Configuration — https://docs.netgate.com/pfsense/en/latest/multiwan/policy-route.html

11. Troubleshooting Gateway Monitoring — https://docs.netgate.com/pfsense/en/latest/troubleshooting/gateway-errors.html

12. Troubleshooting Network Connectivity — https://docs.netgate.com/pfsense/en/latest/troubleshooting/connectivity.html

71 Status → Interfaces

Supervisión física y lógica · DHCP y PPP · Contadores PF · VLAN y switch integrado · Diagnóstico y recuperación

Una interfaz puede presentar enlace físico correcto y, sin embargo, carecer de dirección válida, de ruta de salida o de servicio de red. La página Status → Interfaces proporciona la evidencia operativa inicial: estado, direccionamiento, medio, tráfico, descartes y controles de sesiones dinámicas. Debe leerse conjuntamente con los gateways, registros, tablas de rutas y pruebas activas.

IDEA CENTRAL La pantalla es de supervisión, pero algunos controles —Release, Renew, Disconnect o Connect— ejecutan acciones operativas sobre conexiones reales. Deben tratarse como cambios potencialmente disruptivos.



Figura 71.1. Cuatro niveles de diagnóstico para diferenciar enlace, concesión, encaminamiento y servicio.

71.1. Ruta de acceso, alcance y relación con otras vistas

Ruta exacta: Status → Interfaces. Se muestran las interfaces asignadas, con un bloque por interfaz y los campos pertinentes al tipo configurado. La pantalla no es el formulario de configuración: Interfaces → [nombre] modifica el comportamiento; Status → Gateways supervisa alcance y latencia de puertas de enlace; Diagnostics → Routes y Packet Capture permiten verificar caminos y paquetes.

Vista	Uso técnico	Riesgo de confusión
Status → Interfaces	Estado local, direcciones, medio, errores y contadores.	UP no garantiza Internet.
Interfaces → [interfaz]	Configuración de IPv4/IPv6, MTU, gateway y comportamiento.	Cambios pueden causar pérdida de gestión.
Status → Gateways	Sondas a gateway o monitor, pérdidas y latencias.	Monitor Online no valida todas las aplicaciones.
Diagnostics → Routes	Tabla de encaminamiento activa.	La mera existencia de ruta no prueba llegada.
Diagnostics → Packet Capture	Captura del tráfico real en interfaz seleccionada.	El punto de observación importa por NAT y VLAN.

71.2. Organización de bloques, cabecera y nombres de interfaz

Cada sección comienza con el nombre descriptivo (por ejemplo, WAN, LAN o un enlace auxiliar), seguido del identificador interno y del dispositivo asociado cuando procede. En hardware con switch integrado también puede aparecer la asociación de puertos del switch. El nombre de sistema operativo identifica un recurso real a la hora de utilizar ifconfig o tcpdump; el nombre amistoso facilita la lectura humana y puede modificarse.

Elemento	Significado	Consecuencia administrativa
Nombre amigable	Etiqueta asignada a la interfaz.	Puede cambiar sin alterar necesariamente la NIC subyacente.
Identificador interno	wan, lan, opt1 y otros identificadores de configuración.	Sirve para correlacionar la configuración lógica.

Elemento	Significado	Consecuencia administrativa
Dispositivo del sistema	NIC, VLAN, túnel o interfaz virtual asignada.	Se necesita al consultar ifconfig y capturas CLI.
switchports	Asociación con puerto(s) de switch integrado si está disponible.	Un VLAN UP puede no representar el estado de su cable físico.

71.3. Estados Up, Down, No Carrier, Disabled y Associated

Estado mostrado	Lectura correcta	Siguiente comprobación
Up	Interfaz activa y enlace reconocido.	Dirección, gateway, DNS y prueba de aplicación.
Down	Conexión dinámica inactiva o sin IP en ese momento.	Capa física, negociación y registros DHCP/PPP.
No Carrier	Ausencia de portadora/enlace reconocido.	Cable, óptica, CPE, switch y puerto.
Disabled	Interfaz asignada, deshabilitada por configuración.	Verificar motivo y alcance de activación.
Associated	Enlace inalámbrico asociado al punto de acceso.	RSSI, autenticación y tráfico efectivo.

En las conexiones dinámicas pueden verse indicadores diferentes para Status y DHCP/PPP: uno refleja el enlace y otro la sesión o negociación. No deben fusionarse en un único concepto. Una interfaz física puede recuperar carrier sin que la conexión DHCP obtenga un arrendamiento; también puede conservar información DHCP mientras el enlace subyacente está caído.

71.4. Controles de cabecera e iconografía

Los iconos de la zona superior de la interfaz gráfica pueden ofrecer acceso a ajustes del tema, representaciones de datos, listas y ayuda contextual según la versión. Deben identificarse por su tooltip en el equipo concreto; no se deduce de su icono que reinicien la red. La pantalla mostrada no presenta un botón general de habilitación o guardado; las operaciones efectivas son los controles de conexión asociados a interfaces dinámicas.

71.5. Acción DHCP Release: efecto y riesgos

Cuando una interfaz obtiene su dirección mediante DHCP y mantiene una concesión activa, pfSense puede mostrar el botón Release. Netgate documenta que, sin la opción adicional Relinquish Lease, se abandona el estado operativo local de la concesión; no debe afirmarse que se envía siempre una liberación explícita al servidor. Tras la liberación puede presentarse Renew para solicitar de nuevo una dirección. Cualquiera de estas acciones puede modificar IP, gateway, DNS o rutas y cortar sesiones VPN o de administración.

71.6. Casilla Relinquish Lease: significado exacto

La casilla Relinquish Lease acompaña a Release. Al activarla, el cliente solicita abandonar expresamente su concesión mediante un mensaje especial dirigido al servidor DHCP. Esto facilita que el servidor deje de reservar la dirección anterior según su implementación y política. No obliga a que el servidor entregue una IP diferente después: el resultado depende del pool y de la identidad del cliente.

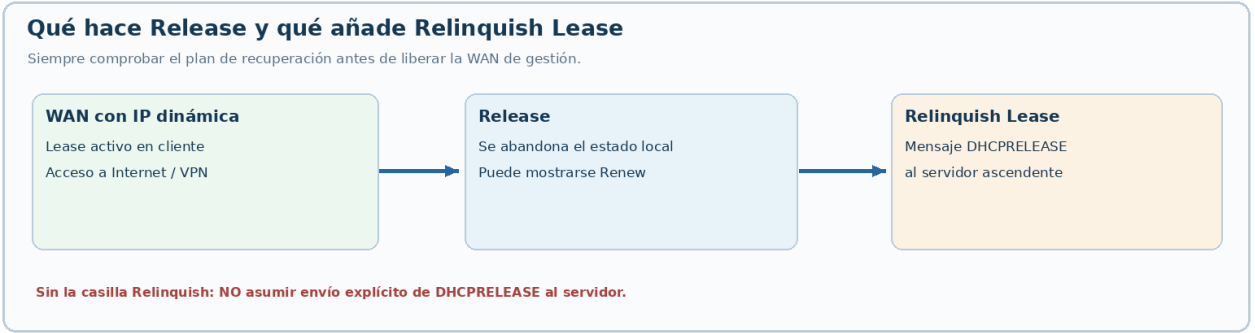


Figura 71.2. Release frente a la liberación explícita de concesión mediante Relinquish Lease.

ADVERTENCIA CRÍTICA No utilizar Release en la WAN que sostiene una sesión remota de gestión sin consola local, enlace alternativo probado y procedimiento de recuperación. Puede perderse la puerta de enlace predeterminada y desconectarse la VPN.

71.7. Acción Renew, DHCPv6 y diferencias entre familias

Cuando no existe lease activo, el control puede mostrar Renew. Solicita iniciar o reintentar el proceso de obtención de la configuración, pero no garantiza respuesta del servidor. En DHCPv6 existen controles análogos cuando el tipo de interfaz utiliza DHCP6; los parámetros resultantes pueden incluir dirección IPv6, prefijo delegado y otros datos dependiendo del modo de configuración. El botón para IPv4 no equivale a renovar DHCPv6 en todas las versiones o configuraciones.

71.8. Acciones PPPoE y otras conexiones punto a punto

Las interfaces que utilizan PPPoE y otros mecanismos PPP pueden presentar Disconnect cuando la sesión está establecida y Connect cuando no lo está. Las operaciones interactúan con la sesión del proveedor; no cambian por sí mismas la configuración persistente del usuario. Si está habilitado dial-on-demand, el tráfico de salida puede reconectar la sesión tras una desconexión manual. La página muestra, cuando aplica, el tiempo activo de la sesión PPP.

71.9. Aviso Dial-on-demand y sus implicaciones

Una advertencia relacionada con dial-on-demand indica que la desconexión manual puede resultar transitoria si paquetes posteriores activan automáticamente la llamada o sesión. Esto afecta a líneas de respaldo de pago por uso y a pruebas de aislamiento: para mantener el enlace efectivamente inactivo hay que cambiar su modo de operación de forma controlada, no confiar solo en Disconnect. La presencia de un aviso no demuestra que el circuito tenga actualmente una sesión PPP en producción.

71.10. Dirección MAC y particularidades de la identificación física

MAC Address identifica la dirección de capa 2 comunicada por la interfaz. No es una dirección IP ni una identidad criptográfica: puede ser cambiada por configuración o por drivers. En interfaces VLAN se hereda con frecuencia del dispositivo padre. Netgate describe que determinados paquetes pueden añadir información del fabricante OUI, cuando está disponible; no debe considerarse una prueba de identidad del dispositivo.

71.11. Dirección IPv4, máscara y gateway

Campo	Interpretación	Consejo de diagnóstico
IPv4 Address	Dirección actualmente asignada a la interfaz.	Comprobar si procede de DHCP o estática.
Subnet mask IPv4	Máscara de red para la IP anterior.	Validar compatibilidad con la red del siguiente salto.
Gateway IPv4	Puerta de enlace asociada, si procede.	Contrastar con rutas y monitorización.
DNS Servers	Servidores entregados por WAN, si los hay.	No asumir que son los DNS de los clientes LAN.

Status → Interfaces no enumera necesariamente direcciones virtuales CARP, IP Alias o todas las VIP de una interfaz. Estas se gestionan y comprueban desde Firewall → Virtual IPs y las vistas correspondientes. Una dirección privada en WAN no equivale a un fallo: puede ser correcta detrás de un router upstream o en redes con CGNAT, pero exige considerar NAT, rutas y VPN.

71.12. IPv6 Link-Local, Scope ID y prefijos

IPv6 Link Local usa normalmente fe80::/10 y sirve para comunicación dentro del enlace. El sufijo de alcance con el nombre de interfaz (scope/zone ID) desambigua interfaces que pueden tener direcciones link-local similares; no representa una dirección pública. La pantalla puede incluir dirección IPv6 global, longitud de prefijo, gateway IPv6 y DNS, de acuerdo con el método empleado: Static IPv6, DHCP6, SLAAC, Track Interface u otro mecanismo compatible.

71.13. MTU: máximo tamaño de paquete

MTU informa del tamaño máximo de unidad de transmisión configurado para la interfaz. En Ethernet sin encapsulación es frecuente observar 1500 bytes, pero VLAN, PPPoE, túneles VPN y proveedores pueden requerir valores diferentes. Ajustar MTU a ciegas puede causar pérdida de conectividad, problemas de PMTUD, fragmentación o aplicaciones que parecen funcionar parcialmente. La pantalla de Status muestra el valor vigente, no el resultado de una prueba completa de Path MTU.

71.14. Media, velocidad y negociación dúplex

El campo Media representa el tipo de enlace y su negociación; una descripción de 1000baseT full-duplex expresa el medio y régimen configurado/negociado, no que se estén transfiriendo continuamente 1 Gb/s. Si una conexión queda en half-duplex o a velocidad inferior a la prevista, revisar el equipo adyacente, la configuración automática, el cableado y las interfaces del switch. La documentación oficial relaciona un desacuerdo dúplex con pérdidas, colisiones y menor caudal.

71.15. Puertos y VLAN de dispositivos con switch integrado

En ciertas plataformas Netgate, varios conectores físicos comparten un switch integrado que conecta por una interfaz interna con el sistema operativo. Para presentar WAN, LAN y OPT como interfaces independientes pueden utilizarse VLAN internas. La relación entre interfaz lógica y puerto físico no es idéntica al cableado de una NIC independiente; la información de los puertos y el parámetro Switch Port permiten interpretar correctamente el link state, según plataforma.

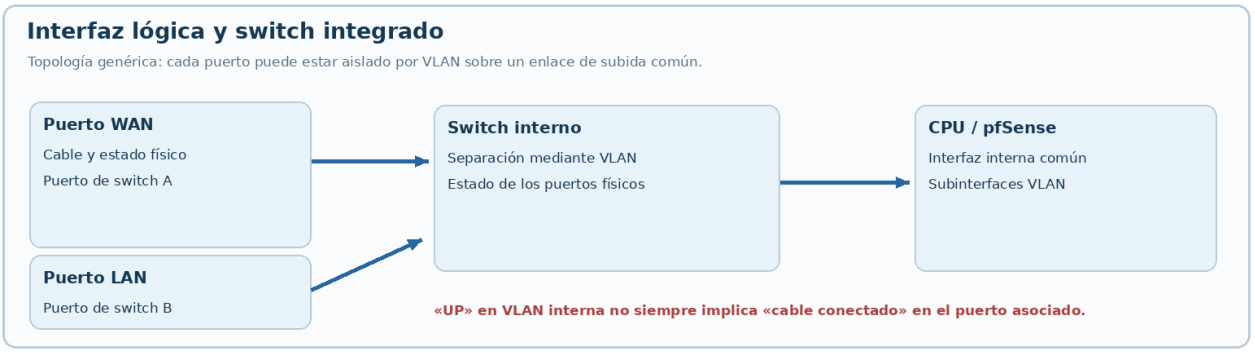


Figura 71.3. Ejemplo conceptual de puertos de switch y subinterfaces VLAN sobre una conexión interna compartida.

PREVENCIÓN Modificar VLAN, asociación de puertos o trunks del switch integrado durante una conexión administrativa remota puede provocar un corte inmediato. Cambiar el puerto utilizado para la GUI solo con acceso alternativo probado.

71.16. In/Out packets: contadores y direcciones

In/Out packets informa de paquetes recibidos y transmitidos por la interfaz, junto con volumen expresado normalmente en unidades como MiB o GiB. La dirección “in” es la vista desde el firewall: lo que entra en la interfaz; “out” representa lo que sale por ella. Los contadores suelen ser acumulativos desde inicialización, reset o cambio de interfaz. Deben compararse en intervalos de tiempo para detectar una tasa real y no inferir caudal instantáneo a partir de su valor absoluto.

71.17. In/Out packets (pass): tráfico admitido por PF

El contador Pass recoge paquetes que el filtrado PF ha dejado pasar sobre la interfaz. Este conteo es de una capa de observación diferente a los contadores físicos; no es seguro asumir que su suma con Block equivale exactamente al total de tramas Ethernet. Para atribuir un flujo a una regla concreta, revisar registros y Diagnostics → States. Un número alto de Pass no demuestra por sí mismo que la aplicación haya recibido la respuesta correcta.

71.18. In/Out packets (block): descartes por el filtro

Block recoge paquetes bloqueados por PF en esa interfaz. Que aumente no significa que la NIC tenga errores ni que exista un ataque: es normal descartar ruido de Internet, sondas y tráfico no permitido. Lo relevante es identificar origen, destino, protocolo y regla de bloqueo, correlacionándolo con System Logs →

Firewall. Un cambio de contadores tras ajustar reglas no implica que se borren los estados de sesiones existentes.

71.19. In/Out errors: errores de recepción y transmisión

Los contadores de errores muestran fallos de entrada y salida: pueden deberse a problemas de cableado, óptica, driver, cola o alta carga. Pocos errores esporádicos no demuestran una incidencia; un incremento sostenido, combinado con pérdida de paquetes, degradación o logs del sistema, debe investigarse. Netgate documenta que determinados controladores permiten estadísticas detalladas mediante sysctl.

71.20. Collisions y diagnóstico de dúplex

Collisions refleja colisiones de capa Ethernet. En enlaces modernos full-duplex con switches se espera habitualmente cero. Si aparecen colisiones o se observa half-duplex inesperado, comprobar negociación en ambos extremos y eventuales equipos antiguos. No forzar velocidad/dúplex sin verificar cómo está configurado el dispositivo opuesto: un ajuste unilateral puede empeorar la comunicación.

71.21. Métricas condicionales: SFP, LAGG, bridge e interfaces inalámbricas

Tipo / condición	Campos adicionales documentados	Valor de diagnóstico
SFP/SFP+ con datos expuestos	Fabricante, temperatura, voltaje y potencia óptica.	Detectar degradación de transceptor y enlace.
LAGG	Protocolo, hashing y puertos miembros.	Verificar LACP, failover y distribución.
Bridge	Pertenencia y estado del puente.	Comprobar capa 2 y puertos participantes.
Wi-Fi compatible	Canal, SSID/BSSID, velocidad y RSSI.	Calidad de asociación y enlace.
PPP celular compatible	RSSI, SIM, modo y velocidades.	Evaluar disponibilidad del enlace móvil.
NIC que lo soporte	Interrupciones acumuladas.	Contrastar carga de NIC, CPU y tasas.

71.22. Diferencias entre “Up”, tráfico y alcance real del gateway

Cuando el enlace está UP y la negociación DHCP también aparece UP pueden fallar rutas, DNS, resolución ARP del gateway o conectividad fuera del CPE. En líneas redundantes es imprescindible correlacionar Status → Interfaces con Status → Gateways: este último determina el estado de las sondas a un monitor y puede estar Pending, Warning o Offline aunque exista carrier. Los paquetes pasan por una secuencia de capas y cualquiera de ellas puede ser la causa del fallo.

71.23. Herramientas de consulta recomendadas

Herramienta	Ruta o comando orientativo	Qué confirma
Estado de interfaz	Status → Interfaces	Dirección, link, counters y opciones dinámicas.
Estado de gateway	Status → Gateways	RTT, pérdida y monitor asociado.
Tabla de rutas	Diagnostics → Routes; netstat -rn	Gateway por defecto, rutas y métricas.
Consulta de interfaz	ifconfig [interfaz]	Carrier, flags, VLAN, MTU y estadísticas.
Eventos	Status → System Logs	DHCP, PPP, driver, interfaces y gateway.
Captura	Diagnostics → Packet Capture	DHCP, ICMP, ARP, TCP y comportamiento real.

Herramienta	Ruta o comando orientativo	Qué confirma
Pruebas	Diagnostics → Ping / DNS Lookup	Conectividad por interfaz y DNS.

71.24. Procedimiento 1: auditoría de interfaces sin interrumpir el tráfico

01 Identificar cada bloque de Status → Interfaces y registrar únicamente los nombres lógicos y métricas necesarias, sin divulgar IP reales, MAC ni inventario de hardware.

02 Anotar la relación entre el estado físico, el estado de concesión dinámica y el campo Media.

03 Comprobar MTU, direcciones IPv4/IPv6 y gateways, separando link-local IPv6 de dirección global.

04 Tomar dos lecturas espaciadas de errores, bloqueos y tráfico para observar tendencias; no confundir acumulados con tasas.

05 Correlacionar los resultados con Gateways, rutas y registros; documentar la conclusión y la evidencia antes de cambiar configuraciones.

71.25. Procedimiento 2: investigar una WAN DHCP sin IP válida

01 Comprobar en Status → Interfaces si hay portadora y el estado específico de DHCP; verificar cable, CPE y puerto antes de intervenir en el cliente DHCP.

02 Inspeccionar los logs DHCP y del sistema; confirmar si se observan solicitudes, ofertas y mensajes de error.

03 Usar Packet Capture desde la interfaz correcta y aplicar un filtro DHCP compatible cuando sea necesario.

04 Verificar VLAN, switch integrado y upstream; comprobar si la dirección corresponde al segmento esperado.

05 Si la interfaz tiene acceso de gestión remoto, confirmar acceso alternativo y ventana de cambio antes de Renew o Release.

06 Validar IP, gateway, DNS, rutas, conectividad y VPN tras restablecer el enlace; guardar observaciones.

71.26. Procedimiento 3: renovar una conexión con control de riesgo

01 Confirmar qué WAN y gateway sostienen la sesión de administración y los servicios críticos; elaborar un plan de retorno.

02 Verificar si existe una concesión activa y determinar el motivo técnico para renovarla o liberarla.

03 Registrar estado anterior, lease, rutas y eventos, sin exportar credenciales o identificadores a informes abiertos.

04 Aplicar la acción necesaria en ventana de mantenimiento y solo cuando exista canal alternativo probado.

05 Comprobar si cambió la IP, gateway, DNS o la ruta; repetir pruebas de conectividad y salud del enlace.

06 Si falla la recuperación, utilizar consola o enlace fuera de banda y restaurar la configuración y los servicios según el plan.

71.27. Procedimiento 4: enlace de backup móvil que no levanta

01 Determinar si el enlace está administrativamente apagado, sin carrier, sin DHCP o sin gateway operativo.

02 Verificar alimentación del módem/router, interfaz del switch, APN o sesión del equipo de acceso si aplica y límites del plan móvil.

03 Si hay dial-on-demand, confirmar si el aviso aplica realmente a la conexión y qué eventos provocan su reactivación.

04 Revisar gateway y grupos de failover; una interfaz de respaldo puede estar UP sin participar en las reglas ni rutas deseadas.

05 Hacer una prueba controlada de salida por el backup y comprobar las rutas de vuelta, NAT y el coste de datos.

06 Restaurar el comportamiento esperado, documentar limitaciones y preservar el enlace principal.

71.28. Procedimiento 5: errores o colisiones que aumentan

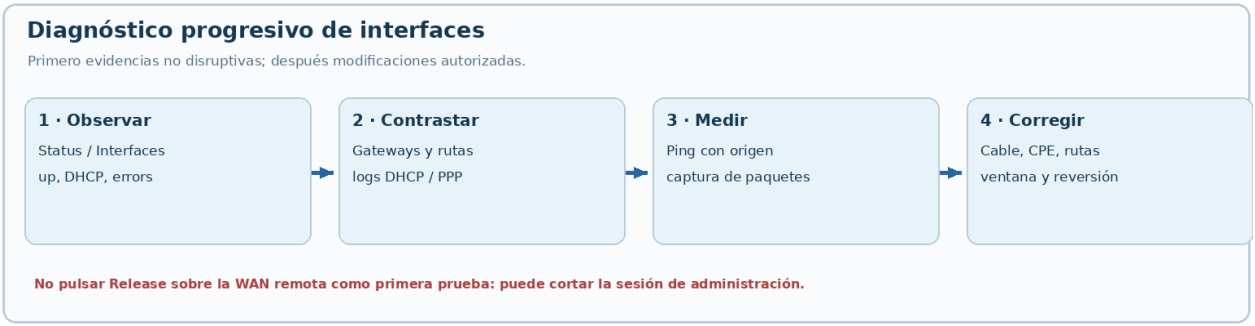


Figura 71.4. Secuencia de resolución de incidencias con prioridad a comprobaciones no disruptivas.

01 Registrar una lectura inicial de errores y colisiones y observar su crecimiento durante un intervalo definido.

02 Comprobar Media, dúplex, velocidad, switch, puerto, cableado, SFP y registros de driver.

03 Comparar con pruebas reales de caudal, pérdida y utilización; diferenciar ruido normal de degradación persistente.

04 Si se sospecha offloading o driver, revisar la guía Netgate para el hardware y planificar cambios controlados.

05 Verificar el resultado con contadores nuevos, gráficos y tráfico de aplicación después de cada intervención.

71.29. Matriz de incidencias y resolución

Síntoma	Causa probable	Primera evidencia útil
WAN Up, sin Internet	Gateway, DNS, ruta o upstream.	Status → Gateways; ping con origen WAN.
DHCP Up, Status Down	Sesión/concesión y portadora desacopladas.	Media, switchports y logs DHCP.
Sin DHCP tras Renew	Servidor, VLAN, relay o filtro upstream.	Captura DHCP y estado CPE.
Link 100 Mb/s inesperado	Cable/pares, puerto o negociación.	Media y contadores de errores.
Collisions crecientes	Desajuste dúplex o equipo legado.	Configuración de ambos extremos.
Block crece, NIC sin errores	Reglas PF rechazan tráfico.	Firewall log y States.
VPN cae al Release	Cambio IP/gateway o pérdida de ruta.	Logs de VPN, WAN y gateway.
Backup no conmuta	Grupo/rules/monitor/NAT no operativos.	Gateways, Rules y NAT.

71.30. Escenarios empresariales didácticos

Escenario	Diseño de la supervisión	Criterio de aceptación
Sede con fibra y respaldo 4G	Comparar estados físicos, DHCP, monitor externo y plan de consumo móvil.	La conmutación se valida con tráfico real.
Firewall con switch integrado	Correlacionar VLAN lógica, puertos físicos y enlace CPU–switch.	Sin bloqueo de gestión al cambiar VLAN.
Enlaces a redes industriales	Registrar errores, colisiones y microcortes; separar tráfico PF bloqueado.	Tendencia estable y latencia compatible.

Escenario	Diseño de la supervisión	Criterio de aceptación
Servidor VPN multi-sede	Correlacionar cambios IP WAN con sesiones VPN y rutas.	Los clientes recuperan DNS y acceso.

71.31. Seguridad, privacidad y cambios en producción

Las capturas operativas de Interfaces pueden exponer direcciones IP, MAC, modelos de hardware, nombres de sedes, topología y otros identificadores sensibles. Los informes compartidos deben sustituirlos por datos de laboratorio. Nunca ejecutar Release/Relinquish, un cambio de VLAN, MTU o velocidad como intento indiscriminado de recuperación. Mantener copia de la configuración, acceso fuera de banda probado y un registro de cambios que describa afectación prevista y marcha atrás.

71.32. Glosario esencial

Término	Definición práctica
Carrier / portadora	Indicación de enlace físico disponible en el medio.
Lease DHCP	Concesión temporal de parámetros de red al cliente.
Relinquish Lease	Liberación explícita de la concesión al servidor DHCP.
MTU / PMTUD	Límite de transmisión por interfaz / descubrimiento de MTU del camino.
Duplex	Capacidad de transmitir y recibir simultáneamente (full) o no (half).
VLAN 802.1Q	Identificación lógica de red mediante etiquetado en capa 2.
PF pass / block	Contadores de paquetes permitidos / bloqueados por el cortafuegos.
Link-local IPv6	Dirección IPv6 válida para el enlace, con alcance de interfaz.
LAGG / LACP	Agregación de enlaces y protocolo de negociación cuando aplica.

71.33. Lista final de verificación

01 La interfaz correcta está identificada por nombre lógico y dispositivo asignado.

02 Se han distinguido portadora, negociación de DHCP/PPP, gateway y conectividad final.

03 Las direcciones IPv4/IPv6, máscaras, gateway y MTU son consistentes con el diseño autorizado.

04 No se confunden errores físicos con paquetes bloqueados por PF.

05 Se han contrastado los contadores de tráfico en el tiempo y revisado Media y duplex.

06 Se conoce el efecto de Release, Relinquish Lease, Renew y dial-on-demand, cuando estén presentes.

07 Los cambios con riesgo de desconexión disponen de ventana, consola alternativa y reversión.

08 Se han documentado las pruebas y no se ha filtrado información identificativa.

71.34. Referencias oficiales verificables

01. Interface Status — https://docs.netgate.com/pfsense/en/latest/monitoring/status/interfaces.html

02. Status Menu Guide — https://docs.netgate.com/pfsense/en/latest/menuguide/status.html

03. Interface Configuration — https://docs.netgate.com/pfsense/en/latest/interfaces/configure.html

04. Interface Types and Configuration — https://docs.netgate.com/pfsense/en/latest/interfaces/index.html

05. WAN vs LAN Interfaces — https://docs.netgate.com/pfsense/en/latest/interfaces/wanvslan.html

06. Integrated Switch Overview — https://docs.netgate.com/pfsense/en/latest/solutions/sg-1100/switch-overview.html

07. Troubleshooting Low Interface Throughput — https://docs.netgate.com/pfsense/en/latest/troubleshooting/low-throughput.html

08. Troubleshooting Lost Traffic — https://docs.netgate.com/pfsense/en/latest/troubleshooting/packet-loss.html

09. Selecting the Proper Capture Interface — https://docs.netgate.com/pfsense/en/latest/diagnostics/packetcapture/interface.html
10. Interface Configuration (Overview) — https://docs.netgate.com/pfsense/en/latest/config/interface-configuration.html
11. Dashboard Widgets — https://docs.netgate.com/pfsense/en/latest/monitoring/dashboard-widgets.html
12. Viewing Firewall States — https://docs.netgate.com/pfsense/en/latest/monitoring/status/firewall-states-gui.html
13. VLANs — https://docs.netgate.com/pfsense/en/latest/vlan/index.html
14. Gateway Status — https://docs.netgate.com/pfsense/en/latest/monitoring/status/gateways.html

72 Status → IPsec

Overview · Leases · SADs · SPDs · IKE y CHILD SA · Supervisión operativa y diagnóstico

IPsec no debe considerarse operativo únicamente porque una fase de negociación figure establecida. Su estado depende de la negociación de asociaciones, de las políticas de selección, del filtrado y de la posibilidad real de transportar y devolver paquetes.

IDEA CENTRAL Una política SPD puede permanecer presente aun sin conexión IPsec activa; comprobarla es esencial si otra VPN o una ruta alternativa deja de transportar tráfico.



Figura 72.1. Relación entre negociación IKE, CHILD SA y bases del núcleo para interpretar el estado de IPsec.

72.1. Ruta de acceso y objetivo de la pantalla

Ruta exacta: Status → IPsec. Esta pantalla permite observar la situación de los túneles configurados, las asignaciones a clientes móviles y las bases de asociaciones y políticas de IPsec. Es una herramienta de supervisión y diagnóstico; no reemplaza la configuración situada en VPN → IPsec ni los registros de Status → System Logs.

Pestaña	Pregunta operativa	Objeto principal
Overview	¿Hay IKE/CHILD SA y cuál es su estado?	Túneles y asociaciones negociadas
Leases	¿Qué direcciones recibieron los clientes móviles?	Pools y concesiones móviles
SADs	¿Qué asociaciones existen en ejecución?	Security Association Database
SPDs	¿Qué tráfico queda seleccionado para IPsec?	Security Policy Database

72.2. Estado mostrado: «IPsec is disabled.»

Cuando IPsec no está operativo, Overview puede presentar el mensaje «IPsec is disabled.» junto al enlace «Configure IPsec.» y una tabla sin entradas. Debe leerse como ausencia de servicio IPsec disponible en ese contexto, no como prueba de daño en el cortafuegos. Puede deberse a la ausencia de túneles habilitados o a que el servicio no esté funcionando; la causa concreta se determina en VPN → IPsec y Status → Services.

ADVERTENCIA No activar IPsec ni modificar reglas desde una sesión remota de gestión sin revisar el diseño del servicio, los selectores y un plan de reversión. Mientras aparece ese aviso, no hay evidencia de túneles activos en la vista.

72.3. Pestañas, encabezado y controles visibles

Elemento visible	Función / interpretación	Precaución
Overview	Vista inicial de túneles habilitados.	Una lista vacía no equivale a pérdida física de WAN.
Leases	Consulta del uso de pools móviles.	No confundir concesiones con sesiones conectadas.
SADs	Vista de asociaciones de seguridad.	La disponibilidad de acciones depende de versión/estado.
SPDs	Vista de políticas de seguridad.	Las políticas pueden existir sin IKE negociada.
Iconos superiores	Controles generales de la interfaz gráfica y acceso a ayuda; sus funciones exactas dependen del tema/versión.	No atribuir una acción de gestión de VPN a iconos sin comprobar tooltip.
Configure IPsec.	Enlace hacia el área de configuración IPsec.	Cambios en producción requieren ventana controlada.

72.4. Cabecera de Overview: descripción de todas las columnas

Campo visible	Explicación técnica	Diagnóstico
ID	Identificador del elemento de túnel visible en el resumen.	Correlacionar con la entrada de configuración y registros.
Description	Texto descriptivo administrativo de la conexión.	Usar nombres neutros que identifiquen función, no secretos.
Local	Extremo local de la asociación; suele representar dirección exterior IKE.	Verificar origen WAN y NAT si hay Multi-WAN.
Remote	Extremo remoto observado o configurado.	Comprobar dirección/DDNS y cambio de ISP.
Role	Rol en la negociación, típicamente iniciador o respondedor cuando se informa.	Diferenciar quién inició el intercambio; no indica prioridad de WAN.
Timers	Temporizadores de mantenimiento, vida o renovación según asociación.	Rekey/reautenticación no implican necesariamente caída.
Algo	Transformaciones criptográficas negociadas.	Confirmar que coinciden con propuestas aceptadas.
Status	Estado actual de conexión/negociación.	Una fase IKE establecida no certifica tráfico útil.

72.5. Listado de túneles, prioridad visual y Child SA desplegables

Según Netgate, Overview lista primero las conexiones establecidas y después las desconectadas. En la presentación compacta se muestra inicialmente la parte IKE de la conexión; el control para ampliar CHILD SA permite ver la parte correspondiente a la fase 2. Los botones de conexión o desconexión manual se muestran en las filas pertinentes cuando el servicio y los túneles están configurados.

La CHILD SA protege el tráfico de datos. La fase IKE negocia autenticación y parámetros de control, pero el tráfico de usuario requiere una CHILD SA apropiada, selectores correctos, paso por las reglas de firewall y una ruta de regreso en los equipos de destino.



Figura 72.2. Lectura progresiva: servicio, IKE, CHILD SA y verificación de tráfico real.

72.6. Acciones Connect, Disconnect y expansión: impacto

Acción documentada	Qué consigue	Riesgo
Expandir CHILD SA	Muestra los detalles de fase 2 sin negociar ni cortar tráfico por sí misma.	No implica activar una fase 2.
Connect / iniciar	Solicita iniciar la conexión o asociación cuando el control aparece.	Puede producir negociación y cambios de estado; evitar pruebas indiscriminadas.
Disconnect / finalizar	Termina la asociación elegida.	Interrupción inmediata de sesiones y aplicaciones dependientes.
Enlace a configuración	Abre el túnel para inspección y edición.	Guardar cambios puede desencadenar reconexiones.

CONTROL DE CAMBIOS No debe confundirse la acción Disconnect con deshabilitar permanentemente una Phase 1 en VPN → IPsec. La reconexión dependerá de la política de inicio/reinicio, DPD, tráfico de activación y configuración del peer.

72.7. IKE SA y CHILD SA: relación entre fases 1 y 2

En el lenguaje operativo de pfSense, Phase 1 corresponde al establecimiento del canal IKE y Phase 2 a las asociaciones de seguridad para datos. En IKEv2 se denominan IKE SA y CHILD SA. En las pantallas, los datos de cada una pueden estar agrupados o desplegables; no asumir que una IKE SA establecida significa que todos los selectores o subredes funcionan.

Evidencia observada	Conclusión permitida	Comprobación faltante
IKE no establecida	No se ha completado negociación de control.	Peer, credenciales, UDP 500/4500, propuestas y logs.
IKE establecida; CHILD ausente	La autenticación IKE puede ser correcta.	Selectores, propuestas ESP/PFS, inicio CHILD.
IKE + CHILD establecidas	Se han negociado SAs.	Reglas IPsec/enc0, rutas y respuesta extremo a extremo.
Contadores TX crecen y RX no	Sale tráfico por la SA pero no retorna al mismo nivel.	Firewall remoto, rutas, NAT, asimetrías y captura.
Rekey repetitivo	Hay renegociaciones frecuentes.	Lifetimes, conectividad, DPD y registros de ambos peers.

72.8. Identificadores, nombres de conexión y correlación con registros

En strongSwan, los nombres internos de conexiones no móviles suelen tomar la forma conX, donde X corresponde al identificador IKE de Phase 1. Las definiciones CHILD pueden figurar como conX o conX_Y, según versión de IKE y la opción Split Connections. No utilizar un nombre supuesto en comandos de terminación: comprobarlo antes mediante swanctl --list-conns y la configuración mostrada en la GUI.

72.9. Leases: función real de las concesiones móviles

La pestaña Leases resume el consumo de los pools de direcciones de clientes móviles IPsec y presenta clientes presentes o conectados recientemente junto con la dirección que les fue asignada. Esta vista se refiere a concesiones de clientes móviles, no a DHCPv4/DHCPv6 general ni a rutas del sistema. Una dirección aún registrada no garantiza una sesión IKE activa.

72.10. Cómo interpretar y auditar un pool de clientes móviles

Dato / situación	Interpretación	Acción recomendada
Pool sin uso	No hay clientes móviles registrados en la vista.	Corroborar si Mobile Clients está habilitado.
Dirección asignada	Registro de asignación de un cliente.	Comparar con Overview y RADIUS/logs.
Pool con poca capacidad	Riesgo de no poder dar nuevas direcciones.	Revisar alcance y grupos/pools en VPN → IPsec.
Cliente reciente, no activo	Concesión conservada tras una sesión previa.	No considerar activo sin asociación ni prueba adicional.
Dirección duplicada o conflicto	Posible solapamiento con otra subred o pool.	Revisar diseños, rutas y clientes actuales.

72.11. Relación con RADIUS, autenticación y desconexiones

Una sesión móvil puede emplear EAP, Xauth o RADIUS según el diseño, y un servidor RADIUS puede participar en asignación de direcciones o contabilización. La pestaña Leases es un indicador de direcciones; la evidencia de autenticación y accounting debe contrastarse en los registros correspondientes. Evitar borrar o modificar pools para “corregir” un fallo de autenticación sin verificar su causa.

72.12. SADs: asociaciones de seguridad activas

La documentación oficial describe SAD como un registro de asociaciones negociadas y señala entradas direccionales entre direcciones externas de los peers. En sentido técnico, la SAD del núcleo contiene asociaciones de procesamiento IPsec (por ejemplo ESP); la negociación IKE que les da origen se mantiene en strongSwan. En la práctica, correlacionar SAD con Overview y los mensajes IKE/CHILD evita confundir ambos niveles.

72.13. SPI, dirección y vida útil: lectura conceptual de una SA

Las asociaciones de IPsec son unidireccionales: una dirección necesita su SA de entrada y la otra su SA de salida. Entre los atributos relevantes están los extremos, el protocolo (habitualmente ESP), el identificador SPI, algoritmos, contadores y tiempo de vida, según lo que presente la implementación y la versión. Los campos y las acciones disponibles en SADs pueden variar según la versión: verificar sus etiquetas antes de operar.

Concepto SAD	Qué significa	Consecuencia práctica
SA entrante	Parámetros con los que se reciben/descifran paquetes.	RX no crece: examinar llegada de ESP/NAT-T.
SA saliente	Parámetros para encapsular y enviar tráfico.	TX crece: la salida no prueba recepción remota.

Concepto SAD	Qué significa	Consecuencia práctica
SPI	Identificador de una SA dentro del protocolo/destino.	Útil para correlacionar mensajes y capturas.
Rekey	Renegociación y sustitución de SAs.	Puede generar asociaciones solapadas transitoriamente.
Ausencia de SA	No hay SA negociada que cubra ese tráfico en ese momento.	Comprobar IKE, CHILD, políticas y logs.

72.14. SPDs: políticas de tráfico seleccionado

La Security Policy Database mantiene políticas de protección/selección de tráfico. En IPsec policy-based los selectores de redes locales y remotas se traducen en políticas que interceptan paquetes para su tratamiento IPsec. Según Netgate, se registran entradas por dirección aun si la conexión no está establecida. Esto explica por qué tráfico de una red puede quedar capturado por IPsec aunque no exista una SA activa.

72.15. Selección local-remota y precedencia frente a rutas

En túneles policy-based no se necesita una ruta estática tradicional para cada red remota: la SPD decide qué paquetes coinciden y deben entrar en IPsec. En IPsec VTI, en cambio, intervienen la interfaz de túnel, el enrutamiento y sus gateways. La diferencia es fundamental al inspeccionar tablas de rutas o investigar tráfico que desaparece.

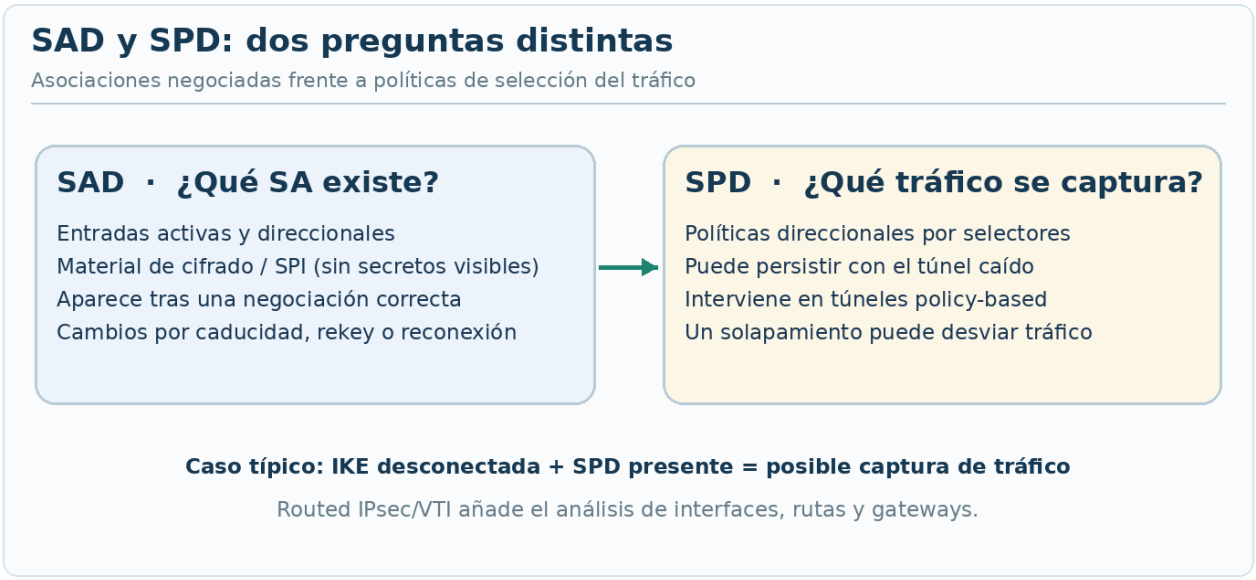


Figura 72.3. Una política SPD puede existir sin SA negociada; no equivale a túnel establecido.

72.16. Políticas residuales y solapamiento con otras VPN

Si un antiguo túnel IPsec policy-based utilizaba los mismos selectores que una VPN alternativa, una entrada SPD residual podría continuar capturando paquetes. Consultar SPDs en Status → IPsec antes de modificar rutas de OpenVPN o WireGuard. Netgate documenta que, tras retirar o deshabilitar la configuración responsable, puede ser necesario detener y reiniciar el servicio IPsec para limpiar políticas residuales; esta acción interrumpe otros túneles IPsec del equipo y exige plan de mantenimiento.

RIESGO OPERATIVO No ejecutar la parada del demonio IPsec como primer paso: revisar qué asociaciones y aplicaciones dependen de él. La limpieza de una política conflictiva debe realizarse en ventana controlada y tras respaldar la configuración.

72.17. Diferencias operativas entre SAD y SPD

Aspecto	SAD	SPD
Pregunta	¿Qué SA está negociada?	¿Qué tráfico debe protegerse?

Aspecto	SAD	SPD
Momento típico	Tras éxito de la negociación.	Tras cargar políticas de configuración.
Naturaleza	Asociaciones activas/direccionales.	Selectores y reglas de procesamiento.
Túnel desconectado	La SA puede faltar.	La política puede seguir presente.
Incidencia típica	Rekey, SPI, ESP/NAT-T.	Solapamiento de redes o selectors incorrectos.

72.18. Puertos y protocolos: cómo interpretar los registros

IKE usa normalmente UDP 500; NAT Traversal utiliza UDP 4500 y encapsula ESP cuando corresponde. ESP es el protocolo IP 50, no un puerto TCP/UDP. La falta de negociación puede deberse a reglas perimetrales, traducciones NAT o negociación incompatible. Un túnel establecido sin tráfico exige analizar también las reglas sobre IPsec/enc0, las redes remotas y la respuesta de los equipos.

72.19. Distinción entre fallos de negociación y fallos de transporte

Síntoma	Hipótesis principal	Herramientas
No IKE SA	Autenticación, reachability o propuestas incompatibles.	System Logs → IPsec; Firewall; WAN capture.
IKE SA sin CHILD SA	Selectores o propuestas fase 2 incompatibles.	Overview expandido; logs CHILD_SA.
CHILD SA activa, tráfico bloqueado	Reglas IPsec/enc0 o interfaces asignadas.	Firewall Rules; firewall log.
TX sin RX	Ruta de retorno, ACL/firewall remoto, NAT.	Counters, packet capture, rutas.
Se corta al renovar	Lifetimes, DPD, peer, rekey.	Temporizadores y registros correlacionados.
Otra VPN no recibe paquetes	Política SPD residual/solapada.	Status → IPsec → SPDs; diseño selector.

72.20. Logs de IPsec y niveles temporales de diagnóstico

Netgate propone, para un análisis focalizado, establecer IKE SA, IKE Child SA y Configuration Backend en nivel Diag y mantener el resto en Control desde VPN → IPsec → Advanced Settings. Aumentar el detalle puede elevar la carga de registros y debe revertirse después de la investigación. En los logs, “IKE_SA ... established” señala la fase de control y “CHILD_SA ... established” indica que la negociación de datos se completó.

72.21. CLI no disruptiva: inventario y estado

Comando orientativo	Uso	Advertencia
swanctl --list-conns	Consulta nombres/definiciones cargadas.	Salida puede revelar identificadores: proteger evidencias.
swanctl --list-sas	Inspecciona SAs observadas en strongSwan.	No confundir IKE con kernel SAD.
setkey -DP	Muestra las políticas SPD del núcleo cuando está disponible.	Comprobar disponibilidad y permisos.
setkey -D	Muestra asociaciones IPsec del núcleo cuando está disponible.	Contiene información operativa sensible.
netstat -rn	Consulta rutas en entornos VTI.	No equivale a políticas SPD en policy-based.

SEGURIDAD Las órdenes de listado son observacionales. No utilizar swanctl --terminate, reinicios, borrados manuales de SPD/SAD ni recargas de servicio sin evaluar previamente los túneles afectados.

72.22. Procedimiento: diagnóstico del aviso IPsec deshabilitado

01. Abrir Status → IPsec → Overview y registrar el texto exacto del aviso, sin publicar detalles de la instalación.

02. Visitar VPN → IPsec → Tunnels y comprobar si existen Phase 1 habilitadas; no activarlas automáticamente.

03. Consultar Status → Services para conocer el estado del servicio IPsec y revisar registros si no está operativo.

04. Identificar si el servicio es requerido por sedes, clientes móviles o enlaces redundantes; preparar respaldo y ventana de cambios.

05. Si la configuración debe activarse, seguir el procedimiento de VPN → IPsec y validar Overview, SADs, SPDs y tráfico real.

72.23. Procedimiento: comprobar un túnel site-to-site

01. Localizar la entrada por descripción e ID en Overview y verificar qué peer figura como Local y Remote.

02. Confirmar IKE SA y expandir las CHILD SA que correspondan a las redes previstas.

03. Correlacionar SAs en SADs y políticas/selector en SPDs; documentar divergencias.

04. Lanzar tráfico de prueba desde un host de la subred local a otro host autorizado en la remota.

05. Comparar contadores, reglas y registros en ambos extremos, con atención a rutas de retorno y firewall de destino.

06. Registrar resultado, tiempo, sentido de prueba y estado final de las asociaciones.

72.24. Procedimiento: auditar acceso remoto móvil

01. Comprobar que el perfil móvil IPsec está habilitado y que los mecanismos de autenticación son los previstos.

02. Consultar Leases y registrar únicamente estadísticas agregadas o direcciones ficticias en el informe.

03. Correlacionar la concesión con sesión IKE/CHILD y evento de autenticación en los registros pertinentes.

04. Comprobar que el cliente recibe una ruta adecuada y puede acceder solo a los recursos permitidos.

05. Verificar desconexión limpia, liberación o caducidad conforme a la política de cliente y retención.

72.25. Procedimiento: investigar tráfico desaparecido

01. Identificar redes origen/destino y confirmar que el problema se reproduce sin cambiar el firewall.

02. Revisar SPDs buscando selectores de túneles antiguos o superpuestos con OpenVPN/WireGuard.

03. Determinar si el esquema es policy-based o VTI y consultar rutas o interfaz asignada según corresponda.

04. Verificar reglas de firewall y captura de paquetes, tanto en WAN como en IPsec/enc0 cuando proceda.

05. Solo tras identificar una política residual, planificar la retirada o corrección de la configuración responsable.

06. Validar conectividad y ausencia de regresiones para otros túneles.

72.26. Diagnóstico de Multi-WAN y gateways remotos

En instalaciones Multi-WAN, una negociación puede usar una dirección externa distinta a la prevista tras un cambio de gateway o DDNS. Verificar WAN de origen, NAT-T, retorno simétrico, reglas para UDP 500/4500 y rutas cuando se utiliza VTI. La vista Overview ayuda a verificar los endpoints realmente utilizados, pero la política de selección del enlace se diagnostica también en Gateways, reglas de firewall y rutas.

72.27. Alta disponibilidad y failover: implicaciones

En despliegues redundantes, el estado de IPsec debe analizarse por nodo: que el par de respaldo esté sano no garantiza que la asociación del nodo principal se haya restaurado tras failover. Confirmar estado CARP, sincronización de configuración, estado de interfaces WAN, negociación nueva IKE/CHILD y disponibilidad del camino de datos. Las capacidades de continuidad dependen del diseño de SA y de la versión; no asumir sincronización transparente de todas las SAs.

72.28. Monitorización de cambios de fase y temporizadores

Las asociaciones IPsec se renuevan por expiración o políticas de reautenticación/rekey. Un cambio de SPI o del temporizador no debe interpretarse por sí solo como ataque. La aparición repetida de desconexiones, renegociaciones fallidas o ausencia de contadores sí exige revisar la negociación y las condiciones del enlace. Correlacionar horas de eventos de ambos peers teniendo en cuenta NTP.

72.29. Guía de comprobación por capas



Figura 72.4. Secuencia de diagnóstico progresiva sin alterar la conectividad de producción.

72.30. Escenario empresarial A: enlace entre dos oficinas

Ejemplo ficticio: la sede A protege 192.0.2.0/24 y la sede B 198.51.100.0/24 únicamente como identificadores didácticos TEST-NET; no son subredes reales recomendadas para despliegue. Una CHILD SA negociada confirma los selectores, pero la prueba del servicio exige conectividad entre equipos de redes privadas configuradas por el administrador. Los prefijos TEST-NET son exclusivamente ilustrativos y deben reemplazarse por direccionamiento legítimo en cualquier entorno real.

Si Overview muestra IKE establecida y no pasa tráfico, comparar SPD con selectores de Phase 2, capturar el flujo y comprobar reglas en ambos extremos. La herramienta de verificación no debe usarse como excusa para reiniciar todos los túneles.

72.31. Escenario empresarial B: usuarios móviles con pools

Un operador detecta que los usuarios autenticados no acceden a aplicaciones. Leases confirma que el pool asignó una dirección; Overview confirma la CHILD SA. La investigación debe continuar con DNS, split tunnel, ruta de retorno y reglas de firewall para recursos internos. El hecho de que exista lease demuestra asignación, no acceso efectivo.

72.32. Escenario empresarial C: migración entre tecnologías VPN

Se migra una red remota desde un túnel IPsec policy-based a WireGuard. Tras deshabilitar IPsec, los paquetes dejan de seguir la nueva ruta. La revisión de SPDs revela una política antigua que coincide con los selectores. Tras retirar la definición responsable en una ventana controlada y limpiar el estado del servicio si la documentación y diagnóstico lo justifican, se repiten pruebas en ambos sentidos y se verifica que no se afectan otros túneles.

72.33. Seguridad y conservación de evidencias

Las pantallas de IPsec y los registros pueden exponer nombres de peers, usuarios, direcciones, topología, certificados e información de negociación. Antes de compartir informes, anonimizar identificadores, rutas, contadores asociados a servicios críticos, sesiones y direcciones. Nunca adjuntar PSK, claves privadas ni archivos de configuración completos a tickets externos. Registrar responsable, motivo, hora y resultado de cualquier acción de conexión, desconexión o reinicio.

72.34. Lista de comprobación operativa

Comprobación	Resultado esperado
Servicio IPsec	Estado coherente con las Phase 1 habilitadas.
IKE y CHILD SA	Establecidas según el diseño y la necesidad de tráfico.
Leases	Asignaciones coherentes para clientes móviles.
SADs	Asociaciones activas en las direcciones esperadas.
SPDs	Selectores precisos y sin solapamientos no previstos.
Firewall	Reglas en IPsec/enc0 y WAN adecuadas al diseño.
Rutas y VTI	Enrutamiento verificado si es IPsec basado en rutas.
Logs	Ausencia de errores críticos repetitivos; horas sincronizadas.
Prueba real	Tráfico de aplicación correcto en ida y vuelta.
Reversión	Procedimiento previsto para toda acción disruptiva.

72.35. Glosario técnico esencial

Término	Significado
IKE / IKE SA	Intercambio de claves y asociación de control autenticada.
CHILD SA	Asociación de IPsec para transporte protegido de datos.
SAD	Base de asociaciones de seguridad negociadas.
SPD	Base de políticas que seleccionan cómo procesar tráfico.
SPI	Índice utilizado para identificar una SA IPsec.
ESP	Protocolo IP 50 de encapsulación y protección.
NAT-T	Encapsulación compatible con NAT, normalmente UDP 4500.
Traffic selectors	Redes/direcciones y condiciones que cubre una CHILD SA.
VTI	Interfaz virtual para IPsec basado en rutas.
Rekey / DPD	Renovación de SA / detección de disponibilidad del peer.

72.36. Referencias oficiales y lectura complementaria

- Netgate — IPsec Status

- Netgate — IPsec Terminology
- Netgate — Troubleshooting IPsec Connections
- Netgate — Troubleshooting IPsec Traffic
- Netgate — Troubleshooting IPsec Logs
- Netgate — Troubleshooting Lost Traffic or Disappearing Packets
- Netgate — IPsec Tunnel Design
- Netgate — IPsec Configuration
- Netgate — Routes and VPNs
- Netgate — IPsec Site-to-Site VPN Example
- Netgate — Dashboard IPsec Widget
- Netgate — Status menu

73 Status → Monitoring

Gráficas RRD · CPU · tráfico · calidad de enlaces · tendencias · percentiles · diagnóstico profesional

La monitorización histórica transforma muestras periódicas del cortafuegos en tendencias comparables. Su valor reside en interpretar correctamente unidades, periodos, resolución y contexto, no solo en localizar picos. Este capítulo explica cómo utilizar los gráficos para decidir con evidencia, sin confundir observación con causalidad.

IDEA CENTRAL Una curva baja o una gráfica vacía no demuestran ausencia de actividad. Las escalas, la consolidación RRD, la selección de fuentes y el periodo consultado condicionan cada conclusión.

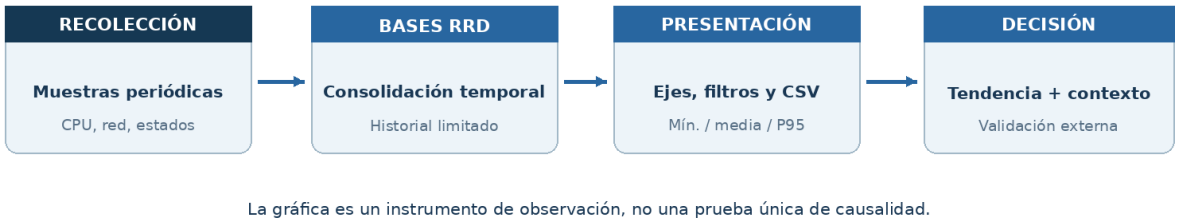


Figura 73.1. Ciclo de supervisión histórica: muestreo, consolidación, análisis y decisión.

73.1. Objetivo, ubicación y alcance de Status → Monitoring

Ruta: Status → Monitoring. La pantalla presenta una vista gráfica interactiva y una tabla de resumen estadístico. Está orientada a observar tendencias históricas de CPU, memoria, tablas de estados, interfaces, paquetes, gateways, servicios y otras fuentes que estén disponibles según el sistema y la configuración. La vista mostrada es «Default» y representa System → Processor en el eje izquierdo; el eje derecho está sin configurar.

La documentación oficial denomina Monitoring Graphs a esta herramienta. Se diferencia de Status → Traffic Graph, que se utiliza para inspección dinámica del tráfico de interfaces, y de Status → Dashboard, orientado a un resumen operativo del momento.

73.2. Elementos visibles de la pantalla de Monitoring

Elemento de la GUI	Qué representa	Criterio de uso
Barra Status / Monitoring	Identifica la página actual y proporciona los iconos de herramientas.	No confundir con una página de configuración de interfaces.
Pestaña Default	Vista o conjunto de preferencias de gráfica mostrado.	Otras vistas pueden aparecer según la configuración.
Icono de llave (wrench)	Despliega el panel de ajustes de gráfica.	No altera por sí solo el tráfico ni las reglas.
Icono de recarga	Actualiza la representación conforme a la configuración elegida.	No equivale a resetear las bases RRD.
Icono de descarga	Exportación de los datos de gráfica en CSV.	Revisar periodo, resolución y unidades.
Ayuda (?)	Acceso a documentación contextual.	Comprobar diferencias entre versiones.
Interactive Graph	Trazado temporal y leyenda de las series.	Unidades y escalas deben interpretarse por separado.
Data Summary	Resumen por serie: Minimum, Average, Maximum, Last y, cuando procede, 95th Percentile.	Una celda vacía no significa cero.

73.3. Estructura del gráfico interactivo y lectura de ejes

Left Axis y Right Axis muestran el par categoría/gráfico seleccionado. Al pasar de un gráfico de CPU a uno de tráfico, el significado del eje cambia. Cuando se comparan dos magnitudes, ambos ejes pueden mostrar unidades diferentes; nunca debe deducirse una proporción por la proximidad visual entre dos curvas. El eje horizontal es temporal y expresa la ventana elegida, no necesariamente un flujo continuo de muestras independientes.

En la parte superior de la gráfica, la leyenda identifica los datos. Pulsar un elemento de la leyenda lo oculta visualmente para despejar el trazado, sin borrar la información almacenada. En el pie figuran el identificador del cortafuegos, el periodo, la resolución y el instante de generación. Para comparaciones rigurosas deben registrarse esos cuatro datos, preservando la confidencialidad del sistema.

73.4. Processor: explicación técnica de las cinco series visibles

Serie	Unidad	Interpretación técnica / posibles causas
user util.	%	Tiempo de CPU dedicado a procesos de espacio de usuario: servicios, utilidades y aplicaciones.
nice util.	%	Tiempo de CPU de procesos ejecutados con prioridad ajustada (nice). No es sinónimo de CPU libre.
system util.	%	Trabajo de kernel/sistema: red, llamadas al sistema y actividades internas.
interrupt	%	Tiempo dedicado a atender interrupciones y E/S; valores elevados pueden relacionarse con NIC, colas o controladores.
processes	número	Número de procesos del sistema; es un recuento, no un porcentaje de CPU.

La serie «processes», al ser un recuento habitualmente muy superior a los valores porcentuales de CPU, puede imponer una escala vertical que haga parecer plana la utilización de procesador. Una lectura visual correcta consiste en ocultar temporalmente la serie de procesos, consultar el resumen numérico o elegir series comparables mediante los ajustes. El hecho de ocultar la línea no modifica la carga ni el número real de procesos.

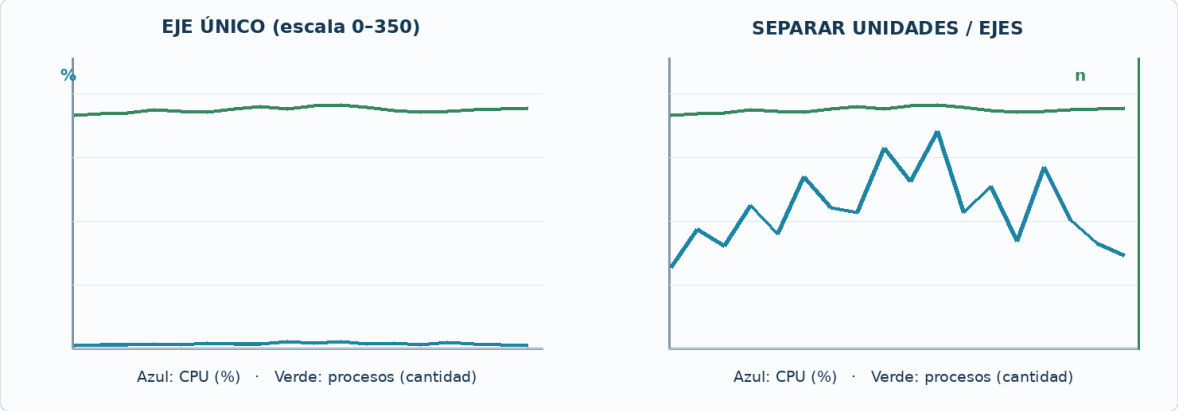


Figura 73.2. Ejemplo didáctico ficticio: el recuento de procesos distorsiona la lectura porcentual cuando comparten escala.

73.5. El resumen estadístico: Minimum, Average, Maximum, Last y P95

Columna	Significado	Precaución
Minimum	Mínimo observado en la serie y el rango.	Puede depender de cómo RRD haya consolidado los intervalos.
Average	Media de valores representados en el periodo.	Puede ocultar interrupciones breves o picos.
Maximum	Mayor valor observado/almacenado para la resolución.	No es garantía de captar un pico entre muestras.

Columna	Significado	Precaución
Last	Último dato de la serie, cuando está disponible.	No es necesariamente una medición instantánea en tiempo real.
95th Percentile	Valor por debajo o igual al cual se sitúa aproximadamente el 95 % de las muestras consideradas.	No representa consumo total; puede no aparecer para todas las series.

El percentil 95 es muy útil para valorar carga sostenida y eliminar el sesgo de algunos picos extremos; por el contrario, en análisis de microcortes, latencia elevada o ráfagas críticas también debe consultarse el máximo y la granularidad de las muestras. Si una columna figura vacía, no atribuirle el valor cero ni suponer que la interfaz carece de soporte: la documentación advierte que el percentil se presenta solo en determinadas series.



Figura 73.3. Percentil 95, media y máximo sobre una distribución sintética; no corresponde a ninguna infraestructura real.

73.6. ¿Qué es RRD y cómo almacena el histórico?

RRD (Round-Robin Database) conserva datos de series temporales con estructura y retención finitas. El cortafuegos recoge muestras y consolida registros de mayor antigüedad; a medida que crece el horizonte de consulta se pierden detalles de corta duración. Por tanto, cambiar de una vista de una hora a otra de varias semanas altera tanto la escala temporal como la resolución efectiva de la evidencia.

No se deben sumar ingenuamente valores medios de una gráfica RRD para obtener el volumen exacto transferido. Netgate explica que las bases gráficas no proporcionan totales fiables de tráfico; para contabilización histórica recomienda herramientas específicamente orientadas a totales. Los huecos pueden deberse a ausencia de datos, periodos anteriores a la activación, problemas de recogida o retención, y no deben interpretarse automáticamente como caídas de red.

73.7. Panel Graph Settings: ejes, categoría y gráfica

La llave del encabezado abre el panel de opciones. En Left Axis / Right Axis se eligen Category y Graph. De forma predeterminada se utiliza solo el eje izquierdo, aunque ambos pueden emplearse para correlacionar fuentes. La lista de categorías y gráficas cambia según hardware, servicios activados, paquetes y versión: no todas las categorías enumeradas en Netgate aparecerán en cada equipo.

Opción documentada	Comportamiento	Uso recomendado
Left Axis / Right Axis	Asigna uno o dos pares categoría/gráfica.	Separar unidades distintas cuando sea apropiado.
Category	Selecciona familia: System, Traffic, Packets, Quality, etc.	Empezar por la hipótesis de diagnóstico.
Graph	Métrica concreta dentro de la categoría.	Elegir interfaz/gateway correcto.
Time Period	Periodo desde 1 hora hasta varios años o Custom según Netgate.	Comparar intervalos equivalentes.
Resolution	Muestras/promedios disponibles de 1 min, 5 min, 1 h o 1 día según histórico.	No exigir detalle que la base ya consolidó.
Inverse	Invierte visualmente una serie, típico en caudal entrante/saliente.	Interpretar signo negativo como convención de presentación.

Opción documentada	Comportamiento	Uso recomendado
Custom Period	Permite fijar fechas y horas de inicio y fin.	La hora final es exclusiva.
Settings / Show Advanced	Muestra opciones adicionales de presentación.	Verificar los campos reales antes de cambiarlos.
Export as CSV	Descarga datos del gráfico según la selección.	Conservar unidad, periodo y resolución.
Save as Defaults	Guarda la visualización elegida como predeterminada.	Documentar cambios en consolas compartidas.
Disable/Enable Graphing	Detiene o reanuda la recogida histórica.	Evitar en producción sin otra fuente de monitorización.
Reset Graphing Data	Borra archivos de bases de gráficas y los recrea vacíos.	Operación destructiva; requiere autorización.
Update Graphs	Redibuja la gráfica con los ajustes aplicados.	No borra el historial.

73.8. Elección del periodo y de la resolución

El periodo determina cuántas horas, días o años se muestran. La resolución expresa el intervalo mínimo de los datos disponibles para esa vista. Una resolución de cinco minutos no significa que el dispositivo solo trabaje una vez cada cinco minutos: representa una agregación temporal de valores. En periodos antiguos puede existir únicamente una media por hora o por día. Los picos de duración inferior al intervalo quedan atenuados o pueden perderse.

Si se selecciona Custom, Start Date y End Date acotan la ventana; Start Hour y End Hour usan el formato de 24 horas. Netgate especifica que la hora final es exclusiva: del inicio a las 10 h al final a las 12 h comprende hasta antes de las 12 h. El sistema no puede mostrar muestras anteriores al momento en que empezó la recogida.

73.9. Opciones de presentación, leyenda, actualización y exportación

La leyenda es interactiva y permite ocultar series para reducir saturación. La actualización redibuja el gráfico; la exportación CSV permite conservar muestras para análisis externo, pero no corrige los vacíos, errores ni consolidaciones de origen. El botón Save as Defaults modifica preferencias de visualización, no el funcionamiento de CPU, NAT o VPN. Las opciones avanzadas de estilo o actualización pueden variar con la revisión de pfSense; conviene utilizar la ayuda de la versión desplegada antes de considerar un control universal.

ADVERTENCIA Reset Graphing Data elimina el histórico local de las gráficas. No ejecutarlo para «arreglar» una curva extraña sin exportar evidencias y confirmar si el problema procede de la fuente, el periodo, el navegador o la presentación.

73.10. Categoría System: procesador, memoria, estados y mbufs

Gráfica	Aspectos que estudia	Alerta / correlación
Processor	Utilización user, nice, system, interrupt y procesos.	Relacionar picos con VPN, carga de paquetes, actualizaciones o servicios.
Memory	Memoria activa, inactiva, libre, cableada y cachés según FS/versión.	Evitar interpretar toda la caché como memoria irrecuperable.
States	Estados PF, NAT, cambios por segundo y direcciones origen/destino.	Distinguir ocupación elevada de tasa alta de creación/destrucción.
Mbuf Clusters	Buffers de red disponibles, actuales, caché y máximo.	Cercanía sostenida al máximo puede requerir diagnóstico de red.

La interpretación de memoria exige considerar FreeBSD y el sistema de archivos: ciertas cifras de caché y memoria cableada tienen significado diferente entre sistemas UFS y ZFS y entre versiones de pfSense Plus. En versiones 23.05 y posteriores Netgate documenta separación de determinados componentes de la caché ZFS en la presentación gráfica. No comparar series históricas de distintas versiones sin señalar cambios metodológicos.

73.11. Categorías Traffic y Packets: caudal frente a paquetes

Traffic representa velocidades (bits por segundo) por interfaz, con diferenciación de tráfico permitido/bloqueado y, en ciertos gráficos, IPv4/IPv6. Packets expresa paquetes por segundo (PPS). Un enlace puede estar lejos de su capacidad nominal en Mbps y, sin embargo, agotar la capacidad de proceso de paquetes cuando predominan tramas pequeñas. La dirección In/Out siempre se interpreta desde la interfaz del cortafuegos, no desde la perspectiva del usuario final.

Indicio	Lectura adecuada	Paso siguiente
Mbps altos, PPS moderados	Grandes bloques de datos.	Revisar saturación de enlace y colas.
PPS muy altos, Mbps moderados	Muchos paquetes pequeños / posibles límites de CPU o NIC.	Correlacionar interrupts, states y contador de errores.
Bloqueo elevado	PF descarta tráfico según reglas.	Verificar logs y reglas sin concluir ataque automáticamente.
Inversión activada	La serie invertida aparece con signo negativo por diseño.	No presentar velocidad negativa real.

73.12. Quality: pérdida, retraso y variabilidad de las WAN

La categoría Quality se basa en la monitorización de gateways y muestra Packet Loss (%), Delay Average (RTT) y Delay Standard Deviation (variabilidad). Estos datos se obtienen respecto a la dirección Monitor IP seleccionada. Una pérdida ICMP elevada puede estar causada por el propio destino de monitorización o por filtrado intermedio; no prueba por sí misma que todas las aplicaciones estén sin conectividad.

Para estudiar Multi-WAN, colocar lado a lado los periodos de calidad de cada enlace, las gráficas de tráfico y el historial de gateways. Diferenciar disponibilidad física de la interfaz, respuesta al monitor y conectividad de la aplicación. Un cambio de ruta o un failover puede manifestarse como variación de latencia sin caída completa de usuarios.

73.13. Otras categorías condicionadas: NTP, DHCP, colas, portal y VPN

Categoría	Datos típicos	Condición
NTP	Offset, jitter, wander, frecuencia y dispersión.	Requiere habilitar las gráficas NTP donde proceda.
DHCP	Concesiones dinámicas, mapeos estáticos y tamaño del pool.	Requiere servidores DHCP activos en interfaces.
Queues / QueueDrops	Uso de colas y descartes de traffic shaping.	Depende de configuraciones ALTQ/colas.
Captive Portal	Sesiones simultáneas y eventos de login.	Depende de zonas de portal activas o históricas.
VPN Users	Usuarios OpenVPN concurrentes.	Depende de servidores OpenVPN.
Cellular / Wireless	Señal 3G/4G o datos Wi-Fi (SNR, canal, tasa).	Solo con hardware/configuración compatible.

Las categorías no disponibles en un equipo no implican necesariamente una avería: algunas requieren activar el servicio o disponer del hardware adecuado. La lista real debe verificarse al desplegar el panel de ajustes de la instancia.

73.14. Diagnóstico integrado: correlación y límites de causalidad

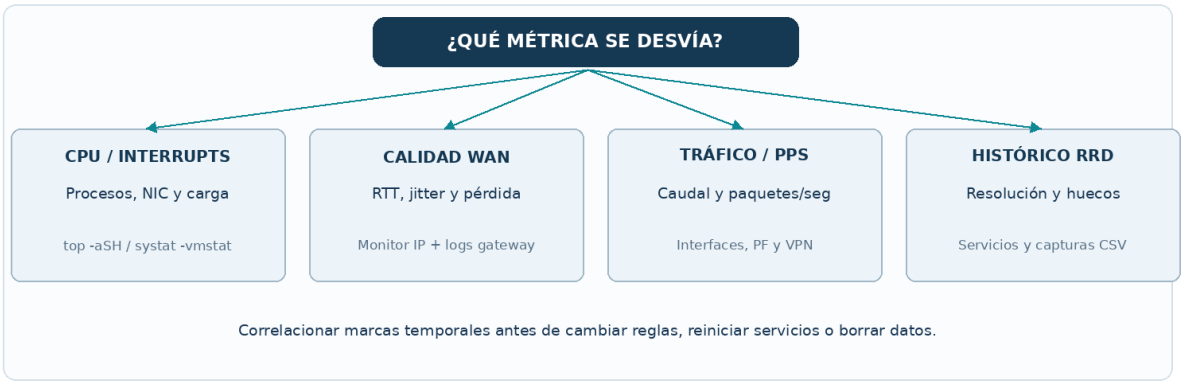


Figura 73.4. Árbol didáctico de correlación para investigar anomalías observadas en las gráficas.

Las métricas son indicadores y deben validarse mediante registros, estado de interfaces, logs de servicios y pruebas de extremo a extremo. Un repunte simultáneo de CPU y RTT no prueba por sí solo que la CPU haya causado la latencia. Establecer secuencia temporal, duración, alcance, disponibilidad de muestras y reproducibilidad antes de modificar parámetros de red.

73.15. Procedimiento 1: investigar un consumo elevado de CPU

01 En Status → Monitoring seleccionar System → Processor, periodo de una hora, y la máxima resolución disponible.

02 Ocultar temporalmente la serie processes si comparte escala con los porcentajes de CPU; anotar máximos, medias y duración de los picos.

03 Contrastar CPU de usuario, sistema e interrupciones, y revisar simultáneamente Packets, States y tráfico WAN.

04 En una ventana autorizada, consultar top -aSH o systat -vmstat 1 para identificar procesos o interrupciones predominantes.

05 Revisar cronología de tareas, actualizaciones y servicios sin reiniciar automáticamente; anotar hipótesis y prueba de verificación.

73.16. Procedimiento 2: investigar microcortes o latencia en Multi-WAN

01 Elegir Quality del gateway afectado y una ventana que abarque el incidente, con resolución suficiente.

02 Identificar picos de Delay Average, Delay Standard Deviation y Packet Loss; comprobar si coincide con el momento reportado por usuarios.

03 Comparar con Status → Gateways, logs del monitor y Traffic/Packets de la interfaz.

04 Comprobar dirección monitorizada y posible limitación de respuesta ICMP; validar aplicaciones y rutas con una prueba controlada.

05 Solo tras confirmar la causa, aplicar ajustes de monitorización, umbrales o rutas mediante el procedimiento de cambios habitual.

73.17. Procedimiento 3: documentar tendencia de caudal y capacidad

01 Escoger Traffic de la interfaz de interés y registrar sentido In/Out, unidades y si Inverse está activo.

02 Elegir periodos comparables de trabajo, preferentemente días de la semana semejantes y mismo horario.

03 Analizar media, máximos y percentil 95 cuando esté disponible, sin extrapolar automáticamente datos RRD a facturación.

04 Cruzar con Packets para distinguir volumen de datos y presión por PPS; revisar pérdidas de calidad del gateway.

05 Exportar CSV y añadir contexto de mantenimiento, actividades de negocio y cambios de configuración en un informe de capacidad.

73.18. Procedimiento 4: exportación CSV para auditoría

01 Revisar que el gráfico seleccionado, el rango, resolución, categoría y ejes coincidan con la consulta.

02 Usar Export as CSV y conservar el fichero con una etiqueta documental neutral, fecha y origen de forma no identificativa.

03 Validar cabeceras, unidades, número de muestras, posibles huecos y si existen valores nulos o no disponibles.

04 Documentar de forma explícita que la fuente es RRD y puede contener consolidación histórica.

05 Al compartir resultados, anonimizar hostnames, interfaces, datos del tráfico y marcas temporales sensibles conforme a la política de seguridad.

73.19. Procedimiento 5: recuperación de gráficas vacías o incompletas

01 Comprobar si el periodo incluye datos desde el comienzo de la recogida y si la resolución solicitada es válida.

02 Cambiar a una ventana corta y a una categoría habitual, como System → Processor, para diferenciar ausencia parcial de ausencia general.

03 Comprobar si la recogida de gráficas está habilitada y si el navegador muestra fallos de presentación o caché.

04 Revisar estado del sistema, almacenamiento y logs relacionados, con atención a problemas de escritura o servicios.

05 No pulsar Reset Graphing Data salvo que se haya diagnosticado corrupción, exportado la evidencia disponible y aprobado la pérdida del histórico.

73.20. Cinco escenarios de uso en una organización

Escenario	Qué correlacionar	Resultado esperado
A. Firewall de borde en hora punta	Processor + Traffic + Packets + States.	Distinguir cuello de botella de enlace, CPU o tabla PF.
B. Enlace WAN con conmutación	Quality + status/logs gateway + Traffic.	Diferenciar pérdida real de conectividad y fallo del monitor.
C. VPN con sesiones inestables	VPN Users + CPU + Quality + logs VPN.	Localizar coincidencias temporales sin atribuir causa prematuramente.
D. DHCP próximo a agotar el pool	DHCP leases + eventos DHCP + cambios de usuarios.	Planificar capacidad y descartar concesiones obsoletas.
E. Alerta de memoria/mbufs	Memory + mbuf + PPS + logs sistema.	Evaluar presión del subsistema de red y descartar variaciones normales.

73.21. Seguridad y gobierno del histórico de monitorización

Las gráficas y los CSV pueden revelar períodos de actividad de una organización, interfaces de comunicación, nombres de equipos y patrones operativos. Limitar la visibilidad mediante usuarios y privilegios, aplicar las políticas de retención de registros y evitar compartir exportaciones sin anonimizar. Los datos gráficos no sustituyen los logs auditables de seguridad, registros externos de monitorización ni pruebas activas autorizadas.

En sistemas con unidades de almacenamiento sometidas a desgaste, RRD realiza escrituras periódicas. Netgate explica que su desactivación puede reducir escritura local, aunque sacrifica capacidad de análisis y debe evaluarse junto con SNMP/NMS externo. Es preferible conservar observabilidad independiente si se decide desactivar la recolección en un cortafuegos de producción.

73.22. Errores frecuentes de interpretación y respuesta correcta

Interpretación equivocada	Por qué es incorrecta	Qué comprobar
«CPU casi al cero porque la curva queda abajo».	La escala está dominada por un recuento de procesos.	Resumen y leyenda; ocultar processes.
«La media demuestra que no hubo microcorte».	La media y la consolidación suavizan picos.	Máximo, resolución y logs correlacionados.
«0 paquetes perdidos = Internet garantizado».	Quality vigila solo una dirección Monitor IP.	Pruebas de las aplicaciones y rutas.
«P95 es el máximo real».	P95 suele excluir parte de los valores superiores.	Confrontar P95 y Maximum.
«Export CSV = bytes facturados».	Las gráficas históricas no permiten sumas exactas sin matices.	Medidor adecuado de volúmenes/totales.
«Reset arregla el problema del gráfico».	Borra el histórico y no corrige necesariamente la causa.	Validar origen y conservar datos.

73.23. Matriz de resolución de incidencias

Síntoma	Posibles causas	Prueba segura / acción
Gráfica vacía	RRD no inicializada, periodo sin datos, fuente ausente.	Probar System/Processor en periodo corto; revisar recogida.
Salto discontinuo de serie	Retención/consolidación, arranque, huecos.	Cruzar con uptime y eventos; no rellenar artificialmente.
CPU gráfico ≠ Dashboard	Diferencia entre histórico y lectura instantánea.	Comparar misma hora y misma métrica.
Los gráficos parecen lentos	Periodo extenso, navegador, carga.	Reducir ventana y series; comprobar recursos webGUI.
Tráfico anormalmente alto	Inversión, unidad, sentido o interfaz equivocada.	Confirmar ejes, fuente, dirección y unidades.
Valores de monitor desproporcionados	Monitor IP, jitter, ICMP penalizado.	Validar gateway y destino alternativo autorizado.

73.24. Criterios para decidir una intervención sobre producción

Antes de modificar políticas de firewall, interfaces, servicios, firmware o parámetros de rendimiento debe existir una hipótesis técnica respaldada por datos y una ventana aprobada. Recoger una serie de referencia, exportar evidencia, disponer de acceso de recuperación y comprobar la reversibilidad. La correlación temporal es necesaria, pero no suficiente: la causalidad exige pruebas adicionales.

NO DESTRUCTIVO / DESTRUCTIVO Consultar, filtrar, ocultar series y exportar CSV son operaciones de observación. Disable/Enable Graphing cambia la recogida. Reset Graphing Data borra el histórico gráfico almacenado y exige un tratamiento como cambio con pérdida de evidencias.

73.25. Glosario de términos esenciales

Término	Definición técnica
RRD	Base de series temporales de tamaño/retención controlados que consolida datos antiguos.
Resolución	Intervalo temporal agregado representado por cada dato del gráfico.
P95	Percentil 95 de una distribución de muestras consideradas.
RTT	Tiempo de ida y vuelta de un sondeo al destino monitorizado.
RTTsd / jitter	Variación estadística de los RTT en una ventana de observación.
PPS	Paquetes por segundo procesados/transmitidos.

Término	Definición técnica
Mbuf	Estructuras de memoria de red de FreeBSD para gestionar buffers de paquetes.
PF States	Estados de flujo mantenidos por el motor de filtrado PF.
Consolidación	Combinación de muestras en intervalos mayores para retención histórica.

73.26. Lista de comprobación para la administración diaria

- ☐ Revisar CPU con sus cinco series y sin confundir procesos con porcentajes.
- ☐ Confirmar al menos una visión histórica de Quality por enlace principal y de respaldo.
- ☐ Cruzar Traffic y Packets cuando el rendimiento parezca anómalo.
- ☐ Registrar resolución, periodo y unidad antes de comparar gráficos.
- ☐ Comprobar tendencias de States y mbufs cuando existan síntomas de saturación.
- ☐ No modificar recolección ni borrar bases gráficas sin autorización.
- ☐ Exportar información relevante antes de un cambio importante y anonimizarla al compartir.

73.27. Ficha de evidencias para una incidencia de rendimiento

La ficha siguiente permite unificar la investigación de incidencias, separar hechos de hipótesis y documentar los datos necesarios para reproducir el análisis. Todos sus campos deben completarse evitando nombres de equipos o usuarios reales cuando el documento se distribuya fuera del equipo autorizado.

Campo de la ficha	Qué registrar	Para qué sirve
Ventana temporal	Fecha y hora de inicio/fin; zona horaria.	Correlacionar la gráfica con logs y reportes.
Vista RRD	Category, Graph, ejes, unidad, periodo y resolución.	Reproducir exactamente la observación.
Magnitud	Mínimo, media, máximo, último, P95 si existe.	Evitar conclusiones basadas en un solo pico.
Evidencia cruzada	Estados, interfaces, gateway, logs, VPN y pruebas.	Buscar señales independientes.
Impacto	Servicio afectado, duración y alcance operativo.	Priorizar medidas sin exagerar síntomas.
Hipótesis y prueba	Causa propuesta, evidencia en contra y prueba segura.	Separar correlación de causalidad.
Cambio / reversión	Acción autorizada y resultado posterior.	Conservar trazabilidad y capacidad de vuelta.

73.28. Plan de revisión y conservación de tendencias

Una rutina útil combina revisión diaria del estado general, revisión semanal de tendencias y revisión mensual de capacidad. En cada periodo deben examinarse siempre las mismas ventanas operativas y los mismos criterios de medida, de modo que los cambios sean comparables. La frecuencia es un ejemplo de práctica administrativa, no un valor obligatorio del producto.

Para una memoria técnica trimestral, registrar los datos agregados de CPU (sin mezclar porcentajes y procesos), picos de PPS, percentiles de tráfico, pérdida y latencia por gateway, evolución de estados y mbufs, incidencias y cambios relevantes. Si se modifican reglas, interfaces, versión o equipos, reflejar esa discontinuidad: comparar sin contexto puede originar falsas conclusiones.

73.29. Referencias oficiales y bibliografía técnica

[01] Netgate: Monitoring Graphs

[02] Netgate: Working with Graphs

[03] Netgate: Graph Settings

[04] Netgate: Graph Category List
[05] Netgate: System Monitoring
[06] Netgate: Menu Status
[07] Netgate: General Configuration Options
[08] Netgate: Firewall Fundamentals (PF States)
[09] Netgate: Gateway Status
[10] Netgate: Troubleshooting High CPU Load
[11] Netgate: Troubleshooting Disk Writes

74 Status → NTP

Sincronización horaria · pares · estratos · Reach · offset · jitter · supervisión y diagnóstico

La precisión temporal sostiene la autenticación, la validez de certificados, los registros y la correlación de incidencias. Este capítulo explica cómo leer de forma rigurosa el estado del servicio NTP de pfSense Plus y cómo detectar errores sin perturbar la red.

IDEA CENTRAL Un servidor señalado como Active Peer es la referencia seleccionada; no implica por sí solo que toda la red esté sincronizada. Reach, offset, jitter y los registros aportan evidencias complementarias.

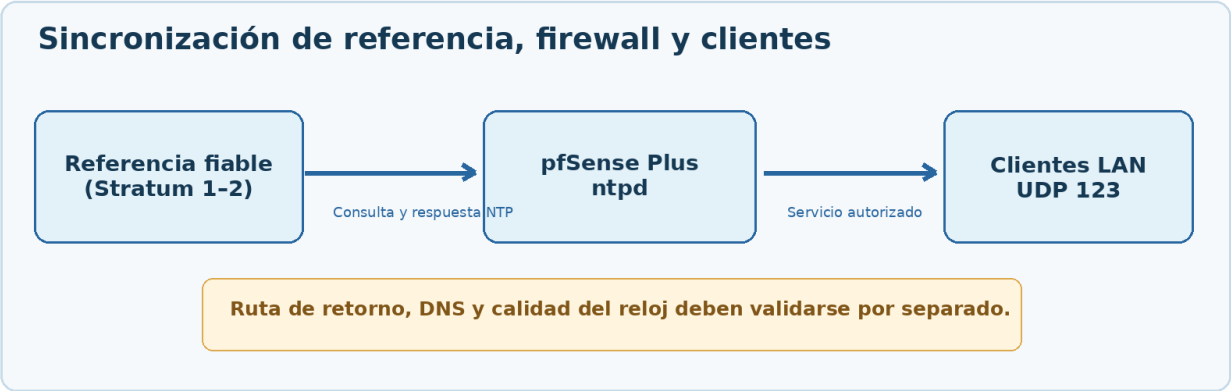


Figura 74.1. Recorrido de referencia temporal NTP desde fuentes externas hasta clientes autorizados de la red.

74.1. Finalidad, ubicación y límites de la pantalla

Ruta: Status → NTP. La pantalla informa sobre el daemon ntpd que mantiene el reloj del cortafuegos y, si así se configura, atiende consultas NTP de clientes locales. Es una vista de estado; la definición de servidores, interfaces, acceso y GPS corresponde a Services → NTP. [N1, N2]

Las filas representan asociaciones o fuentes conocidas por ntpd. Algunas son fuentes consultadas, otras son candidatos descartados y una entrada de pool puede ser únicamente un marcador dinámico. Los valores fluctúan por el intervalo de sondeo, cambios de calidad y selección del algoritmo. No deben tratarse como parámetros estáticos.

74.2. Qué observa el administrador: inventario de la interfaz

Zona / control visible	Función	Precaución de uso
Barra de navegación Status / NTP	Identifica la vista de diagnóstico de hora.	No cambia la configuración del servicio.
Reiniciar servicio (flecha circular)	Reinicia o recarga el daemon según implementación.	Puede interrumpir el servicio a clientes; usar en ventana controlada.
Detener servicio (cuadrado en círculo)	Detiene el daemon NTP en ejecución.	Los clientes dejarán de obtener hora del firewall.
Ajustes relacionados (deslizadores)	Abre Services → NTP.	Los cambios requieren analizar fuente, reglas y direcciones.
Acceso a registros (icono de lista)	Abre la vista de registros pertinente cuando está disponible.	Usar para correlacionar eventos y cambios.
Ayuda (? azul/rojo según tema)	Accede a ayuda vinculada con la pantalla.	No presupone un enlace externo permanente.
Tabla Network Time Protocol Status	Muestra estado y medidas por asociación NTP.	Puede desplazarse horizontalmente para ver columnas finales.

En esta versión de la interfaz los iconos de la cabecera representan accesos habituales documentados por Netgate. La disponibilidad exacta depende del estado del daemon, permisos y versión. [N3]

74.3. Fundamentos del protocolo NTP y papel del firewall

NTP utiliza habitualmente UDP/123 para intercambiar marcas de tiempo y estimar desfase y retardo de red. El servidor de pfSense conserva la hora del propio dispositivo a partir de fuentes elegidas. Una vez sincronizado, puede actuar como servidor horario para equipos autorizados; ese segundo papel exige configurar las interfaces de escucha y las políticas de firewall. [N2]

No debe confundirse la hora UTC que mantiene el sistema con la zona horaria empleada para presentarla en la GUI y los registros. Cambiar la zona horaria no equivale a sincronizar el reloj. Una desviación temporal relevante puede alterar Kerberos/AD, validación TLS, registros y tareas programadas.

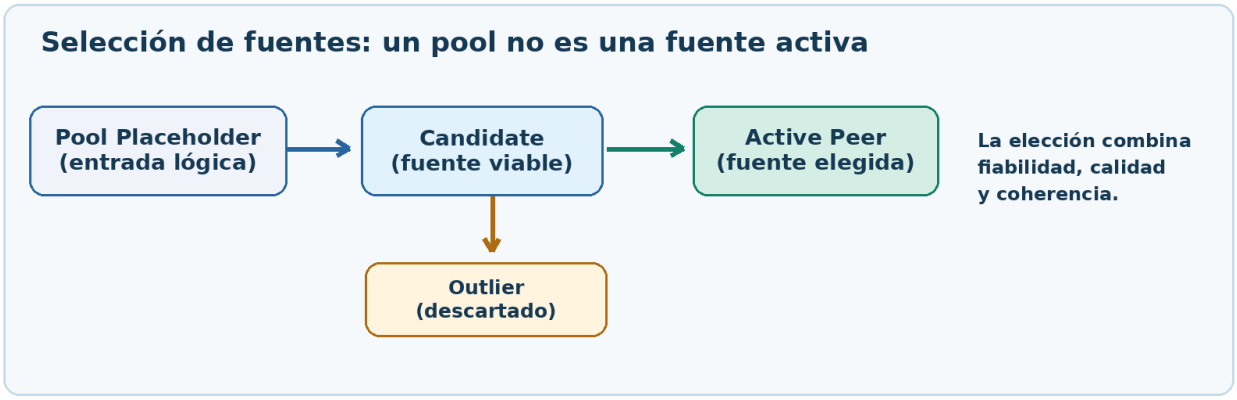


Figura 74.2. Diferencias conceptuales entre una entrada de pool, un candidato, una referencia activa y un outlier.

74.4. Lectura exhaustiva de columnas: identidad y calidad de fuente

Columna	Definición contrastada	Interpretación administrativa
Status	Clasificación de selección para el peer.	Comprobar Active Peer, Candidate, Outlier, Unreach/Pending y Pool Placeholder.
Server	IP o nombre de la fuente NTP, o FQDN del pool.	La identidad de un peer no implica que haya sido elegido.
Ref ID	Referencia que utiliza ese servidor: IP previa o código (.GPS., .POOL., .PPS.).	Sirve para conocer procedencia y evitar bucles; no es ID de asociación.
Stratum	Distancia lógica respecto a una referencia primaria.	1: reloj de referencia; 2–14: fuentes derivadas; 16: no sincronizado/marcador.
Type	Modo de asociación: u, p, l, b, s, etc.	u: unicast; p: pool; l: reloj local; b: difusión; s: simétrico.
When	Segundos transcurridos desde la última respuesta.	Un guion puede significar ausencia de respuestas; compararlo con Poll.
Poll (s)	Intervalo programado entre sondeos, en segundos.	Puede adaptarse dinámicamente; más corto no siempre es mejor.
Reach	Registro desplazable octal de las últimas ocho consultas.	377_8 indica ocho éxitos; 0 indica ausencia de éxito reciente.
Delay (ms)	Retardo ida/vuelta estimado hasta el par.	No confundir con latencia de ida o prueba ICMP.
Offset (ms)	Diferencia estimada entre la fuente y el reloj local.	El signo informa del sentido del ajuste; comparar tendencia y estabilidad.
Jitter (ms)	Estimación RMS de variabilidad del offset.	Jitter elevado puede indicar fuentes o red inestables.
AssocID	Identificador interno de la asociación de ntpd.	Sirve para diagnóstico con ntpq; no es un ID persistente del servidor.

Columna	Definición contrastada	Interpretación administrativa
Status Word	Palabra codificada de estado del peer, si se muestra.	Interpretar con la referencia de ntpd; no confundir con categoría Status.

En pantallas estrechas AssocID y Status Word pueden quedar a la derecha y requerir desplazamiento horizontal. La documentación de Netgate describe explícitamente las columnas hasta Jitter; AssocID/Status Word son campos adicionales visibles en la versión mostrada y se interpretan conforme a las herramientas ntpq y especificaciones NTP. [N1, N9, N10]

74.5. Estados de selección: qué significa cada uno

Estado	Significado	Acción razonable
Pool Placeholder	Marcador del pool; ntpd descubrirá pares por DNS.	No esperar tráfico propio ni interpretar su stratum 16 como fallo.
Unreach/Pending	Aún no hay suficientes respuestas o no hay acceso.	Esperar nuevos sondeos; comprobar DNS, rutas, UDP/123 y reach.
Active Peer	Fuente usada en la sincronización del reloj.	Verificar estabilidad con Reach, offset, jitter y registros.
Candidate	Fuente válida que podría ser elegida.	Conservar redundancia; no forzar selección por menor RTT.
PPS Peer	Fuente que utiliza una señal pulso por segundo.	Confirmar hardware y calidad de referencia.
Selected	Se incluye en el algoritmo de combinación.	Normal en una selección con múltiples fuentes.
Excess Peer	Válido, pero excede el conjunto utilizado.	No implica error de red.
False Ticker	Descartado por el algoritmo de intersección.	Buscar fuente divergente y comparar con otras.
Outlier	Descartado por el algoritmo de agrupamiento.	No necesariamente está fuera de servicio; revisar consistencia.

La fuente con RTT mínimo puede ser descartada si no concuerda con otras mediciones. Los algoritmos favorecen la consistencia temporal y la robustez frente a relojes erróneos, no únicamente la proximidad de red. [N1]

74.6. Reach: interpretación octal y evolución con los sondeos

Reach no es un porcentaje ni un contador acumulativo de disponibilidad. Es un registro de ocho bits mostrado en base ocho, que se desplaza en cada sondeo. A medida que llegan respuestas satisfactorias se observan valores como 1, 3, 7, 17, 37, 77, 177 y 377 (octal), si el historial empezó en cero. Un fallo provoca el desplazamiento sin establecer el bit del sondeo fallido.

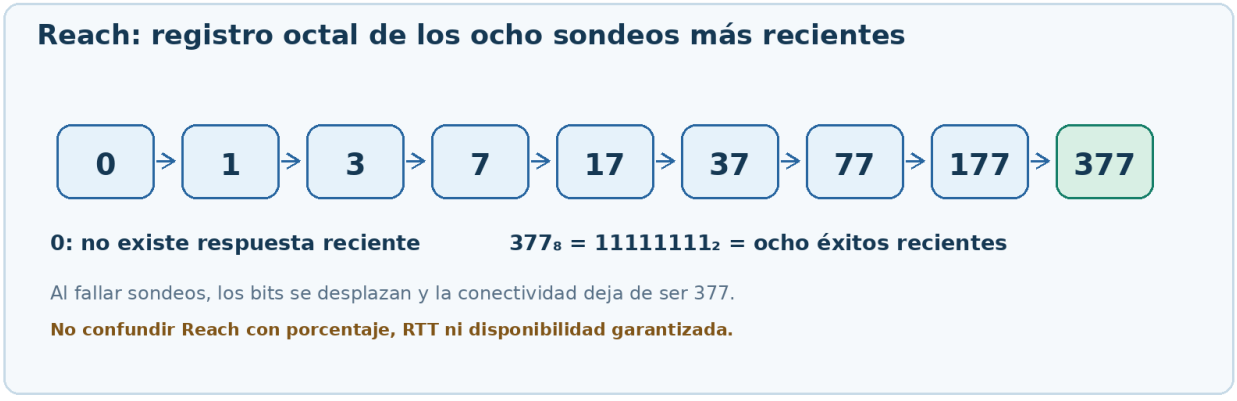


Figura 74.3. Secuencia didáctica de ocho respuestas NTP positivas y registro de alcanzabilidad en octal.

Reach (octal)	Lectura rápida	Límite de la interpretación
0	No se han registrado éxitos recientes.	Puede ser normal al inicio o en pool placeholder.
1, 3, 7, 17…	Secuencia reciente de respuestas que está creciendo.	No obliga a elegir esta fuente.
377	Ocho respuestas positivas de las ocho más recientes.	No demuestra exactitud del reloj ni salud continua.
Valores intermedios	Respuestas perdidas o recuperadas en las últimas ocho.	Analizar también Poll y When.

74.7. Delay, Offset y Jitter: tres magnitudes distintas

Delay es tiempo de ida y vuelta de los intercambios NTP. Offset es la estimación del desfase temporal entre el firewall y la fuente, obtenida a partir de las marcas de tiempo del protocolo; valores cercanos a cero son habituales en enlaces estables, pero no garantizan por sí solos precisión absoluta. Jitter refleja la variabilidad de sucesivas estimaciones de offset. [N1, N9]

Ejemplo completamente ficticio: Fuente A con delay 8 ms, offset +1,5 ms y jitter 0,4 ms puede ser mejor candidata que Fuente B con delay 3 ms, offset +180 ms y jitter 42 ms. Aun así, la selección depende de otras fuentes, dispersiones y reglas del algoritmo; no existe un umbral universal que garantice buena sincronización.

RECOMENDACIÓN Para diagnosticar una fuente irregular, comparar mediciones sucesivas durante varios intervalos Poll; no basar cambios permanentes en una sola lectura.

74.8. Stratum, Ref ID y Type: genealogía temporal

Elemento	Ejemplo documental	Lectura correcta
Stratum 1 + Ref ID .GPS.	clock-a.example.com (dato ficticio)	Servidor con referencia primaria GPS; no implica disponibilidad ni fiabilidad automática.
Stratum 2 + Ref ID 192.0.2.10	ntp-b.example.com (dato ficticio)	Servidor que toma referencia de otra fuente NTP.
Stratum 16 + Ref ID .POOL.	2.pfsense.pool.ntp.org (dominio público)	Marcador de pool, no peer sincronizado.
Type u	Asociación con fuente unicast.	Es habitual en servidores NTP consultados.
Type p	Entrada de pool.	Descubrimiento dinámico de otros peers.

El valor Stratum no es una escala lineal de calidad: un servidor Stratum 1 con señal defectuosa puede ser peor que un Stratum 2 estable. Lo crítico es la sincronización efectiva, la dispersión y la coherencia entre fuentes. [N1]

74.9. AssocID y Status Word: diagnóstico extendido

AssocID identifica la asociación NTP en la sesión de ejecución del daemon. Permite inspeccionar variables específicas desde ntpq. Status Word agrupa bits y campos codificados que describen configuración, alcanzabilidad, autenticación, selección y últimos eventos. El significado exacto debe contrastarse con la implementación y el formato usado; no es un código de error único ni el equivalente numérico de Active Peer. [N9, N10]

Cuando se necesita investigar un par concreto, identificar su AssocID y consultar ntpq -c associations seguido de ntpq -c "rv <ID>" en un entorno con acceso autorizado, donde <ID> representa el identificador real recuperado. Los IDs pueden variar después de reiniciar el servicio o redescubrir peers.

74.10. Controles de la barra: uso seguro

Control	Qué sucede	Recomendación operacional
Reiniciar NTP	Provoca reinicio del servicio (o recarga según mecanismo).	No usar como primera prueba; planificar en entornos críticos.
Detener NTP	Termina temporalmente el servicio de sincronización.	Puede dejar sin referencia a clientes LAN que consulten al firewall.
Settings	Navega a Services → NTP.	Revisar cambios antes de guardar/aplicar.
Logs	Acceso a eventos del daemon NTP.	Correlacionar con hora del sistema y red.
Help	Documentación de la pantalla.	Consultar diferencias entre versiones.

ADVERTENCIA Interrumpir ntpd afecta la disciplina de reloj del firewall y puede afectar a clientes que consuman NTP local. No diagnosticar un problema de ruta reiniciando de inmediato el servicio.

74.11. Dependencias: DNS, firewall, NAT, rutas y Multi-WAN

Si el servidor está definido mediante hostname o pool, el firewall necesita poder resolverlo. Si NTP sale por una WAN distinta, el origen de consulta, las reglas, los gateways y la ruta de retorno deben ser coherentes. En entornos Multi-WAN, una pérdida del enlace o una ruta asimétrica puede producir Reach bajo o fuentes Pending sin que ntpd sea el causante del fallo.

El tráfico NTP usa habitualmente UDP/123. Para clientes locales que consultan al firewall, deben existir reglas y escuchas adecuadas en interfaces internas. No debe exponerse de forma indiscriminada como servicio abierto a Internet. La opción Interface en Services → NTP influye también en el origen de consultas salientes cuando se restringe la vinculación del daemon. [N2]

74.12. Sistema horario: UTC, zonas e impacto en servicios

Un desfase real del reloj puede afectar a tokens, certificados, logs, gestión de identidades, comprobación de expiraciones y correlación SIEM. Una zona horaria visual equivocada produce marcas diferentes sin representar necesariamente una falta de sincronización NTP. Documentar UTC, zona, origen NTP y deriva observada por separado. [N8]

74.13. Recomendaciones para elegir fuentes y acceso

Netgate recomienda, para buen equilibrio de resiliencia, utilizar normalmente entre tres y cinco fuentes temporales bien elegidas, sin confundir un pool dinámico con una fuente estática única. Las fuentes deben ser independientes cuando sea posible y se recomienda verificar que los clientes utilicen solo servidores autorizados. [N2]

Decisión	Criterio técnico	Riesgo de una mala elección
Pool público	Adecuado si DNS y acceso externo son fiables.	Dependencia de DNS y conectividad externa.
Servidores corporativos	Útiles cuando hay política horaria centralizada.	Si todos dependen del mismo reloj, hay fallo común.
Fuentes GPS/PPS	Para requisitos especiales y hardware compatible.	GPS USB/serie puede introducir variaciones de calidad.
Una sola fuente	Sencillo, pero sin redundancia.	Difícil detectar si el reloj de esa fuente es erróneo.
NTP servido a LAN	Permite dar referencia local de forma controlada.	El firewall puede convertirse en dependencia crítica.

74.14. Procedimiento 1 — Validar sincronización sin cambios

1. Acceder a Status → NTP y anotar la hora de revisión y el estado general del servicio.
2. Localizar Active Peer; si no existe, esperar varios ciclos Poll antes de concluir un fallo.

3. Examinar Reach y comprobar que no decrezca repetidamente; no confundir Pool Placeholder con fuente real.
4. Comparar offset, jitter, delay y el estado de al menos dos peers alternativos.
5. Revisar Status → System Logs → NTP y registrar cualquier evento de pérdida o cambio de fuente.
6. Contrastar la fecha/hora del firewall y los sistemas consumidores con una referencia autorizada.

74.15. Procedimiento 2 — Diagnosticar todos los peers en Pending

1. Confirmar que NTP está en ejecución mediante Status → Services y Status → NTP.
2. Si se usan nombres, comprobar resolución DNS desde el firewall y verificar rutas y gateways.
3. Revisar reglas de salida y estado de interfaces; probar conectividad UDP/123 con capturas de paquetes cuando sea necesario.
4. Observar si salen consultas y vuelven respuestas sin exponer el tráfico ni modificar el firewall.
5. Confirmar en Services → NTP que los servidores y la vinculación a interfaces son coherentes con el diseño.
6. Únicamente después de identificar la causa, aplicar una modificación controlada y verificar recuperación de Reach.

74.16. Procedimiento 3 — Offset o jitter persistente alto

1. Comparar al menos tres fuentes e identificar valores aislados frente a desplazamiento común.
2. Comprobar pérdida, jitter de red, rutas cambiantes o saturación WAN.
3. Revisar reloj de hardware, BIOS/UEFI, entorno virtualizado y cambios de zona horaria.
4. Consultar registros de NTP para saltos importantes de tiempo y eventos de selección.
5. Corregir la causa y monitorizar la estabilización durante varios sondeos, documentando resultados.

74.17. Procedimiento 4 — Comprobar el servicio a clientes LAN

1. Identificar el segmento autorizado y las interfaces de escucha en Services → NTP.
2. Comprobar que los clientes consultan la dirección prevista del firewall y que existe una regla adecuada.
3. Desde un equipo de laboratorio, realizar una consulta al servidor NTP y verificar que responde con tiempo válido.
4. Corroborar que el firewall tiene Active Peer o dispone de una política corporativa explícita de referencia local.
5. Validar que no se ha permitido acceso no autorizado a UDP/123 por WAN.

74.18. Comandos de observación avanzados

Comando de referencia	Propósito	Precaución
ntpq -pn	Lista peers sin resolver nombres; útil para aislar problemas DNS.	Puede no estar disponible con otras implementaciones NTP.
ntpq -c associations	Lista asociaciones y estados internos.	Los IDs no son estables tras reinicios.
ntpq -c rv	Muestra variables del reloj local/daemon.	Interpretar root delay/dispersion con referencia documental.
ntpq -c "rv <ID>"	Inspección de una asociación concreta.	Sustituir <ID> por AssocID vigente; no usar los signos literales.
tcpdump -ni <interfaz> udp port 123	Comprueba solicitudes y respuestas NTP en la interfaz elegida.	Solo en diagnóstico autorizado; controlar volumen de capturas.

Los comandos son ejemplos de ntpd/FreeBSD y pueden depender del firmware y herramientas instaladas. La alternativa de GUI para comprobar tráfico es Diagnostics → Packet Capture. No se requiere ni se recomienda activar el acceso de control NTP desde redes no fiables. [N9]

74.19. Matriz de incidentes, causas y acciones

Síntoma	Posibles causas	Validación previa / respuesta
Pool Placeholder con stratum 16	Entrada lógica de pool.	Buscar peers descubiertos; no tratar como avería.
No aparece Active Peer	Arranque reciente, sin fuentes fiables, hora muy desviada.	Observar ciclos; revisar DNS, Reach, logs y hora de sistema.
Todos los peers Reach 0	DNS, WAN, firewall, bloqueo UDP/123 o servicio.	Captura NTP en interfaz de salida y revisión de rutas.
Hay Candidate pero no Active Peer	Fuente no seleccionada aún, condiciones de calidad.	Consultar mensajes del daemon; no forzar cambios sin datos.
Outliers frecuentes	Fuentes discordantes, ruta variable, hardware.	Comparar deriva de varias fuentes durante suficiente tiempo.
Offset sube lentamente	Reloj local inestable, virtualización, mala referencia.	Verificar clock source, firmware, CPU y registros.
Jitter alto solo en WAN secundaria	Pérdidas y variación de retardo.	Correlacionar gateway, WAN y NTP con capturas.
Firewall sincroniza, clientes no	Interfaz de escucha o reglas LAN.	Verificar consulta desde cliente sin abrir UDP/123 a WAN.
Hora mostrada desplazada 1–2 horas	Zona horaria/DST mal seleccionada.	Verificar UTC y configuración horaria; no reiniciar NTP sin motivo.

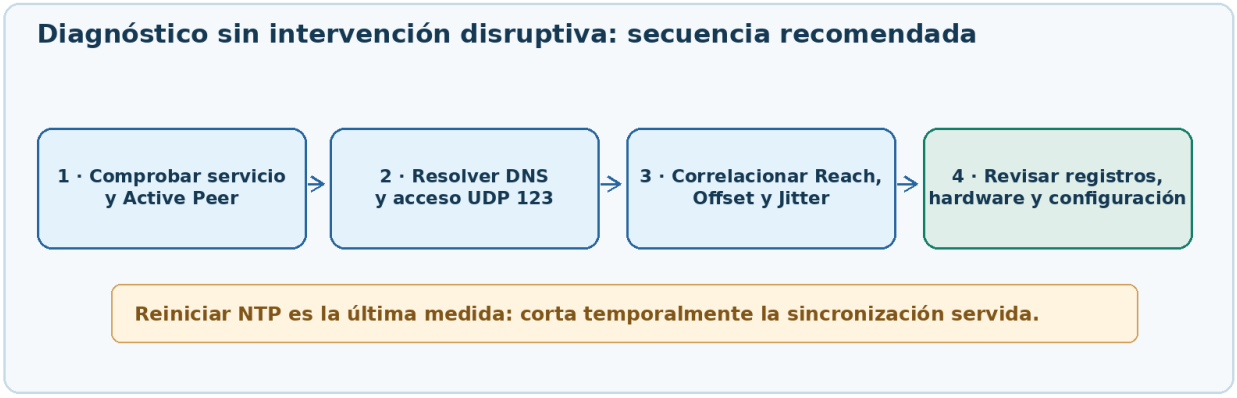


Figura 74.4. Árbol de revisión operacional de NTP, priorizando observación antes de acciones disruptivas.

74.20. Escenario profesional A — Red corporativa con autenticación centralizada

Un firewall ofrece NTP a clientes de una VLAN administrativa; servidores de identidad y estaciones requieren coherencia temporal. Diseño recomendado: fuentes externas verificadas, escucha interna restringida, registros NTP habilitados y comprobaciones después de cambios WAN. Validación: Active Peer estable, Reach alto en varias fuentes y clientes capaces de consultar al firewall.

74.21. Escenario profesional B — Doble WAN con enlace de contingencia

El enlace principal falla y NTP continúa usando una ruta incorrecta. Se inspeccionan las asociaciones y el gateway efectivo, se correlacionan pérdidas y cambios de RTT con la ruta WAN y solo entonces se ajusta el enlace o regla de salida correspondiente. La selección de fuentes NTP no sustituye la política de routing.

74.22. Escenario profesional C — Aislamiento o conectividad exterior limitada

Una sede técnica con escaso acceso externo requiere mantener hora coherente para logs y servicios. Debe definirse una referencia interna fiable, no asumir que Orphan Mode sustituye a una fuente exacta. Orphan Mode puede preservar continuidad de servicio horario ante ausencia de upstream, pero la precisión absoluta puede degradarse y debe documentarse. [N2]

74.23. Escenario profesional D — Servidor horario con GPS/PPS

En instalaciones especializadas pueden emplearse referencias GPS/PPS habilitadas en Services → NTP. Verificar calidad de la señal, conexiones, jitter de hardware y que no se priorice un GPS defectuoso frente a otras fuentes. La documentación señala que el adaptador USB-serie puede generar incertidumbre de temporización mayor que un puerto serie convencional. [N1]

74.24. Seguridad del servicio de tiempo

La alteración maliciosa de la hora puede repercutir en TLS, autenticación, auditoría y sistemas de monitorización. Limitar el acceso entrante a NTP, gestionar fuentes confiables y monitorizar cambios inesperados de offset. No asumir que el protocolo NTP básico garantiza autenticación criptográfica por defecto; las opciones de autenticación disponibles dependen de la versión y del diseño.

74.25. Buenas prácticas de explotación y disponibilidad

Registrar qué servidores externos e internos se usan y quién gestiona los cambios.

Observar al menos dos fuentes utilizables, con redundancia y límites explícitos de aceptación.

Comparar valores en varios sondeos y evitar interpretar una única lectura aislada.

Correlacionar eventos del servicio con cambios de WAN, DNS, virtualización y cortes de energía.

Documentar las consecuencias de detener NTP si el firewall sirve hora a clientes locales.

Evitar reinicios de NTP o cambios de configuración durante una investigación forense salvo necesidad justificada.

74.26. Glosario operativo

Término	Definición aplicada a la supervisión
NTP	Protocolo de sincronización temporal que intercambia marcas de tiempo.
Peer	Fuente o asociación de sincronización conocida por el daemon.
Stratum	Nivel lógico de separación respecto a un reloj de referencia.
Offset	Diferencia estimada entre reloj local y referencia temporal.
Delay	Retardo de ida y vuelta medido por el intercambio NTP.
Jitter	Variabilidad de offset entre muestras.
Reach	Registro octal de ocho resultados de sondeo.
AssocID	Identificador interno de una asociación NTP.
PPS	Pulso por segundo utilizado como referencia temporal.
Outlier	Fuente descartada por el algoritmo de agrupamiento.

74.27. Ficha de evidencias y verificación periódica

Dato a registrar	Cómo obtenerlo	Objetivo operativo
Fecha/hora y zona	System Information / GUI.	Correlación trazable de eventos.
Fuente Active Peer	Status → NTP.	Verificar referencia principal.
Reach / Poll / When	Status → NTP / ntpq.	Detectar pérdidas y falta de respuestas.
Offset / Jitter / Delay	Status → NTP.	Evaluar estabilidad temporal.
Cambios de fuente	NTP logs / revisión periódica.	Detectar fallos intermitentes.

Dato a registrar	Cómo obtenerlo	Objetivo operativo
Relación con gateways	Status → Gateways.	Correlacionar cambios WAN y calidad de reloj.
Prueba de clientes	Consulta NTP autorizada en LAN.	Confirmar servicio completo a consumidores.

Rutina de mantenimiento sugerida: comprobar periódicamente el Active Peer, revisar una muestra de Reach y offset en fuentes alternativas, inspeccionar eventos anómalos y documentar si hay alteraciones relevantes tras mantenimiento, cambios WAN o actualizaciones. La periodicidad depende de la criticidad de los servicios.

74.28. Referencias técnicas verificables

Netgate · estado y servicio	Netgate · operación	NTP · IETF · referencia
[N1] NTP Daemon Status	[N6] NTP service overview	[N10] NTP — Event Messages and Status Words
[N2] NTP Server Configuration	[N7] NTP status dashboard widget	[N11] RFC 5905 · Network Time Protocol Version 4
[N3] GUI shortcut icons	[N8] General Configuration, Time Zone	[N12] RFC 9327 · NTPv4 Control Messages
[N4] Troubleshooting Clock Issues	[N9] NTP — ntpq manual	[N13] NTP metrics in RRD graphs
[N5] NTP Logs		

75 Status → OpenVPN

Supervisión de túneles · instancias cliente y servidor · contadores · acciones de servicio · diagnóstico

La vista Status → OpenVPN reúne el estado de las instancias OpenVPN y permite diferenciar la salud del proceso, la sesión negociada y el tráfico útil que atraviesa la red. Esta distinción evita decisiones precipitadas durante una incidencia y permite documentar el estado de los túneles de acceso remoto y entre sedes.

IDEA CENTRAL Connected (Success) indica que OpenVPN ha establecido la sesión según su estado interno, pero no certifica que todos los destinos, servicios o rutas de retorno funcionen. Correlacionar siempre estado, logs, rutas, firewall y pruebas extremo a extremo.

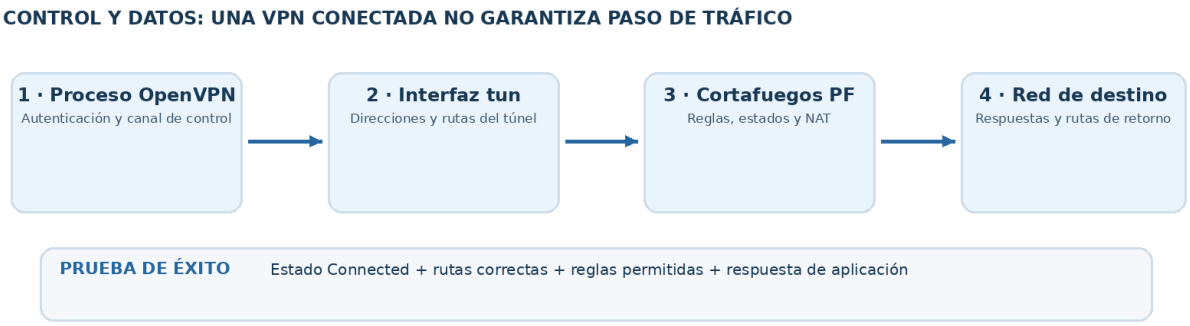


Figura 75.1. Relación entre el establecimiento del túnel y el recorrido real del tráfico.

75.1. Objetivo de Status → OpenVPN y ruta de acceso

Ruta de administración: Status → OpenVPN. El contenido depende de si pfSense actúa como servidor, cliente o ambos y del modo de OpenVPN: SSL/TLS con múltiples clientes o peer-to-peer. Cada instancia puede disponer de controles de servicio propios, evitando tener que reiniciar indiscriminadamente todas las VPN.

La pantalla es de supervisión y administración operativa. Las opciones de servidor, cliente, certificados, cifrado, redes y tiempos de ping se editan en VPN → OpenVPN, no en la tabla de estado. La presencia de una fila no convierte por sí misma la VPN en una ruta válida de producción.

75.2. Inventario de elementos y controles visibles

Elemento	Propósito	Precaución
Ruta Status / OpenVPN	Identifica la página de supervisión de OpenVPN.	No cambia la configuración.
Icono de ajustes (deslizadores)	Acceso a la configuración relacionada con el servicio.	Revisar qué instancia se edita.
Icono de registros	Acceso a System Logs → OpenVPN.	Los eventos pueden contener identidad técnica; tratar como evidencia reservada.
Icono de lista / estado	Acceso de navegación contextual a páginas de estado relacionadas.	La disponibilidad varía según versión.
Ayuda (?)	Abre ayuda o documentación contextual.	Puede diferir entre versiones.
Client Instance Statistics	Tabla de instancias cliente configuradas.	No equivale a una prueba de conectividad de red.
Service	Indicador y controles por instancia.	Reiniciar o detener interrumpe la sesión.

Los atajos situados en la barra superior siguen el patrón general de Netgate para navegación a configuración, registros y estado. Los iconos concretos y su disponibilidad pueden variar por versión y permisos.

75.3. Lectura detallada de Client Instance Statistics

Columna	Significado	Lectura correcta
Name	ID interna (por ejemplo, ovpnc1), descripción y protocolo/puerto de la instancia.	No confundir ovpnc1 con un adaptador WAN ni con la identidad del cliente remoto.
Status	Estado de la instancia y, cuando hay información, éxito de la conexión.	Connected no garantiza rutas, DNS ni respuesta desde la LAN remota.
Last Change	Fecha y hora del último cambio de estado conocido.	No es tiempo de actividad garantizado; correlacionar con logs y zona horaria.
Local Address	Dirección y puerto locales usados por la conexión.	Puede reflejar una IP privada detrás de NAT; no necesariamente la IP pública.
Virtual Address	Dirección o dato de interfaz virtual informado por OpenVPN.	La forma concreta depende del modo; verificar dirección real y rutas.
Remote Host	Extremo remoto de transporte, con puerto.	Un puerto no estándar es válido si coincide y está autorizado.
Bytes Sent	Bytes enviados desde el contexto de la instancia pfSense.	Contador acumulado del periodo visible, no tasa instantánea.
Bytes Received	Bytes recibidos por la instancia pfSense.	Un valor no nulo no demuestra que un servicio concreto funcione.
Service	Estado del proceso y controles de gestión.	Afecta al túnel asociado; comprobar dependencia de sedes antes de actuar.



Figura 75.2. Guía de lectura por bloques de las columnas de las instancias cliente.

75.4. Interpretar la identidad de instancia y los extremos

Un nombre como ovpnc1 identifica una instancia OpenVPN cliente dentro de pfSense; el identificador no prueba por sí solo qué interfaz WAN utiliza. La descripción es una etiqueta de administración. UDP4, por ejemplo, indica uso de UDP sobre IPv4. El par Local Address y Remote Host identifica el transporte exterior, mientras que Virtual Address se refiere al lado del túnel. Deben evitarse conclusiones basadas exclusivamente en una dirección de estas columnas.

Ejemplo totalmente ficticio: una instancia denominada VPN-Laboratorio podría conectarse desde 192.0.2.25:49152 hacia 203.0.113.20:1194 mediante UDP; la dirección interna del túnel pertenece a otro espacio de direccionamiento. 192.0.2.0/24 y 203.0.113.0/24 son rangos reservados para documentación, no direcciones de la instalación descrita.

75.5. Estados de conexión: conexión, espera y reconexión

Estado o situación	Interpretación	Siguiente comprobación
Connected (Success)	La instancia informa de establecimiento satisfactorio.	Probar ping/traza con origen correcto y servicio real.
Waiting / Listening	Proceso servidor preparado, sin cliente remoto confirmado.	Comprobar si se espera conexión y revisar intento de cliente.
Reconnecting / Connecting	Intenta establecimiento o restablecimiento.	Revisar OpenVPN logs, red WAN y autenticación.

Estado o situación	Interpretación	Siguiente comprobación
Stopped / Disabled	Instancia no ejecutándose o deshabilitada.	Ver configuración y motivo antes de iniciarla.
Sin fila o estado incompleto	No hay instancia visible o información del proceso.	Comprobar configuración, estado de servicios y logs.

Los nombres exactos y el nivel de detalle pueden diferir con la versión de OpenVPN y de pfSense. En particular, los modos punto a punto disponen de menos información de conexión que un servidor SSL/TLS con clientes individuales.

75.6. Análisis de los contadores Bytes Sent y Bytes Received

Son contadores en unidades de almacenamiento (KiB, MiB, GiB), no medidas instantáneas de velocidad en bit/s. La interpretación debe hacerse desde la perspectiva de la instancia de pfSense. Un aumento solo en un sentido puede indicar respuesta ausente, ruta de retorno errónea, bloqueo por firewall o simplemente comportamiento asimétrico normal de la aplicación.

Los contadores pueden reiniciarse tras una reconexión, un reinicio de servicio o cambios del proceso, por lo que no deben usarse como estadísticas históricas de facturación. Para estimar velocidad, registrar dos muestras comparables y calcular la diferencia de bytes dividida por segundos; multiplicar por ocho para expresarlo en bit/s.

LIMITACIÓN DCO Según la documentación vigente de Netgate, el uso de OpenVPN Data Channel Offload puede hacer que las estadísticas por peer en Status → OpenVPN no reflejen correctamente los bytes reales transferidos. No confundir cifras bajas con ausencia de tráfico.

75.7. Botones Service: ejecución, reinicio y parada

Indicador/acción	Función	Impacto operativo
Indicador verde	Confirma que el servicio o instancia se informa como ejecutándose.	No prueba que el extremo remoto responda.
Restart (flecha circular)	Reinicia o recarga la instancia según el servicio.	Interrumpe sesiones y renegocia el túnel.
Stop (círculo/cuadrado)	Detiene la instancia.	Corta el acceso hasta nuevo inicio o restablecimiento.
Start (cuando aparece)	Inicia una instancia que está detenida.	Puede recuperar operación si la causa se ha solucionado.



Figura 75.3. Alcance de acciones sobre instancias y sesiones, con sus precauciones.

INTERRUPCIÓN DE SERVICIO Antes de seleccionar Restart o Stop en una VPN entre sedes, confirmar un acceso administrativo alternativo. Si la administración remota usa el propio túnel, el cambio puede desconectar al operador e impedir la recuperación inmediata.

75.8. Diferencia entre reiniciar una instancia y desconectar una sesión

Restart y Stop pertenecen al control del servicio OpenVPN y afectan a una instancia completa. En un servidor SSL/TLS de acceso remoto, las acciones de una fila de cliente pueden cerrar únicamente su sesión. Netgate diferencia Clear Client Session (desconecta permitiendo reconexión) y Halt Remote Client (solicita al extremo remoto detener su proceso, si lo admite). No son acciones equivalentes.

75.9. Supervisión de servidores SSL/TLS con varios clientes

Cuando un servidor SSL/TLS utiliza una red de túnel capaz de alojar múltiples clientes, la vista muestra un bloque con nombre de interfaz ovpnsN, descripción, protocolo/puerto y total de clientes, seguido de conexiones individuales. Esta presentación no es la misma que la de una instancia peer-to-peer.

Campo en servidor	Información mostrada	Observación
Common Name	Nombre común del certificado y/o usuario autenticado.	Depende de modo TLS, autenticación y Username as Common Name.
Real Address	Origen exterior del cliente visto por el servidor.	Puede corresponder a CGNAT o VPN de acceso exterior.
Virtual Address	IPv4/IPv6 asignadas al cliente dentro del túnel.	No equivale a la IP física del equipo.
Connected Since	Momento de conexión o último cambio informado.	Contrastar con registros si hay reconexiones.
Bytes Sent / Received	Tráfico en el contexto del servidor hacia/desde el cliente.	Puede ser inexacto por peer con DCO.
Ciphers	Cifrado negociado y utilizado para esa sesión.	Puede diferir entre clientes por negociación.
Actions	Desconexión, halt remoto e información condicional.	Impacto por usuario o sesión: aplicar con cautela.

75.10. Botones específicos en servidores de acceso remoto

Netgate documenta Clear Client Session, Halt Remote Client y Show Routing Table para servidores SSL/TLS con clientes individuales. Show Routing Table presenta las redes y direcciones conocidas a través de cada cliente, útil para análisis de escenarios site-to-site con múltiples peers. Puede aparecer un icono adicional de información si la conexión usa RADIUS y recibe reglas personales de firewall.

MODOS DE OPENVPN Una instancia cliente presenta información distinta de un servidor de acceso remoto. El cierre de sesiones de usuarios y las tablas de rutas del servidor corresponden a los modos que ofrecen esas funciones. Comprobar el tipo de instancia antes de interpretar sus controles.

75.11. Modo Peer-to-Peer: particularidades de la supervisión

En modo peer-to-peer, incluida la configuración SSL/TLS con red /30, OpenVPN presenta una fila por instancia cliente o servidor y no dispone del inventario detallado de clientes que ofrece el modo de acceso remoto. El servidor puede mostrar que está esperando o que un peer está conectado; el cliente puede mostrar conexión pendiente o activa.

Una instancia peer-to-peer puede informar correctamente de enlace establecido, aunque falten rutas para redes internas. Esta modalidad no dispone del mismo mecanismo de distribución de parámetros a clientes que el modo SSL/TLS multiusuario, por lo que hay que revisar explícitamente ambos extremos.

75.12. Cruzar Status → OpenVPN con otras vistas

Vista relacionada	Qué verifica	Pregunta que resuelve
Status → System Logs → OpenVPN	Negociación, errores TLS, reinicios, autenticación.	¿Por qué no se establece o se reinicia?
Status → System Logs → Firewall	Bloqueos al puerto WAN o al tráfico dentro del túnel.	¿Se bloquea la conexión o tráfico de usuario?
Diagnostics → Routes	Rutas del sistema hacia redes remotas.	¿El tráfico saldrá por la interfaz esperada?
Diagnostics → Ping / Traceroute	Conectividad real con origen conocido.	¿El otro extremo responde de ida y vuelta?
Diagnostics → Packet Capture	Tráfico en WAN, tun y LAN.	¿En qué interfaz deja de avanzar?
Status → Gateways	Salud del enlace WAN y calidad de transporte.	¿El fallo está en el acceso exterior?

Vista relacionada	Qué verifica	Pregunta que resuelve
Status → Dashboard / Services	Estado agregado de servicio y recursos.	¿La instancia y el firewall están sanos?

75.13. Procedimiento 1. Verificar una instancia conectada sin cambiar nada

- Abrir Status → OpenVPN y localizar la instancia por su descripción administrativa, no solo por ovpncN.
- Anotar en el parte técnico Status, Last Change y contadores de envío y recepción, con fecha y zona horaria.
- Abrir Status → System Logs → OpenVPN y correlacionar la conexión con la negociación registrada.
- Verificar Diagnostics → Routes para confirmar la red remota y la interfaz tun correspondiente.
- Realizar ping o traza desde el firewall con un origen adecuado hacia un destino autorizado, y comprobar una aplicación real.
- Si falla, seguir con la inspección de firewall y captura de paquetes sin reiniciar la instancia inicialmente.

75.14. Procedimiento 2. Diagnosticar una VPN que aparece Connected pero no comunica

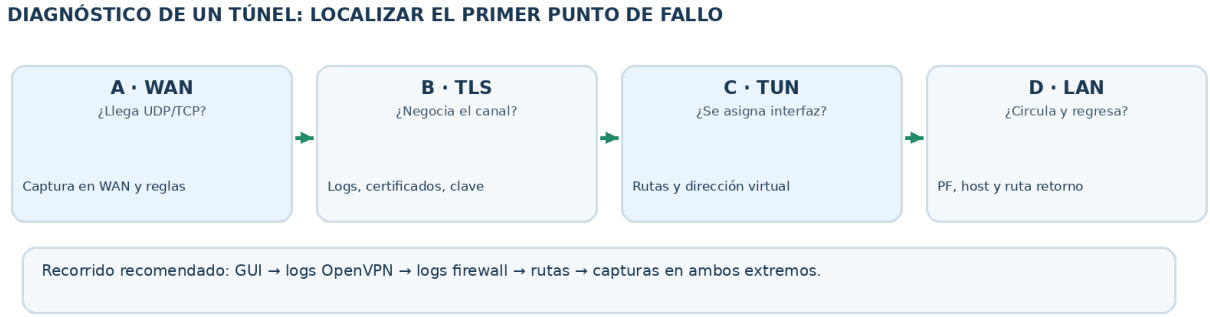


Figura 75.4. Secuencia de diagnóstico por capas desde WAN hasta red de destino.

- Probar el extremo del túnel y después un host de la LAN remota; distinguir fallo de transporte de fallo de encaminamiento.
- Revisar redes remotas configuradas, rutas locales y rutas de retorno del sitio contrario.
- Verificar las reglas en Firewall → Rules → OpenVPN o en la interfaz asignada, según el diseño.
- Descartar solapamientos de subred y políticas SPD IPsec que coincidan con la misma pareja local/remota.
- Si persiste la incidencia, capturar tráfico en LAN, tun y WAN; repetir el proceso en el extremo remoto.
- Documentar el primer punto donde desaparecen los paquetes y corregir solo la regla, ruta o componente responsable.

75.15. Procedimiento 3. Investigar reconexiones y caídas periódicas

- Comparar las marcas de Last Change con los registros de OpenVPN y de gateways.
- Consultar eventos de timeout, ping-restart, pérdida de red o cambio de interfaz WAN.
- Verificar que la ruta al servidor remoto sigue el enlace correcto en entornos Multi-WAN.
- Comprobar si el servidor o cliente remotos realizan mantenimiento, actualizaciones o renovaciones de certificados.
- Revisar el impacto de keepalive y ping-restart, evitando tiempos demasiado agresivos que creen reconexiones innecesarias.
- Solo después de identificar la causa, realizar cambios en una ventana acordada y validar permanencia del túnel.

75.16. Procedimiento 4. Reiniciar una sola instancia de forma segura

- Confirmar que existe conectividad administrativa independiente del túnel afectado.
- Verificar qué servicios dependen de esa instancia y establecer una ventana de intervención.
- Guardar evidencias de estado y últimos mensajes de log antes del cambio.
- Aplicar Restart únicamente a la instancia identificada, no al conjunto de VPN.
- Seguir su paso por Connecting o Reconnecting hasta Connected (Success), cuando proceda.
- Validar rutas, DNS y aplicaciones, y registrar cualquier variación de tráfico.

NO NORMALIZAR REINICIOS Reiniciar reiteradamente una VPN sin comprender el fallo puede ocultar síntomas, alterar evidencias y cortar producción. El estado debe verificarse antes y después de la acción.

75.17. Procedimiento 5. Inspección CLI y obtención de evidencias

En una consola autorizada, la consulta de registros con tail permite observar eventos sin alterar la sesión. Netgate documenta el siguiente ejemplo; comprobar que el archivo es el utilizado por la versión instalada:

```
tail -F /var/log/openvpn.log
```

También es posible operar una instancia por medio de pfSsh.php playback svc, pero estas órdenes sí modifican el servicio. Ejemplo de la sintaxis documentada:

```
pfSsh.php playback svc restart openvpn client 2
```

El número es un identificador de ejemplo. Nunca ejecutar órdenes de reinicio copiadas de un libro sin revisar la correspondencia exacta con la instancia actual y el impacto en sesiones activas.

75.18. Escenario empresarial 1. VPN site-to-site entre dos sedes

Dos redes empresariales intercambian servicios a través de un túnel OpenVPN, usando un firewall como cliente y otro como servidor. La pantalla marca Connected y los bytes transmitidos aumentan, pero un equipo de la sede remota no responde. La verificación de rutas, reglas LAN/OpenVPN y gateway del host permite encontrar problemas de retorno que el estado del túnel por sí solo no revela.

75.19. Escenario empresarial 2. Acceso remoto de usuarios

Un servidor SSL/TLS recibe clientes con certificados y, opcionalmente, autenticación de usuario. El administrador observa Common Name, Real Address y Connected Since. Si una sesión se queda bloqueada, puede desconectarla individualmente sin detener el servicio ni afectar al resto de usuarios, siempre tras confirmar cuál es el cliente correcto.

75.20. Escenario empresarial 3. Multi-WAN y resiliencia del cliente

Una instancia cliente usa un enlace principal y una segunda salida de respaldo. En un grupo de gateways exclusivo de failover, la salida puede cambiar de WAN según su nivel de disponibilidad; la transición implica renegociación y puede generar corte temporal. En ocasiones una ruta estática hacia el host remoto será necesaria para fijar el enlace esperado.

La asociación de OpenVPN a un grupo de gateways no convierte el propio túnel en un mecanismo de balanceo de sesiones simultáneas. Netgate diferencia expresamente failover y load balancing, y aconseja grupos con un gateway por tier para el caso de OpenVPN.

75.21. Escenario empresarial 4. Anomalías de estadísticas con DCO

En pfSense Plus con DCO, algunos contadores por peer pueden no representar todo el volumen cifrado que circula realmente. Si una aplicación funciona y los contadores visibles parecen bajos, deben corroborarse con la monitorización del interfaz y los registros. Esta limitación depende de la implementación y su estado puede evolucionar con las versiones.

75.22. Matriz de incidencias de supervisión OpenVPN

Síntoma	Causas probables	Prueba prioritaria
No hay instancia visible	Servicio no configurado, deshabilitado o modo diferente.	VPN → OpenVPN y Status → Services.

Síntoma	Causas probables	Prueba prioritaria
Connecting recurrente	Fallo de red, DNS, firewall WAN o extremo remoto.	OpenVPN logs, DNS, captura WAN.
TLS handshake fallido	CA, certificado, tls-auth/crypt o parámetros incompatibles.	Comparar logs de ambos extremos y vigencia de certificados.
Connected sin acceso	Ruta ausente, regla PF, NAT o retorno incorrectos.	Rutas, captura tun/LAN, firewall.
Solo funciona un destino	Host firewall, máscara errónea o ruta selectiva.	Captura en destino y ruta de retorno.
Contadores no crecen	Sin uso real, sesión recién reiniciada o límite DCO.	Probar tráfico controlado y medir interfaz.
Caídas periódicas	Keepalive, fluctuación WAN, Multi-WAN o peer remoto.	Correlacionar timestamps de OpenVPN y Gateways.
Sedes con mismas redes	Solapamiento de subredes/rutas.	Comparar prefijos y políticas NAT.
Conecta, pero DNS no resuelve	DNS no propagado o no alcanzable dentro del túnel.	nslookup/dig con servidor autorizado.
Una sesión conflictiva	Certificados reutilizados o identidades duplicadas.	Lista de clients y Common Name.

75.23. Consideraciones de seguridad y protección de evidencias

- Nunca publicar capturas de Status → OpenVPN con nombres reales de instancias, direcciones IP, identidades de usuarios o identificadores de dispositivo.
- Evitar compartir archivos de configuración y logs completos sin revisar claves, rutas de certificación y datos de conexión.
- Usar cuentas y certificados diferenciados para los distintos clientes; evitar certificados compartidos.
- Seleccionar algoritmos vigentes y mantener las fechas/horas del sistema sincronizadas para facilitar validación y correlación.
- Registrar toda acción de parada o reinicio, su causa y la persona autorizada a ejecutarla.
- Mantener rutas de acceso administrativo alternativas a una VPN crítica para poder recuperar servicio.

75.24. Rendimiento, tiempos y retención de evidencias

Las cifras de Bytes Sent y Bytes Received deben interpretarse junto con Monitor/Traffic Graph, utilización de CPU, pérdida de paquetes y contexto temporal. Una VPN puede tener una sesión estable pero rendimiento bajo por ancho de banda, latencia, MTU/MSS, características criptográficas o limitaciones de hardware.

Los logs pueden rotar o perder detalle con el tiempo. Para una incidencia, conservar ventana temporal, zona horaria, versión de pfSense/OpenVPN, estado de gateway, rutas y observaciones antes de hacer un cambio. Las capturas deben anonimizarse antes de integrarlas en informes externos.

75.25. Relación con el capítulo de configuración VPN → OpenVPN

El capítulo 60 desarrolla la creación de instancias, certificados, cifrados y parámetros de OpenVPN. Status → OpenVPN no sustituye aquellas tareas, sino que es el punto de observación operativo. Cada ajuste en servidor, cliente o Client Specific Override debe validarse aquí, en los registros y en las redes de usuario implicadas.

75.26. Ficha de aceptación de una VPN en producción

Control	Criterio de validación	Evidencia a conservar
Proceso	Instancia arrancada sin error recurrente.	Estado y hora.
Negociación	TLS y canal de datos establecidos.	Evento de logs.
Enrutamiento	Rutas remotas presentes y correctas.	Tabla de rutas anon.

Control	Criterio de validación	Evidencia a conservar
Filtrado	Reglas permiten solo flujos necesarios.	Reglas verificadas sin secretos.
Conectividad	Aplicaciones reales responden en ambos sentidos.	Resultado de prueba.
Continuidad	Sin reconexiones imprevistas en ventana de observación.	Intervalo y registros.
Recuperación	Procedimiento de rollback y acceso alternativo.	Referencia al plan de cambio.

75.27. Glosario de términos esenciales

Término	Significado práctico
ovpncN / ovpnsN	Identificadores internos de instancias cliente/servidor.
tun / tap	Adaptador virtual de nivel 3 / nivel 2, según configuración.
Peer	Extremo participante en la conexión VPN.
Handshake TLS	Intercambio para autenticación y establecimiento del canal de control.
Common Name	Nombre común del certificado, potencial identidad de cliente.
DCO	Data Channel Offload: procesamiento de datos OpenVPN en el kernel, con restricciones.
Last Change	Último cambio reportado para el estado de una instancia.
Split Tunnel	Solo ciertas redes se encaminan por VPN.
Full Tunnel	El tráfico general del cliente se dirige por el túnel, si rutas y reglas lo implementan.
Keepalive	Mensajes y temporizadores para mantener y evaluar la conexión.

75.28. Referencias técnicas oficiales

01. Netgate — OpenVPN Server and Client Status
02. Netgate — Troubleshooting OpenVPN
03. Netgate — OpenVPN Logs
04. Netgate — Service Status
05. Netgate — GUI Shortcuts
06. Netgate — OpenVPN and Multi-WAN
07. Netgate — OpenVPN Data Channel Offload (DCO)
08. Netgate — OpenVPN Ping Settings
09. Netgate — OpenVPN Advanced Options
10. Netgate — OpenVPN Endpoint Configuration
11. Netgate — PHP Shell and service playback
12. Netgate — OpenVPN Documentation Index

76 Status → Queues

Supervisión de colas ALTQ · QoS · planificación del tráfico · pérdidas · diagnóstico

El menú Status → Queues permite observar el comportamiento de las colas de Traffic Shaping basadas en ALTQ. Su lectura relaciona prioridad, capacidad de salida, paquetes procesados, ocupación y descartes. No es una pantalla de creación de políticas: sirve para verificar si una configuración de colas está clasificando tráfico y si funciona bajo carga.

ADVERTENCIA CONCEPTUAL El aviso «Traffic shaping is not configured» implica que no hay colas ALTQ que esta página pueda representar. No permite concluir que no existan limitadores dummynet ni reglas de QoS de otro tipo.



Figura 76.1. Recorrido del tráfico con ALTQ y ubicación independiente de la supervisión de limitadores.

76.1. Finalidad y ruta de acceso

Ruta exacta: Status → Queues. La página pertenece al área de supervisión del cortafuegos. Los objetos ALTQ se crean o modifican desde Firewall → Traffic Shaper, generalmente con el asistente o mediante las pestañas de configuración avanzada By Interface y By Queue. Para los limitadores se utiliza Firewall → Traffic Shaper → Limiters; su inspección corresponde a Diagnostics → Limiter Info.

Los indicadores básicos deben interpretarse junto con la configuración de ALTQ. Los drivers compatibles, los planificadores disponibles, la integración con paquetes y el comportamiento de las estadísticas pueden variar por versión; contrastarlos con la documentación del sistema instalado.

76.2. Lectura de la pantalla sin configuración ALTQ

Elemento visible	Qué representa	Comportamiento y limitación
Status / Queues	Ruta de navegación; confirma el área de trabajo.	No aplica ni deshace reglas.
Aviso amarillo	«Traffic shaping is not configured».	La vista no tiene colas ALTQ que mostrar; no demuestra ausencia de limitadores.
X del aviso	Cierre visual de la notificación.	No configura ALTQ ni habilita el servicio.
Icono de ajustes	Acceso contextual a la configuración relacionada.	La acción exacta del atajo puede variar según la edición de GUI.
Icono de navegación	Atajo contextual hacia una vista relacionada.	Consultar tooltip; el destino depende de la pantalla y la versión.
Icono de ayuda (?)	Ayuda contextual.	No produce cambios de tráfico.

Un mensaje de ausencia de colas es coherente tanto en una instalación que no necesita QoS como durante una puesta en marcha. No es un fallo automático de red, una caída del cortafuegos ni una indicación de que deban crearse colas de inmediato.

76.3. Qué es Traffic Shaping y para qué sirve

Traffic Shaping regula el orden o la velocidad de salida del tráfico para reducir la competencia entre flujos. La calidad de servicio (QoS) busca proteger las aplicaciones sensibles a retardo o variación de retardo, por

ejemplo voz, control remoto y operaciones de negocio, cuando comparten capacidad con descargas o copias masivas.

La existencia de prioridad no aumenta la velocidad física de una línea. En un enlace saturado, asignar mejor los tiempos de transmisión puede reducir latencia y descartes de determinados flujos a costa de demorar otros. Conviene definir el objetivo del proyecto —priorizar, limitar, garantizar capacidad o reducir bufferbloat— antes de elegir un mecanismo.

76.4. ALTQ y Limiters: dos mecanismos distintos

Criterio	Colas ALTQ	Limitadores dummynet
Motor	Planificación de colas sobre PF y el driver de red.	Pipes/queues dummynet; independiente de ALTQ.
Propósito principal	Clasificar y priorizar tráfico; jerarquías según scheduler.	Limitar caudal por política, dirección, IP o red; pesos en colas hijas.
Lugar de configuración	Firewall → Traffic Shaper: wizard, By Interface, By Queue.	Firewall → Traffic Shaper → Limiters.
Lugar de supervisión	Status → Queues.	Diagnostics → Limiter Info.
Requisito de NIC	Depende del soporte de ALTQ en el driver.	No exige compatibilidad ALTQ.
Ejemplo de decisión	Reservar o priorizar flujo crítico frente a descarga.	Establecer límite por usuario o zona de invitados.

ERROR HABITUAL No añadir un limiter y esperar automáticamente ver estadísticas en Status → Queues. El uso de dummynet se inspecciona en Diagnostics → Limiter Info.

76.5. Ubicación del punto de salida y sentido de las colas

ALTQ planifica cuando el firewall transmite por una interfaz. Para una subida LAN → Internet, el punto habitual de regulación es la salida WAN; para una descarga Internet → LAN, puede ser la salida LAN. Esta perspectiva es distinta de la etiqueta In/Out utilizada por algunas reglas y resulta esencial al diseñar QoS.



Figura 76.2. Direcciones de subida y bajada vistas desde las interfaces por las que sale el tráfico.

En conexiones Multi-WAN hay varios puntos de salida que requieren dimensionamiento coherente. La priorización de VPN debe tener en cuenta la encapsulación: un mismo flujo forma parte tanto del tráfico del túnel como de la capacidad física compartida de la WAN.

76.6. Vista cuando existen colas ALTQ

Al configurar colas ALTQ, la documentación de Netgate describe una lista de nombres y estadísticas de utilización. Las columnas oficiales son Queue, Statistics, PPS, Bandwidth, Borrows, Suspends, Drops y Length. Algunos indicadores no son relevantes para todos los schedulers. La forma exacta de presentación depende de la versión.

Columna	Significado técnico	Cómo interpretarla
Queue	Nombre de cola ALTQ.	Correlacionar con la jerarquía y las reglas que clasifican el flujo.
Statistics	Barra gráfica de la actividad o llenado de la cola.	Se representa según el tipo de estadística seleccionado.

Columna	Significado técnico	Cómo interpretarla
PPS	Ritmo en paquetes por segundo.	Ayuda a detectar flujos intensivos en paquetes pequeños.
Bandwidth	Tasa instantánea aproximada en bits por segundo.	Contrastar con la capacidad útil del enlace, no con velocidad nominal de NIC.
Borrows	Uso de capacidad disponible de otra clase / cola según planificador.	La interpretación depende del scheduler; resulta especialmente relevante en CBQ.
Suspends	Contador de acciones de aplazamiento.	Utilizado por CBQ; se espera cero en otros schedulers.
Drops	Paquetes descartados por gestión de cola.	No son conexiones enteras descartadas; revisar tendencia y contexto.
Length	Paquetes en espera frente a capacidad máxima de la cola.	Ocupación alta y sostenida sugiere congestión o dimensionamiento insuficiente.



Figura 76.3. La lectura conjunta de las métricas evita interpretar un contador aislado como una avería.

76.7. Opciones de visualización: Refresh Rate y Statistics

Control documentado	Valores	Efecto / precaución
Refresh Rate	Entre 0,5 y 5 segundos; predeterminado 1 segundo.	Frecuencia de actualización automática de estadísticas en la página.
Statistics	PPS (predeterminado) o Bandwidth.	Selecciona el dato utilizado para las barras gráficas de ocupación/actividad.

Estos controles no aparecen en la pantalla sin colas, porque no hay estadísticas disponibles. Cambiar la frecuencia de refresco no modifica el planificador ni la prioridad de los paquetes; cambia únicamente la cadencia de consulta y representación de datos.

76.8. PPS frente a Bandwidth: paquetes y bits no son equivalentes

Dos flujos con idéntico ancho de banda pueden generar un número muy diferente de paquetes por segundo. Paquetes pequeños aumentan la carga de procesamiento por paquete y pueden reducir el rendimiento efectivo. Por ejemplo didáctico, 1000 paquetes/s de 100 bytes de carga útil equivalen a 0,8 Mbit/s de esa carga, sin sumar cabeceras ni encapsulación. Se deben comparar magnitudes homogéneas.

76.9. Drops: descartes, retransmisiones y límites de interpretación

Drops contabiliza paquetes descartados por las colas, no «usuarios desconectados». Las pérdidas pueden provocar retransmisiones TCP o pérdidas perceptibles en aplicaciones de tiempo real. Una cifra aislada puede representar actividad histórica o competencia puntual; conviene correlacionar su incremento durante una ventana de carga con RTT, jitter, calidad de voz y ocupación.

No todos los drops son necesariamente defectos: un planificador puede descartar para mantener latencia o garantizar política. La ausencia de drops tampoco prueba que la QoS sea eficaz si un flujo no coincide con las reglas de clasificación.

76.10. Length y Statistics: ocupación y demora potencial

Length es un cociente entre paquetes en espera y tamaño de la cola; su lectura es puntual y no equivale al tiempo exacto de cola. Una cola grande puede absorber ráfagas, pero también aumentar el tiempo de espera (bufferbloat). Para verificar impacto real, observar bajo la misma carga la latencia hacia un destino estable y la calidad de los servicios.

76.11. Borrows y Suspends según el planificador

CBQ admite préstamo de capacidad disponible al hijo cuando está permitido; el contador Borrows proporciona información útil para comprender ese aprovechamiento. Suspends registra aplazamientos propios de CBQ. No se deben trasladar estas interpretaciones mecánicamente a PRIQ, HFSC, FAIRQ o CoDel.

76.12. Planificadores ALTQ y sus aplicaciones

Scheduler	Comportamiento distintivo	Riesgo / criterio de uso
PRIQ	Atiende colas según prioridad (0–15), sin jerarquía profunda.	Puede privar a colas de menor prioridad si hay saturación sostenida.
CBQ	Clases jerárquicas, bandas y posible préstamo desde el padre.	Exige definir capacidades y coherencia entre hijos y padres.
HFSC	Curvas de servicio y garantías temporales en estructura jerárquica.	Complejidad mayor: evaluar mínimos, ráfagas, upper limit y árbol.
CoDel	Gestión activa para reducir demora asociada a colas saturadas.	No equivale a garantía universal de caudal ni reemplaza medir bufferbloat.
FAIRQ	Intenta equilibrar tráfico entre flujos y prioridades.	Requiere configuración manual; el asistente no lo crea.

Los algoritmos pueden tener limitaciones adicionales según dispositivo, versión y driver. Una política de colas no es adecuada únicamente porque admita prioridad numérica: su rendimiento debe verificarse con la carga de producción prevista.

76.13. Creación de colas: relación con Firewall → Traffic Shaper

Un procedimiento de implantación comienza midiendo el caudal real disponible, identificando servicios críticos y decidiendo el planificador. El wizard genera colas y reglas comunes, normalmente sobre la pestaña Floating; las reglas tipo Match asignan tráfico a una cola sin modificar por sí solas la decisión de permitir/bloquear.

Después se valida que las reglas tienen un orden y criterios correctos, que las colas pertenecen a la interfaz de salida prevista y que las conexiones nuevas pasan por las políticas actualizadas. No es aconsejable editar colas en producción de forma improvisada: pueden cambiar el rendimiento general del firewall.

76.14. Procedimiento 1. Comprobar por qué aparece «not configured»

- Abrir Status → Queues y confirmar que se presenta el aviso, sin ejecutar ningún cambio.
- Ir a Firewall → Traffic Shaper y verificar si existen colas ALTQ habilitadas y aplicadas en By Interface / By Queue.
- Comprobar por separado si hay limitadores en la pestaña Limiters; no suponer que deban aparecer en Queues.
- Consultar Diagnostics → Limiter Info si existen limitadores aplicados a reglas.
- Si la organización no precisa QoS, registrar el estado como normal y no crear colas solo para eliminar el aviso.

76.15. Procedimiento 2. Validar el funcionamiento de una cola existente

- Identificar una aplicación de prueba controlada y el criterio de clasificación que debería coincidir.

- Comprobar la regla Firewall / Floating / Queue y la interfaz de salida correspondiente; registrar el valor previo de PPS, Bandwidth y Drops.
- Generar tráfico autorizado durante una ventana breve y observar cómo evolucionan la cola y las métricas.
- Cambiar Statistics de PPS a Bandwidth para comparar volumen y número de paquetes sin alterar las políticas.
- Correlacionar con Diagnostics → pfTop (vista Queue), Status → Monitoring y la calidad real del servicio.
- Si no hay variación, verificar si el tráfico coincide con otra regla o permanece en una cola predeterminada.

76.16. Procedimiento 3. Evaluar congestión y calidad de servicio

- Medir RTT en reposo desde un punto fijo y repetirlo mientras se satura un enlace de manera controlada.
- Anotar pérdida de paquetes, jitter y crecimiento de Drops/Length en la cola pertinente.
- Comprobar que la velocidad configurada para la cola raíz refleja el caudal útil real y no exclusivamente la velocidad nominal.
- Revisar prioridades y capacidad garantizada sin modificar simultáneamente varias clases.
- Aplicar un cambio aislado en ventana autorizada y repetir exactamente el ensayo inicial.

76.17. Procedimiento 4. Diagnosticar reglas que no asignan cola

Netgate advierte que un flujo mal priorizado a menudo coincide con otra regla antes de la prevista, o con ninguna regla que asigne cola. Hay que verificar el orden real y las reglas automáticas o de paquetes que pueden intervenir, el sentido del tráfico, las traducciones NAT y la clase predeterminada. El problema puede estar en el criterio de clasificación y no en la cola.

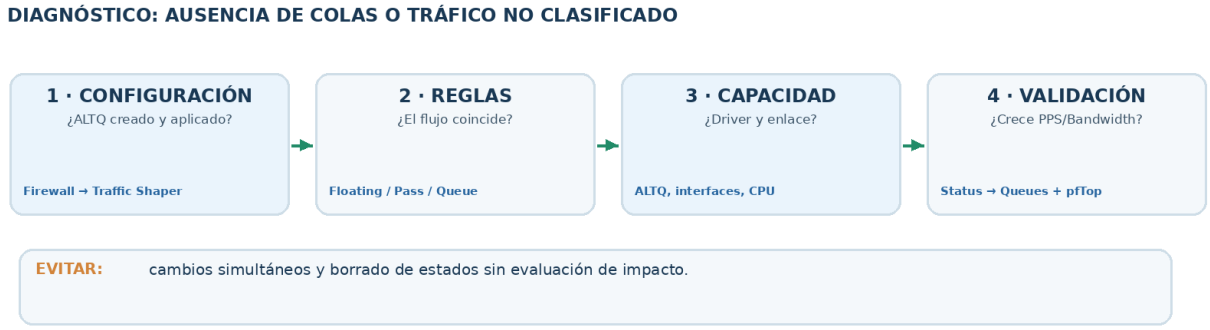


Figura 76.4. Secuencia de diagnóstico desde la configuración de colas hasta la comprobación del flujo.

76.18. Procedimiento 5. Validar QoS en VPN y Multi-WAN

Una VPN encapsula datos y comparte el caudal de su WAN. No se deben sumar «capacidad VPN» y «capacidad WAN» como si fueran enlaces distintos. Identificar qué interfaz transmite, qué regla reconoce el tráfico encapsulado y qué ocurre durante un failover. En Multi-WAN las velocidades y grupos de gateways deben medirse y verificarse por camino.

76.19. Limitaciones físicas y rendimiento

ALTQ necesita control desde el driver. La documentación de Netgate mantiene una lista de drivers compatibles, pero recomienda contrastarla con la implementación concreta del firmware. En entornos virtualizados el soporte ALTQ puede precisar ajustes del adaptador virtual con consecuencias sobre la capacidad de procesamiento; algunos cambios requieren reinicio del firewall.

El coste adicional de ALTQ puede reducir el máximo rendimiento del equipo. La alternativa con dummynet no tiene el mismo requisito de driver ALTQ y puede ser más práctica para limitación por host o mitigación de bufferbloat. El mecanismo se selecciona por objetivo y compatibilidad, no por la presencia de la opción en el menú.

76.20. Relación con los estados PF y los cambios de reglas

Las conexiones ya establecidas pueden retener clasificación y estados derivados de reglas anteriores. Una modificación de shaping puede no afectar inmediatamente al tráfico existente. La eliminación masiva de estados es disruptiva: solo debe valorarse cuando el procedimiento lo requiera, con aprobación y acceso alternativo, nunca como primera prueba.

CAMBIO DE PRODUCCIÓN La modificación de colas, las reglas Floating o el reinicio de estados pueden afectar voz, terminales, enlaces VPN y aplicaciones críticas. Registrar valores previos, garantizar reversión y ejecutar en una ventana apropiada.

76.21. Diagnóstico diferencial: ¿problema QoS o problema de conectividad?

Síntoma	Causas candidatas	Prueba recomendada
No aparece ninguna cola	ALTQ no configurado; solo existen limiters.	Revisar Firewall → Traffic Shaper y Limiter Info.
Cola visible, PPS siempre cero	Regla no coincide, tráfico ausente o interfaz equivocada.	Revisar regla y generar un flujo autorizado.
La QoS no parece surtir efecto	Flujo en clase predeterminada, ruta alternativa o estados antiguos.	Inspeccionar reglas, pfTop Queue y ruta.
Drops suben mucho durante carga	Congestión, planificador o capacidad configurada.	Observar jitter/RTT y clase afectada.
Solo cae la voz cuando hay descarga	Bufferbloat, falta de clasificación o colas mal dimensionadas.	Comparar latencia o jitter bajo carga controlada.
Desciende throughput al activar ALTQ	Sobrecarga de CPU/driver o limitación demasiado baja.	CPU, NIC, tasas y pruebas con reversión.
Multi-WAN se comporta de forma desigual	Capacidad distinta por WAN o clasificación direccional errónea.	Separar pruebas y salidas por gateway.
Gráficas antiguas dejan de aparecer	RRD de colas regenerados tras cambios de configuración.	Revisar historial de cambios y nuevos datos.

76.22. Escenario empresarial 1. Telefonía IP y saturación de subida

En una sede, videoconferencias y copias masivas consumen el enlace de subida. Una planificación de colas diseñada con mediciones previas da prioridad al tráfico de voz y reduce la espera. La validación requiere comprobar calidad de llamada real, PPS de cola relevante, RTT y posibles efectos sobre el resto del tráfico; no basta con que el indicador de cola aumente.

76.23. Escenario empresarial 2. Usuarios invitados con limitación individual

Una red Wi-Fi de invitados necesita un máximo de velocidad por usuario. El mecanismo adecuado suele ser un limiter enmascarado por IP, no una cola ALTQ global. Su inspección se hace en Diagnostics → Limiter Info, mientras que Status → Queues puede seguir mostrando que ALTQ no está configurado.

76.24. Escenario empresarial 3. Dos salidas a Internet con capacidades distintas

Una organización tiene una WAN principal y otra de respaldo con ancho de banda diferente. Durante la conmutación las colas de una interfaz pueden no representar la capacidad efectiva de la otra. El administrador debe revisar los criterios del diseño Multi-WAN y medir carga y latencia por enlace en vez de copiar un porcentaje de capacidad fijo entre conexiones.

76.25. Escenario empresarial 4. Conexiones VPN y copias nocturnas

Un túnel entre sedes transporta copias de seguridad y aplicaciones interactivas. La clasificación debe tener en cuenta el tráfico encapsulado y el cuello de botella físico. Se comprueba la continuidad de la VPN, las clases implicadas y el rendimiento durante copias programadas. Si una VPN usa interfaz virtual con limitaciones del driver, puede ser más apropiado trabajar sobre WAN o estudiar limitadores.

76.26. Buenas prácticas para operación y mantenimiento

- No activar Traffic Shaping por rutina: primero definir un problema medible y su prioridad de negocio.
- Mantener registro de velocidades medidas, enlaces, interfaces, número de colas y periodo de prueba.
- Comparar PPS y Bandwidth en la misma ventana; separar paquetes por segundo de bits por segundo.
- No interpretar un Drop aislado como pérdida de sesión. Medir incrementos y calidad de servicio.
- Verificar compatibilidad ALTQ de NIC y costos de CPU en equipos o hipervisores.
- No asumir que una regla editada reasigna todas las conexiones activas sin revisar estados PF.
- Documentar los límites y la ruta de reversión antes de cambios en Multi-WAN, VPN o telefonía.
- Tratar capturas, métricas y esquemas de la red como información operativa reservada.

76.27. Ficha de revisión y aceptación

Comprobación	Criterio de aceptación	Evidencia
Inventario	Mecanismo QoS identificado (ALTQ o limiter).	Ruta de configuración y objetivo.
Conectividad	Aplicaciones esenciales operativas con y sin carga.	Pruebas de aplicación.
Clasificación	El flujo esperado contabiliza en la cola prevista.	Cola y ventana de prueba.
Capacidad	Velocidad coherente con el enlace real.	Medición de throughput.
Calidad	RTT/jitter/pérdida adecuados al caso de uso.	Muestras comparativas.
Impacto	Sin deterioro inesperado de CPU y conexiones críticas.	CPU y contadores.
Reversión	Configuración anterior y plan de recuperación disponibles.	Referencia del cambio.

76.28. Glosario esencial

Concepto	Definición operativa
ALTQ	Marco de colas y planificación vinculado a PF y drivers compatibles.
QoS	Gestión diferenciada de tráfico según objetivos de calidad.
Scheduler	Disciplina que decide el orden y las oportunidades de transmisión.
Queue / Class	Grupo de paquetes con política común de tratamiento.
PPS	Paquetes por segundo.
Bandwidth	Volumen de transmisión expresado como tasa en bits por segundo.
Drops	Paquetes descartados dentro del tratamiento por colas.
Bufferbloat	Aumento de latencia por exceso de buffers bajo carga.
Limiter	Mecanismo dummynet de límite de velocidad/colas independiente de ALTQ.
Floating Rule	Regla de firewall con alcance interinterfaces y criterios de coincidencia.
CBQ / HFSC	Disciplinas de clases jerárquicas con diferentes mecanismos de servicio.
pfTop	Herramienta de observación del tráfico y estados, con vista Queue.

76.29. Referencias oficiales y documentación complementaria

01. Netgate — ALTQ Traffic Shaper Queue Monitoring
02. Netgate — Traffic Shaper, conceptos y modos
03. Netgate — ALTQ Scheduler Types
04. Netgate — Limiters y Diagnostics → Limiter Info
05. Netgate — Limitaciones hardware ALTQ
06. Netgate — Troubleshooting Traffic Shaping
07. Netgate — Advanced Customization

08. Netgate — ALTQ Wizard
09. Netgate — CoDel Limiters y Bufferbloat
10. Netgate — pfTop, vista Queue
11. Netgate — Reset State Table
12. Netgate — QoS en redes VPN
13. Netgate — ALTQ en interfaces virtuales
14. Netgate — RRD de colas y su reset

77 Status → Services

Demonios del sistema · estado operativo · acciones · dependencias · diagnóstico

Status → Services centraliza la consulta del estado de numerosos servicios base y servicios de paquetes de pfSense Plus. Presenta qué procesos están iniciados, ofrece controles de administración y enlaza directamente con su configuración, su supervisión y sus registros. Es una consola operativa: sirve para reaccionar ante incidencias, pero no reemplaza las pruebas funcionales ni el análisis de la configuración.

CRITERIO DE EXPLOTACIÓN El símbolo de servicio en ejecución confirma que pfSense lo considera activo, no que DHCP entregue concesiones, DNS resuelva o una VPN transporte tráfico de extremo a extremo. La actuación debe basarse en síntomas contrastados, no en un único icono.



Figura 77.1. Relación entre el estado de los servicios y la verificación de funciones de red.

77.1. Objetivo y alcance de la página

Ruta exacta: Status → Services. La página agrupa la mayoría de los demonios principales y servicios que los paquetes registran en la interfaz. Algunas funciones internas del sistema no aparecen aquí como entradas administrables; por tanto, el listado no es un inventario completo de procesos de FreeBSD. La documentación oficial de Netgate define los estados generales Running y Stopped, además de los controles disponibles para cada fila [1].

Desde esta vista pueden diagnosticarse interrupciones del servicio de resolución DNS, entrega DHCP, sincronización horaria, monitorización de gateways o conectividad VPN. No es necesario reiniciar servicios durante el funcionamiento normal; hacerlo injustificadamente puede provocar microcortes o alterar el contexto necesario para investigar una incidencia.

77.2. Lectura estructurada de la pantalla

Columna	Qué presenta	Interpretación y precaución
Service	Identificador técnico del demonio: dpinger, kea-dhcp4, ntpd, unbound, etc.	Se usa para correlacionar logs, guías y algunos comandos de administración; no describe por sí solo la configuración.
Description	Descripción funcional o de instancia, cuando está disponible.	Un servicio por instancia puede añadir un texto administrativo; no es un nombre de host ni una prueba de conectividad.
Status	Icono visual del estado del servicio.	Un check verde equivale a ejecución detectada; una señal de no ejecución o deshabilitación requiere comprobar contexto.
Actions	Controles de proceso y accesos rápidos a otras páginas.	La disponibilidad depende del servicio, del estado y de las páginas relacionadas que existan.

La captura correspondiente a este capítulo presenta ocho clases o instancias de servicios. Los identificadores y nombres de equipos de los ejemplos de este capítulo son genéricos; los estados de una captura concreta no deben extrapolarse a todas las instalaciones.

77.3. Estados, colores y límites de interpretación

Indicador	Lectura operativa	Comprobación necesaria
Marca verde	Servicio detectado como iniciado/Running.	Probar la función real: concesión, consulta, sesión, destino o sincronización.
Icono de parada o no ejecución	Servicio parado o no activo según la implementación de su estado.	Revisar si está habilitado, si tiene configuración y si debería existir actividad.
Icono de prohibición o inhabilitación	Puede señalar función deshabilitada/no operativa en la integración correspondiente.	No interpretarlo automáticamente como error o caída; consultar Settings y Status.
Ausencia de controles de proceso	El paquete puede no ofrecer inicio/parada en esta vista.	Utilizar las rutas específicas oficialmente disponibles, sin inferir botones inexistentes.

ATENCIÓN «Parado» no equivale siempre a «averiado»: un servicio opcional puede permanecer inactivo deliberadamente. A la inversa, una marca verde no descarta errores de autenticación, reglas firewall restrictivas ni problemas de rutas.

77.4. Acciones de servicio: arranque, parada y reinicio

Acción	Efecto documentado	Riesgo operativo
Restart (flecha circular)	Reinicia el servicio en funcionamiento. En algunos demonios recarga configuración en vez de ejecutar una secuencia completa de parada/arranque.	Puede cortar sesiones, liberar caché, renovar sockets o causar una interrupción temporal.
Stop (cuadrado en círculo)	Detiene un servicio que está ejecutándose.	Los clientes que dependen de él pueden perder la prestación inmediatamente.
Start (triángulo en círculo)	Inicia un servicio detenido cuando su control está disponible.	No resuelve errores de configuración; el servicio puede fallar al iniciar.
Settings (deslizadores)	Abre el formulario de ajustes relacionado.	Guardar cambios en los parámetros puede provocar recargas o efectos más amplios.
Status (gráfico)	Accede a la página de estado específica, si existe.	Es navegación y supervisión; no es una acción de reinicio.
Logs (lista)	Abre los registros relacionados, si el acceso está implementado.	Es preferible consultarlos antes de reiniciar para conservar el contexto.

Netgate advierte que Restart no tiene una semántica idéntica para todos los demonios: puede implicar una recarga de configuración. Los iconos de navegación solo se muestran cuando el destino existe [1, 2].



Figura 77.2. Secuencia de intervención de menor a mayor impacto ante un síntoma de servicio.

77.5. Controles superiores, navegación y enlaces

En la barra de navegación aparecen Status, Services y el acceso a ayuda contextual (icono «?»). En cada fila pueden presentarse accesos rápidos a Settings, Status y Logs. No todos los servicios muestran todas las opciones. La barra de herramientas no debe confundirse con acciones universales de inicio o parada; los controles de operación están situados en cada servicio [2].

77.6. Servicio dpinger — Gateway Monitoring Daemon

dpinger supervisa destinos de monitorización de gateways mediante sondeos y calcula indicadores de latencia y pérdida. Sus resultados sirven para marcar estados de los gateways y pueden activar políticas de recuperación o conmutación Multi-WAN cuando la configuración así lo determina. El hecho de que dpinger esté Running no certifica que cada gateway esté Online.

Comprobar	Dónde	Lectura diagnóstica
Estado de enlaces	Status → Gateways	Online, Warning o Offline; observar RTT, RTTsd y pérdida.
Eventos de alarma	Status → System Logs → System/Gateways	Comparar los cambios Alarm/Clear con la incidencia.
Selección de monitor	System → Routing → Gateways	El destino de monitorización debe ser representativo y responder de forma estable.

MULTI-WAN Reiniciar dpinger durante una incidencia puede alterar temporalmente la información de salud de los gateways. Antes de hacerlo, comprobar si el problema es del enlace, del objetivo de monitorización o de la ruta realmente utilizada.

77.7. Servicios kea-dhcp4 y kea-dhcp6

Kea DHCPv4 entrega parámetros IPv4 a clientes cuando las interfaces y pools están correctamente definidos. Kea DHCPv6 gestiona concesiones IPv6 y, cuando se configura, delegación de prefijos. Ambos son servicios distintos: uno puede operar sin que el otro sea necesario. El backend DHCP se selecciona bajo System → Advanced → Networking y el comportamiento depende de la versión instalada [9, 10].

Servicio	Prueba funcional	Qué no demuestra el estado Running
kea-dhcp4	Comprobar DORA, nueva concesión IPv4 y Status → DHCP Leases.	No asegura que el pool tenga direcciones libres o que una VLAN reciba difusión DHCP.
kea-dhcp6	Comprobar IA_NA/IA_PD y Status → DHCPv6 Leases; contrastar Router Advertisements.	No asegura que un cliente use DHCPv6: SLAAC puede funcionar sin concesiones DHCPv6.
Ambos	Buscar mensajes Kea y verificar el servicio en la interfaz prevista.	No elimina problemas de relay, firewall, interfaces mal asociadas o configuración inválida.

Interrupción esperable: una detención temporal puede afectar a las solicitudes nuevas y renovaciones de concesiones. Las direcciones ya concedidas no desaparecen necesariamente de inmediato de los clientes; su comportamiento depende del tiempo de vida y de la reacción del sistema operativo.

77.8. Servicio ntpd — sincronización horaria

ntpd mantiene el reloj de pfSense sincronizado con servidores upstream y puede responder consultas NTP de la red según configuración. Su estado Running debe complementarse con Status → NTP: Active Peer, Candidate, Stratum, Reach, Offset y Jitter. La selección de un peer no depende exclusivamente del menor RTT [11].

Un reloj incorrecto afecta a la correlación de logs, a certificados y a mecanismos de autenticación sensibles al tiempo. Reiniciar ntpd no es el primer paso cuando se observa offset transitorio: debe verificarse conectividad UDP/123, DNS de los servidores, fuentes disponibles y tiempo de convergencia.

77.9. Servicio openvpn — instancias y dependencias

OpenVPN puede registrar en la lista una instancia de cliente o servidor. El nombre de instancia interna no sustituye a la página Status → OpenVPN, donde se inspeccionan la conexión negociada, direcciones virtuales, datos transmitidos y estados de reconexión. Una instancia iniciada puede seguir sin establecer sesión por problemas de certificado, autenticación, alcance del endpoint o firewall [7].

INTERRUPCIÓN DE SERVICIO Restart o Stop sobre una instancia OpenVPN puede interrumpir el acceso remoto o la conectividad entre sedes, y obligar a renegociar el túnel. En administración remota, verificar antes una ruta alternativa de acceso.

77.10. Servicio syslogd — registro del sistema

syslogd recolecta registros locales del firewall y de múltiples servicios, con opciones de reenvío remoto. Su disponibilidad es crítica para la trazabilidad y el diagnóstico. Status → System Logs organiza los mensajes por subsistemas; los archivos locales se mantienen en /var/log/ en versiones modernas de pfSense Plus [3, 8].

Detenerlo durante una avería puede suprimir evidencia futura. No debe hacerse como método habitual para “limpiar” registros: existen políticas de rotación y administración de logs específicas. El registro remoto no debe suponerse cifrado por defecto; Netgate advierte que syslog convencional remoto transmite sin cifrado salvo que se proteja el transporte [12].

77.11. Servicio unbound — DNS Resolver

unbound implementa el DNS Resolver recursivo, validador y caché de pfSense. Puede funcionar en modo resolución o como reenviador. Que figure iniciado no garantiza que resuelva nombres internos y externos, especialmente si existen problemas de DNSSEC, políticas de salida, servidores forwarding o datos obsoletos [4].

El reinicio completo de unbound limpia su caché interna; Netgate también documenta operaciones más limitadas mediante unbound-control para recargar o vaciar entradas concretas. La caché de equipos clientes y navegadores puede conservar respuestas anteriores [5].

```
dig @127.0.0.1 example.com
unbound-control -c /var/unbound/unbound.conf dump_cache
```

PRODUCCIÓN No reiniciar DNS indiscriminadamente para resolver un fallo de nombre aislado. Correlacionar la consulta con registros, overrides, TTL, caché local y upstream.

77.12. Servicio wireguard — paquete y túneles

WireGuard se integra mediante paquete y presenta sus ajustes bajo VPN → WireGuard → Settings. La opción Enable determina si está habilitado. Su indicador puede representar un servicio no activo o no habilitado; la captura de una fila no basta para atribuir una avería. WireGuard no tiene una noción clásica de “sesión conectada” equivalente a OpenVPN: su verificación incluye handshakes, contadores RX/TX, peer, rutas y firewall [6].

El paquete puede estar instalado sin tener túneles activos. Ante un indicador de inactividad, empezar por VPN → WireGuard → Settings y Status, comprobar que exista al menos un túnel pertinente y revisar sus reglas antes de intervenir.

77.13. Cuadro comparativo de riesgo por servicio



Figura 77.3. Dependencias funcionales de los servicios y posibles áreas afectadas por una interrupción.

Servicio	Impacto posible al detenerlo	Prueba tras recuperación
dpinger	La monitorización de gateways se interrumpe; las decisiones Multi-WAN pueden perder una señal de salud.	Verificar Status → Gateways y eventos Alarm/Clear.
Kea DHCPv4/v6	Fallan nuevas asignaciones/renovaciones mientras no responda el backend.	Renovar en un cliente de prueba; comprobar leases y logs.
ntpd	La referencia horaria puede derivar mientras el demonio no opere.	Comprobar peer elegido, offset y reach.
OpenVPN	Se pueden cortar túneles y flujos empresariales.	Comprobar status de la instancia y tráfico bidireccional.
syslogd	Se pierde continuidad de registros según destino y configuración.	Generar evento controlado y confirmar recepción.
unbound	Fallas de resolución en clientes que usan el firewall como DNS.	Consultar nombres internos y externos desde firewall y cliente.
WireGuard	Pérdida potencial del tráfico que dependía de los túneles.	Revisar handshake, RX/TX y alcance IP.

77.14. Diferenciar configuración, proceso, puerto y función

La comprobación rigurosa atraviesa cuatro capas: (1) configuración y habilitación; (2) proceso o instancia iniciada; (3) escucha o conectividad en el puerto esperado; (4) prestación del servicio extremo a extremo. Ninguna capa aislada demuestra las demás. Este modelo evita reinicios que ocultan la causa original.

Capa	Ejemplo	Evidencia objetiva
Configuración	DNS Resolver habilitado	Settings y configuración aplicada.
Proceso	unbound iniciado	Status → Services o salida de procesos.
Transporte	UDP/TCP 53 operativo	Consulta local y captura, cuando proceda.
Función	Nombre resuelto correctamente	Respuesta DNS esperada y repetible en el cliente.

77.15. Herramientas complementarias de diagnóstico

Las rutas más útiles son Status → System Logs (mensajes del servicio), Diagnostics → Packet Capture (tráfico), Diagnostics → Ping y DNS Lookup (pruebas), Status → Gateways (monitorización) y las páginas específicas de NTP, OpenVPN o WireGuard. Para las rutas de logs, utilizar siempre la pestaña del subsistema correspondiente cuando exista; la posición puede variar con la versión y los paquetes [3].

Desde la consola, Netgate documenta el reproductor PHP del sistema para administrar servicios registrados en la GUI. Es una herramienta avanzada: confirmar el identificador de instancia y privilegios antes de ejecutar comandos [13].

```
pfSsh.php playback svc <start|stop|restart> <service> [opciones_de_instancia]
pfSsh.php playback svc restart openvpn client 2
```

El segundo comando es un ejemplo sintáctico de la documentación oficial y no representa una instancia real. No debe ejecutarse automáticamente en un equipo de producción.

77.16. Reiniciar frente a recargar una configuración

Según la implementación, la acción de reinicio puede provocar relectura de configuración sin un reinicio completo del proceso. Para unbound, por ejemplo, Netgate diferencia la recarga selectiva del servicio del reinicio que vacía completamente su caché. Por tanto, no debe afirmarse que todas las acciones Restart eliminan estados, cachés o sesiones [1, 5].

77.17. Procedimiento: comprobar un DNS que aparece Running

PROCEDIMIENTO · Resolver consultas intermitentes sin reiniciar al primer síntoma

1. Confirmar en Status → Services que unbound esté iniciado y registrar la hora del síntoma.

2. Consultar un nombre de documentación, como example.com, desde el propio firewall y desde un cliente autorizado.

3. Comparar la respuesta con el servidor DNS efectivo, la ruta utilizada y los registros de Unbound.

4. Comprobar si afecta a dominios internos, externos o ambos; verificar DNSSEC y forwarding cuando apliquen.

5. Aplicar la corrección mínima y repetir la prueba; reservar el reinicio para cuando exista una razón técnica documentada.

77.18. Procedimiento: DHCPv4 o DHCPv6 que no entrega concesiones

PROCEDIMIENTO · Aislar backend, interfaz y alcance de la petición

1. Confirmar qué backend DHCP utiliza el firewall y si el servicio correspondiente está habilitado.

2. Examinar concesiones, capacidad del pool y registros DHCP.

3. Probar con un cliente controlado en el segmento afectado, sin realizar cambios masivos en la red.

4. Si hay relay o VLAN, seguir los paquetes DHCP y la asociación de interfaces con captura.

5. Corregir el origen del fallo; verificar una concesión nueva y una renovación sin intervenir en otras VLAN.

77.19. Procedimiento: servicio OpenVPN activo sin tráfico útil

PROCEDIMIENTO · Separar túnel iniciado, conexión negociada y enrutamiento

1. Consultar Status → OpenVPN para conocer el estado de la instancia y su última transición.

2. Revisar eventos de autenticación y handshake en los logs.

3. Comparar redes del túnel, rutas efectivas, reglas de firewall y NAT.

4. Probar comunicación IP entre direcciones documentales en un laboratorio representativo; evitar credenciales de producción.

5. Solo tras identificar la causa, aplicar el cambio y validar tráfico bidireccional y servicios de aplicación.

77.20. Procedimiento: dpinger Running con un gateway en alarma

PROCEDIMIENTO · Confirmar monitorización y failover

1. Registrar RTT, RTTsd, pérdida y estado del gateway en Status → Gateways.

2. Comprobar los eventos temporales de alarma/recuperación en Gateway Logs.

3. Validar si el host de monitorización responde de forma estable o filtra sondas.

4. Comprobar qué rutas y reglas policy routing utilizan dicho gateway.

5. Realizar una prueba controlada de conmutación solo con un plan de reversión y ventana autorizada.

77.21. Procedimiento: fallo de registros o auditoría

PROCEDIMIENTO · Verificar syslogd y retención de evidencias

1. Comprobar el estado del servicio y revisar Status → System Logs.

2. Generar un evento controlado de bajo impacto y confirmar su aparición.

3. Si existe servidor syslog remoto, verificar conectividad, destino y seguridad del transporte.

4. Inspeccionar política de rotación, ocupación de almacenamiento y recepción en el colector.

5. Documentar cualquier pérdida de eventos y restablecer el registro sin borrar evidencia previa.

77.22. Criterios para operar en alta disponibilidad

En un clúster HA, antes de controlar un servicio comprobar nodo activo, estado CARP, pfsync y sincronización XMLRPC cuando proceda. No asumir que las instancias y su impacto son simétricos en ambos nodos. Coordinar los reinicios para evitar interrupciones simultáneas del servicio principal y del respaldo; registrar los cambios en la ventana autorizada.

ADMINISTRACIÓN REMOTA No detener un servicio VPN que sostiene la propia conexión de gestión sin una vía alternativa de acceso (consola, gestión fuera de banda o enlace redundante) y sin confirmación del impacto.

77.23. Seguridad y permisos administrativos

Limitar el acceso a Status → Services y a los controles de gestión mediante cuentas y privilegios apropiados de pfSense, con autenticación robusta y trazabilidad. Los iconos de acceso a configuración no eliminan la necesidad de autorización. Para labores sensibles, establecer supervisión, ticket de cambio, copia de configuración y validación de reversión.

No usar reinicios como sustituto de la investigación: pueden borrar conexiones, cachés o contexto. Evitar copiar pantallas operativas completas en documentación de terceros: contienen nombres de servicios personalizados, destinos remotos, usuarios o identificadores internos.

77.24. Escenarios empresariales de aplicación

Escenario	Detección / análisis	Actuación razonada
Caída parcial del DNS corporativo	unbound Running; consultas internas fallan mientras externas funcionan.	Revisar overrides, dominios y servidores forward antes de tocar el demonio.
Nuevos puestos no reciben IPv4	kea-dhcp4 Running; pool agotado o relay no llega.	Consultar leases y capturar DORA, corregir el origen sin borrar todas las concesiones.
Sede remota accesible a ratos	openvpn Running; servidor renegocia o cambia la ruta WAN.	Cruzar logs, gateway, handshake y tráfico; examinar MTU y rutas.
Línea de respaldo mal evaluada	dpinger Running, pero gateway Warning.	Comparar sondas al objetivo, pérdida de paquetes real y política Multi-WAN.
Histórico de eventos incompleto	syslogd figura activo; el colector externo no recibe.	Revisar destinos, transporte, logs locales y cola/rotación.
WireGuard instalado sin túneles	Icono de inactividad con paquete presente.	Comprobar habilitación y configuración antes de atribuirlo a una avería.

77.25. Matriz rápida de incidencias y decisiones

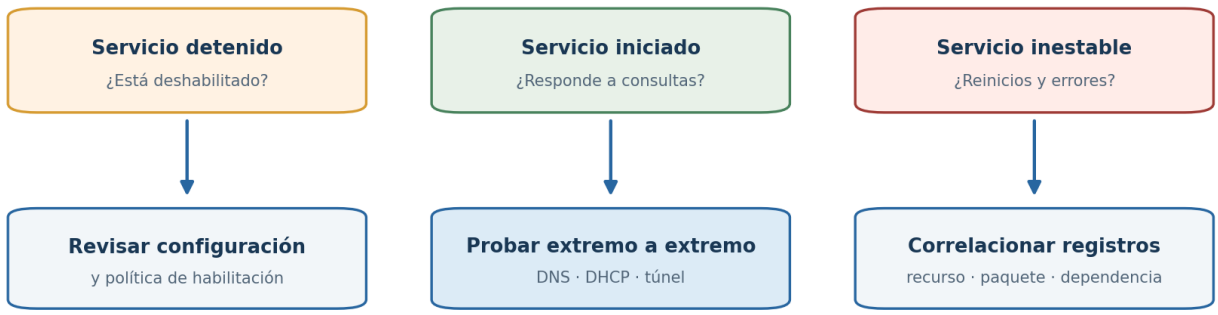


Figura 77.4. Diferenciar servicio detenido, activo sin funcionalidad y servicio inestable.

Síntoma	Hipótesis inicial	Siguiente comprobación
Check verde, pero sin DNS	fallo de resoluciones upstream o ACL	Consulta con dig, DNS Resolver y registros.
DHCP Running, nuevos equipos sin IP	pool, VLAN, relay o reglas	Lease status y captura DORA.
OpenVPN Running, túnel desconectado	TLS, autenticación, endpoint	Status → OpenVPN y registros de la instancia.
WireGuard no activo	paquete o túnel deshabilitado	VPN → WireGuard → Settings y Status.

Síntoma	Hipótesis inicial	Siguiente comprobación
Gateway Warning con dpinger activo	objetivo de monitorización o enlace	RTT, loss y Gateway Logs.
syslogd activo, no hay mensajes remotos	destino syslog o conectividad	Comprobar recepción en servidor y transporte.

77.26. Lista de comprobación antes y después de actuar

Antes de la acción	Después de la acción
Identificar el servicio exacto y su función de negocio.	Comprobar que su estado volvió al esperado.
Verificar si la incidencia afecta a uno o varios segmentos.	Validar una operación funcional real desde un cliente.
Consultar logs y conservar marcas de tiempo.	Verificar ausencia de errores nuevos y correlacionar eventos.
Evaluar impacto sobre conexiones y servicios críticos.	Comprobar gateways, VPN, DNS o DHCP dependientes.
Disponer de acceso alternativo y reversión cuando proceda.	Registrar resultado, responsables y evidencias desidentificadas.

77.27. Glosario técnico

Término	Definición
Daemon / demonio	Proceso de sistema que presta un servicio en segundo plano.
Running / Stopped	Estado iniciado o detenido presentado por la interfaz de supervisión.
Reload	Relectura de configuración; su mecanismo concreto depende de la implementación del servicio.
dpinger	Herramienta de monitorización de gateways utilizada en pfSense.
Kea DHCP	Backend moderno para proporcionar DHCPv4 y DHCPv6.
unbound	Software de DNS Resolver recursivo y caché.
syslogd	Servicio de recepción y almacenamiento de mensajes del sistema.
HA	High Availability; diseño de redundancia de equipos y funciones.

77.28. Referencias técnicas oficiales

Las funcionalidades se han contrastado con la documentación oficial vigente de Netgate. La disponibilidad de servicios y accesos rápidos depende de la versión de pfSense Plus, el backend seleccionado y los paquetes instalados. Las referencias siguientes deben utilizarse para comprobar particularidades de nuevas versiones.

Referencia oficial / acceso directo	Referencia oficial / acceso directo
[1] Service Status	[2] Quickly Navigate the GUI with Shortcuts
[3] System Logs	[4] DNS Resolver
[5] Troubleshooting the DNS Cache	[6] WireGuard Settings
[7] Troubleshooting OpenVPN	[8] Working with Log Files
[9] Networking: DHCP Server Backend	[10] Kea Settings Tab
[11] NTP Daemon Status	[12] Remote Logging with Syslog
[13] Using the PHP Shell	[14] Gateway Logs

78 Status → System Logs

Registro y trazabilidad · filtros · servicios · conservación · análisis de incidencias

Los registros del cortafuegos constituyen una fuente esencial para reconstruir cambios, detectar fallos de servicios y correlacionar incidencias de red. La vista Status → System Logs permite consultar eventos clasificados por subsistema, aplicar filtros y controlar preferencias de registro; la interpretación adecuada exige distinguir un mensaje informativo, una advertencia y un fallo corroborado por pruebas operativas.

PRINCIPIO DE DIAGNÓSTICO Un log confirma que un proceso ha emitido un mensaje, no necesariamente que exista una incidencia activa. Para diagnosticar, correlacione fecha, servicio, estado, interfaz y evidencia de tráfico.



Figura 78.1. Origen, almacenamiento, consulta y conservación centralizada de eventos.

78.1. Objetivo, alcance y ruta de acceso

Ruta: Status → System Logs. El visor centraliza categorías de sistema, seguridad, DHCP, autenticación, VPN, NTP y paquetes. Las páginas exactas y subpestañas pueden variar según versión de pfSense Plus, hardware, servicios activos y paquetes instalados.

El acceso al visor requiere permisos de administración apropiados. La página de registros no sustituye a una monitorización externa con alertas y retención definida. En pfSense Plus moderno los archivos están bajo /var/log/ y se mantienen como texto plano con rotación.

78.2. Mapa de pestañas y subpestañas



Figura 78.2. Agrupación conceptual de los registros disponibles en System Logs.

Pestaña principal	Información que suele aportar
System	Eventos generales del sistema y subcategorías del sistema operativo, servicios y plataforma.

Pestaña principal	Información que suele aportar
Firewall	Paquetes que coinciden con reglas registradas, incluyendo bloqueos y pases.
DHCP	Negociaciones, renovaciones, fallos de concesión y clientes WAN DHCP.
Authentication	Accesos, errores de autenticación y actividad relacionada.
IPsec	Negociación IKE/CHILD SA y mensajes de strongSwan.
PPP / PPPoE-L2TP Server	Sesiones PPP de interfaces WAN y registros de servicios PPP alojados.
OpenVPN	Inicio, renegociación, errores, conexiones y desconexiones de instancias.
NTP	Sincronización horaria, asociación de peers y avisos temporales.
Packages	Registros de paquetes que utilizan la integración central de logging.
Settings	Preferencias globales, rotación y envío remoto a syslog.

ALCANCE DE LAS PESTAÑAS En la interfaz aquí documentada, System presenta General, Netgate Nexus, Gateways, Routing, DNS Resolver, Wireless, GUI Service y OS Boot. Su disponibilidad y contenido son específicos de la versión o de los servicios activos.

78.3. Cómo se genera, almacena y muestra una entrada

Los eventos provienen de procesos como el kernel, los demonios de servicio y los componentes de la interfaz web. syslogd encamina mensajes a archivos separados. El visor interpreta la línea, ofrece filtros y puede mostrar varias entradas de archivos rotados. La marca temporal y el proceso emisor permiten construir una cronología, pero el texto de un evento siempre debe evaluarse en su contexto.

Elemento de log	Interpretación
Fecha y hora	Orden temporal del evento; verificar zona horaria, NTP y posibles reinicios.
Proceso	Componente emisor; kernel, syslogd, dpinger, OpenVPN, charon, php-fpm, etc.
PID	Identificador de proceso cuando consta; ayuda a separar ejecuciones o reinicios.
Mensaje	Resultado, advertencia, causa probable o acción realizada; no todo mensaje es error.
Severidad	Nivel syslog cuando está presente; no debe confundirse con impacto real.
Cantidad visible	La GUI puede mostrar un subconjunto del fichero. El límite de vista no es retención total.

78.4. System: General y lectura de mensajes de arranque

General reúne eventos heterogéneos del sistema que no se redirigen a otra categoría: inicialización de controladores, cambios de enlace, ejecución de tareas de arranque, sesiones administrativas y notificaciones de servicios. En un arranque es normal observar muchos mensajes kernel, descubrimiento de dispositivos y cambios de interfaces de DOWN a UP.

Patrón genérico	Qué significa y cómo verificar
kernel: link state changed	Cambio de portadora física o de estado lógico. Correlacionar con switch, VLAN y Status → Interfaces.
check_reload_status: Reloading filter	Se solicita regeneración de reglas. Revisar Status → Filter Reload y conectividad.

Patrón genérico	Qué significa y cómo verificar
php-fpm: HOTPLUG	Evento de conexión o desconexión de red; contrastar con DHCP, gateway y switch.
syslogd: restarting	Rotación, reinicio del demonio o cambios de servicio. Revisar continuidad de escritura.
login: Successful login	Evento de acceso: verificar usuario, origen, horario y registro de cambios.
Bootup complete	Marca de fin de proceso de arranque; no certifica que todos los servicios sean funcionales.

PRECAUCIÓN Entradas sobre controladores no encontrados o puertos de hardware opcionales pueden ser inocuas. Evalúe el dispositivo concreto y el síntoma antes de modificar BIOS, firmware o interfaces.

78.5. Subpestañas System

Subpestaña	Lectura práctica
General	Cronología transversal, errores de carga, reinicios, procesos y configuración.
Netgate Nexus	Eventos de la funcionalidad Nexus donde esté incluida; comportamiento dependiente de versión y plataforma.
Gateways	Mensajes de dpinger de inicio de monitorización, alarma y recuperación.
Routing	Avisos de protocolos, rutas, anuncios o cambios de encaminamiento.
DNS Resolver	Mensajes de Unbound y fallos de carga, puertos, forwarders o validación DNSSEC.
Wireless	Eventos de servicio inalámbrico cuando existe interfaz/punto de acceso compatible.
GUI Service	Registros del servicio web de administración y posibles fallos de interfaz.
OS Boot	Mensajes del arranque del sistema operativo, kernel y detección de hardware.

Una subpestaña sin mensajes no es necesariamente un fallo. Puede corresponder a un subsistema inactivo, a una separación distinta de archivos en esa versión o a eventos fuera de la retención actual.

78.6. Firewall: registros de reglas y tráfico

Firewall muestra paquetes que coinciden con reglas configuradas para registrar actividad y diversas reglas internas. Se recomienda correlacionar la interfaz, acción de pass/block, origen, destino, puertos, protocolo y la regla responsable. Los registros de firewall por sí solos no muestran necesariamente todo el tráfico: la visibilidad depende de qué reglas tengan logging activado.

Campo/filtro	Uso diagnóstico
Source / Destination IP	Determina quién inicia la comunicación y hacia dónde se dirige.
Source / Destination Port	Aísla protocolos de aplicación cuando utilizan puertos.
Pass / Block	Distingue tráfico autorizado o rechazado en el punto de evaluación.
Interface	Localiza la dirección del tránsito y el lugar de la coincidencia.
Protocol / TCP Flags	Diferencia TCP/UDP/ICMP y estados de establecimiento TCP.
Rule / Tracker	Identifica la regla que produjo la entrada cuando está disponible.

SEGURIDAD No habilite registro indiscriminado de todo el tráfico en equipos con almacenamiento reducido sin estimar volumen, rendimiento y necesidades de auditoría.

78.7. DHCP y autenticación: asignaciones y accesos

DHCP permite revisar intercambios DHCPv4/DHCPv6 y actividad del cliente DHCP de WAN. Para asignaciones, búsquedas de MAC, DUID y hostnames deben contrastarse con Status → DHCP Leases/DHCPv6 Leases, evitando atribuir todo fallo de conectividad a DHCP.

Authentication ofrece evidencias de accesos válidos, fallidos y otras autenticaciones. Un mismo origen puede generar varios mensajes por sesiones que expiran, reintentos o mecanismos de seguridad; la conclusión debe apoyarse en la secuencia completa y, cuando proceda, en el proveedor RADIUS/LDAP.

78.8. IPsec, PPP, PPPoE/L2TP Server y OpenVPN

Origen	Mensajes habituales y prueba complementaria
IPsec / strongSwan	IKE_SA y CHILD_SA, DPD, propuestas incompatibles; verificar Status → IPsec y reglas UDP 500/4500.
PPP	Negociación, PPPoE o enlaces WAN PPP; verificar Status → Interfaces y el gateway.
PPPoE/L2TP Server	Sesiones de servidores PPP alojados, autenticación y terminación de túneles.
OpenVPN	Inicio, TLS, reconexión y errores; contrastar Status → OpenVPN, rutas, DNS y firewall.

Un mensaje de establecimiento de VPN confirma una fase de negociación. Para declarar servicio operativo debe comprobarse tráfico bidireccional de aplicación, rutas de retorno y, cuando corresponda, NAT.

78.9. NTP, Packages y eventos de tiempo

NTP refleja eventos del demonio de sincronización y operaciones temporales. Ante errores de sincronización, verificar primero WAN, DNS, UDP/123, estado del servicio y peers en Status → NTP. En particular, una advertencia durante el primer arranque puede estar relacionada con ausencia de tiempo válido antes de sincronizarse.

Packages agrupa solo los paquetes que escriben mediante la integración central; otros pueden registrar su salida en System o en archivos específicos, de acuerdo con su implementación. No asumir ausencia de actividad solo porque esta pestaña esté vacía.

78.10. Filtrado avanzado y navegación de resultados

El filtro avanzado del visor se abre con el icono correspondiente en la barra de navegación. Los campos dependen de la pestaña; en registros generales pueden incluir Message, Time, Process, PID y Quantity. El filtro de firewall añade origen, destino, interfaz, protocolo y acciones pass/block.

1. Elegir la pestaña que corresponde al servicio afectado.
2. Abrir Advanced Log Filter y limitar primero por proceso o término sencillo.
3. Añadir una hora aproximada y, si procede, un identificador no sensible o un PID.
4. Aplicar el filtro, ampliar la ventana temporal y revisar líneas anteriores y posteriores.
5. Correlacionar con estado del servicio, tráfico o configuración antes de intervenir.

EXPRESIONES REGULARES El filtro Message admite expresiones regulares; una expresión demasiado amplia puede producir resultados masivos o difíciles de interpretar.

78.11. Settings: preferencias globales de presentación y registro

Opción verificada	Efecto y precaución
Log Message Format	BSD RFC 3164 (predeterminado) o RFC 5424; comprobar compatibilidad del colector.
Forward/Reverse Display	Invierte la presentación cronológica, sin alterar el archivo fuente.

Opción verificada	Efecto y precaución
GUI Log Entries	Número de líneas por vista (predeterminado 50); no determina la retención.
Raw Logs	Muestra texto crudo, con mayor detalle y menor estructuración visual.
Show Rule Descriptions	Oculta, coloca en columna o en segunda fila; puede añadir coste de procesamiento.
Local Logging	La opción de deshabilitar registro local impide guardar logs en el cortafuegos.
Default Log Level	Umbral de severidad; aumentar detalle puede producir ruido o carga.
Log default firewall rules	Habilita registros para categorías de bloqueos internos, según opciones.
Web Server / Configuration Changes	Controla eventos de interfaz web y de modificaciones administrativas.
Reset Log Files	Vacía registros locales; destruye evidencias si no existe respaldo validado.

IMPORTANTE Guardar cambios de Settings antes de pulsar Reset Log Files: el borrado no guarda automáticamente las opciones recién modificadas. No borrar registros durante una investigación.

78.12. Rotación, tamaño, compresión y retención

En versiones modernas de pfSense Plus, los archivos de texto se rotan por tamaño y pueden conservar copias comprimidas. El valor predeterminado documentado para Log Rotation Size es 500 KiB por archivo, sin sumar el espacio ocupado por las rotaciones. El formato de compresión y número de copias determinan el almacenamiento máximo aproximado.

Concepto	Efecto
Archivo activo	Recibe nuevas entradas en /var/log/.
Tamaño de rotación	Al superar el umbral, el archivo se renombra y se crea uno nuevo.
Rotaciones conservadas	Un mayor número alarga el histórico pero aumenta consumo.
Compresión	Reduce espacio; con ZFS puede aprovecharse su compresión del sistema de archivos.
RAM disk en /var	Un apagado incorrecto puede impedir la restauración de registros locales.
Límite de 500 líneas en una vista	Es un límite de presentación, no garantía de conservación de 500 eventos.

78.13. Remote Logging y centralización con Syslog

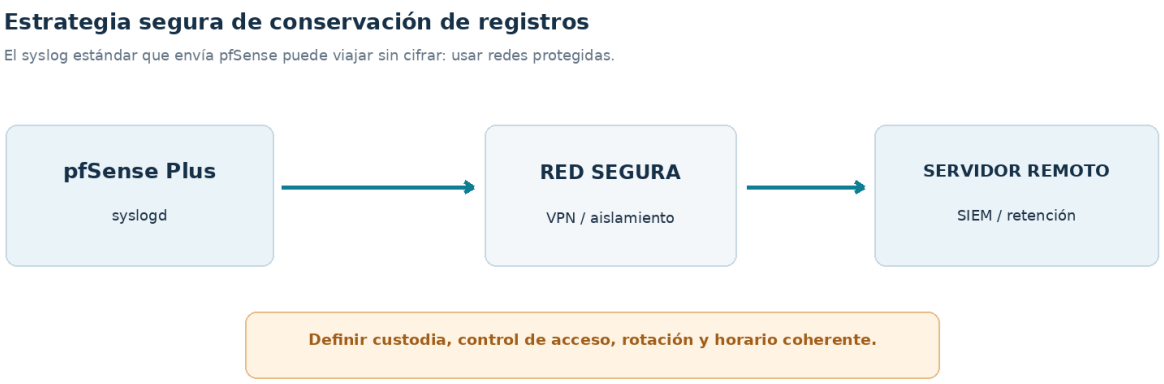


Figura 78.3. Diseño de recogida remota de registros sobre un transporte protegido.

Settings permite enviar categorías elegidas a servidores syslog remotos. La configuración nativa documentada admite hasta tres destinos y usa UDP, normalmente 514 si no se especifica puerto. El envío por este mecanismo no cifra el contenido: una VPN o un canal protegido es imprescindible para redes no confiables. El paquete syslog-ng ofrece opciones adicionales, incluidas modalidades cifradas.

Ajuste	Decisión administrativa
Source Address	Auto/Any suele ser adecuado; en IPsec policy-based puede requerirse IP incluida en el selector Phase 2.
IP Protocol	Preferencia IPv4/IPv6 cuando se fija dirección de origen.
Remote Log Servers	Registrar destino(s) accesibles por red protegida; por defecto UDP/514.
Remote Syslog Contents	Seleccionar System, Firewall, DHCP, VPN, DNS, NTP y otras categorías pertinentes.
Comprobación	Generar un evento inocuo, verificar llegada, marca temporal, equipo de origen y almacenamiento.

78.14. Herramientas de consola y conservación de evidencias

En pfSense Plus moderno, los archivos de /var/log/ se pueden consultar con herramientas estándar. No se recomienda editarlos a mano ni borrar archivos directamente para ahorrar espacio; utilizar los mecanismos oficiales de rotación y mantenimiento.

Comando de solo lectura	Propósito
tail -F /var/log/system.log	Sigue el log general incluso si rota.
grep -i "error" /var/log/system.log	Busca texto sin diferenciar mayúsculas.
tail -F /var/log/filter.log	Sigue entradas del filtro de paquetes.
bzgrep -i "error" /var/log/system.log.0.bz2	Busca en una rotación bzip2 (si se usa ese formato).
ls -lh /var/log/	Inspección de tamaños y rotaciones presentes.

MANEJO DE PRUEBAS Al exportar evidencias, preservar originales y trabajar con copias anonimizadas. No incorporar contraseñas, tokens, usuarios, topologías ni direcciones operativas en informes públicos.

78.15. Diagnóstico correlacionado: enlace, DHCP, DNS y VPN

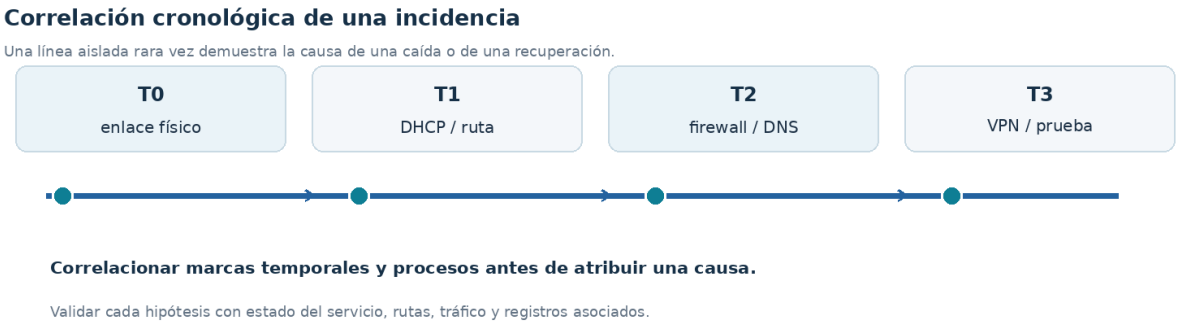


Figura 78.4. Orden de correlación de eventos frente a un corte de conectividad.

Ante una pérdida de conexión, el orden de comprobación más útil suele ser enlace físico → DHCP y gateway → regeneración de reglas → DNS → túneles VPN y servicios. Los eventos pueden aparecer con segundos de diferencia y no siempre siguen una secuencia idéntica; considerar concurrencia y retrasos de escritura.

1. Anotar el momento aproximado de la incidencia con la zona horaria utilizada por el cortafuegos.
2. Consultar System / General u OS Boot para descartar reinicios y cambios de enlace.
3. Consultar System / Gateways y Status → Gateways para determinar si hubo pérdida de monitorización.
4. Cruzar DHCP, DNS Resolver y Firewall para descartar falta de direccionamiento o bloqueo.
5. Revisar OpenVPN/IPsec si el incidente afecta a sedes o usuarios remotos.
6. Probar conectividad local y remota, comprobar tiempos y conservar evidencias antes de modificar configuración.

78.16. Patrones técnicos frecuentes y su interpretación

Patrón abstracto	Hipótesis y comprobación (no diagnóstico definitivo)
Repeated WAN link up/down	Posible inestabilidad de enlace, puerto o negociación física; revisar cableado y switch.
No default gateway available	Ausencia transitoria de gateway válido; contrastar tabla de rutas y DHCP WAN.
DNS servers not available	Fallo de resolución o estado aún no inicializado; probar salida IP y consulta a DNS.
DNS Resolver: address in use	Conflicto de escucha de puerto o proceso anterior; inspeccionar sockets y servicio antes de reiniciar.
NTP command timed out	No respuesta de fuente horaria, DNS o conectividad; revisar peers NTP, reloj y UDP/123.
VPN endpoints changed	Actualización del origen o destino por cambio WAN; confirmar reconexión y rutas.
Firmware or boot environment notice	Analizar compatibilidad de firmware/DTB y notas oficiales antes de instalar actualizaciones.
Configuration Change	Evento de auditoría que debe correlacionarse con el cambio aprobado y su horario.

CONTROL DE RIESGO Ninguna advertencia abstracta justifica por sí sola modificar parámetros de kernel, reinstalar paquetes ni reiniciar servicios críticos. Priorice acciones no disruptivas.

78.17. Procedimientos profesionales de explotación

A. Fallo intermitente de salida a Internet

1. Examinar cronología WAN en General y Gateways.
2. Comprobar Estado de Interfaces y del gateway sin forzar renovaciones DHCP.
3. Buscar eventos de cambio de IP, recarga de reglas y reinicio de túneles.
4. Si hay repetición, registrar frecuencia y comprobar capa física, monitor IP y operador.

B. Problema de resolución DNS

1. Filtrar DNS Resolver por warning o error.
2. Verificar que Unbound funciona y escucha en el puerto esperado.
3. Comprobar consulta DNS interna y contra forwarder configurado si se utiliza.
4. Anotar si hay correlación temporal con cambios de WAN, firewall o hora.

C. VPN establecida pero tráfico no operativo

1. Buscar eventos de establecimiento y renegociación en IPsec/OpenVPN.
2. Validar estado, túnel y negociación; diferenciar control y datos.
3. Comparar rutas, selectores, reglas y retorno en ambos extremos.
4. Comprobar pérdida y MTU sin modificar cifrados en producción.

D. Auditoría de cambio administrativo

1. Identificar evento de cambio autorizado y su instante.
2. Preservar log de autenticación y registro de cambios asociado.
3. Correlacionar con config history y estado posterior del servicio.
4. Exportar una versión anónima y guardar el original en repositorio protegido.

78.18. Seguridad, protección de datos y cadena de custodia

Los logs pueden contener identidades, direcciones de red, identificadores de hardware, nombres de dispositivos, rutas, eventos de acceso y detalles de configuración. Deben tratarse como información operativa sensible, aplicando control de acceso de mínimo privilegio, cifrado de transporte y almacenamiento, retención definida y auditoría de consultas.

La anonimización de informes debe reemplazar topologías y nombres por ejemplos de documentación (p. ej. 192.0.2.10, 198.51.100.20 y example.com), sin conservar claves originales, direcciones MAC reales ni identificadores derivados. Antes de borrar los logs originales, comprobar si existen obligaciones legales o de investigación.

78.19. Lista de comprobación y medidas de continuidad

Verificación	Resultado esperado
Sincronización NTP y zona horaria	Timestamps comparables entre servicios y servidores.
Persistencia del registro local	Eventos recientes visibles y rotaciones presentes.
Tamaño/rotaciones definidos	Histórico compatible con almacenamiento y política.
Syslog remoto verificado	El receptor almacena eventos y el canal está protegido.
Registro de cambios activado	Las actuaciones administrativas quedan trazadas.
Prueba de recuperación	Se sabe dónde consultar logs si falla la GUI.
Política de acceso y custodia	Personal autorizado, integridad y periodo documentados.

78.20. Glosario de términos

Término	Definición
Syslog	Mecanismo de recogida y reenvío de mensajes de procesos.
Severity / Facility	Prioridad y clasificación de mensajes de syslog.
PID	Identificador numérico de una ejecución de proceso.
Log rotation	Cambio del archivo de escritura y conservación de versiones previas.
dpinger	Servicio de supervisión de gateways de pfSense.
Filterlog	Registro del motor de filtrado de paquetes.
SIEM	Plataforma para centralizar, correlacionar y alertar sobre eventos de seguridad.
SLA/MTTR	Objetivos de servicio y tiempo medio de recuperación utilizados en explotación.

78.21. Referencias técnicas oficiales

Netgate — System Logs

Netgate — Log Settings

Netgate — Remote Logging with Syslog

Netgate — Working with Log Files

Netgate — Viewing the Firewall Log

Netgate — Raw Filter Log Format

Netgate — DHCP Logs

Netgate — Gateway Logs

Netgate — IPsec Logs

Netgate — OpenVPN Logs

Netgate — NTP Logs

Netgate — Package Logs

Netgate — Troubleshooting IPsec Logs

Los controles específicos de una versión o de un paquete deben comprobarse en la ayuda integrada de la instalación antes de ejecutarlos.

Itinerarios de consulta recomendados

Si se investiga…	Consulta recomendada
Pérdida de enlace o failover	System Logs + Gateway Logs + Status → Interfaces y Gateways.
Bloqueos del cortafuegos	Viewing the Firewall Log + Raw Filter Log Format.
Problemas DHCP / DNS	DHCP Logs + DNS Resolver y estado de los servicios.
Incidencias de VPN	IPsec Logs / OpenVPN Logs + estado de conexiones y rutas.
Auditoría y conservación	Log Settings + Remote Logging + Working with Log Files.

79 Status → Traffic Graph

Tráfico en tiempo real · interfaces · direcciones IP · análisis de congestión · diagnóstico de redes

La página Traffic Graph presenta un gráfico de utilización instantánea de la interfaz elegida y una tabla orientativa de actividad por dirección IP. Es una herramienta de observación inmediata: ayuda a localizar picos, confirmar circulación de tráfico y decidir qué comprobación adicional realizar. No sustituye al histórico RRD ni a un sistema de contabilidad de tráfico por usuario.

CRITERIO DE INTERPRETACIÓN Una gráfica que muestra actividad no identifica por sí sola al usuario o aplicación responsable. El contexto depende de la interfaz observada, la dirección del tráfico, el NAT, las rutas, la agregación de muestras y el periodo de observación.



Figura 79.1. Cadena conceptual de observación instantánea y sus límites.

79.1. Objetivo y ruta de acceso

Ruta exacta: Status → Traffic Graph. Se muestra una interfaz cada vez, seleccionable mediante el control Interface. La información se actualiza continuamente mientras está activa la visualización; para observar varias WAN a la vez puede utilizarse el widget Traffic Graphs del Dashboard, o varias ventanas independientes.

Los datos son tasas de transferencia actuales, útiles para responder preguntas como: «¿Está pasando tráfico por esta WAN?», «¿Se está consumiendo ancho de banda?» o «¿Qué direcciones aparecen en esta muestra?». Para reconstruir un incidente ocurrido ayer deben consultarse Monitoring, los logs o una plataforma de telemetría.

79.2. Arquitectura técnica: qué mide y qué no mide

Elemento	Lectura correcta
Gráfico de interfaz	Representa la tasa de tráfico que pasa por la interfaz seleccionada en función del tiempo.
Tabla por host	Ofrece muestras de direcciones vistas momentáneamente; no constituye un inventario completo ni una clasificación forense.
Tráfico in/out	Siempre debe interpretarse desde la perspectiva de la interfaz que se está observando.
NAT y túneles	Pueden cambiar qué direcciones son visibles y dónde se contabiliza cada paquete.
Datos históricos	Los mantiene Status → Monitoring mediante RRD, no esta gráfica instantánea.

79.3. La página: bloques, barra y controles

La pantalla contiene Graph Settings, el botón Save y el bloque Traffic Graph. Graph Settings se divide en una fila de selección (Interface, Sort by, Filter, Display y Mode) y otra de comportamiento (Background updates, Invert in/out y Graph Smoothing). La gráfica inferior incluye la leyenda de los sentidos de tráfico y una tabla de actividad por dirección.

El icono de ayuda en la cabecera abre documentación contextual. Los nombres de entradas visibles en el cuadro de configuración dependen de las interfaces del firewall y de la versión instalada.

79.4. Graph Settings: Interface

Interface elige el origen de la medición. Seleccionar WAN permite observar el tráfico que entra o sale del enlace exterior, mientras que una interfaz LAN, VLAN o VPN —cuando aparezca en la lista de esa instalación— ofrece otra perspectiva. La página se actualiza al cambiar de interfaz según describe Netgate.

ATENCIÓN En escenarios Multi-WAN, un valor bajo en WAN principal no demuestra inactividad global: puede existir tráfico por la segunda WAN o por una interfaz virtual distinta. Comprobar también Status → Gateways y las reglas de encaminamiento.

79.5. Graph Settings: Sort by

Valor documentado	Qué hace	Interpretación
Bandwidth In	Ordena las filas de hosts según su tasa de entrada observada.	Útil al investigar recepción/descargas según la interfaz elegida.
Bandwidth Out	Ordena las filas de hosts por tasa de salida observada.	Útil para picos de envío o tráfico saliente.

El orden no modifica los paquetes ni aplica limitación: solamente reorganiza la presentación del cuadro de direcciones en tiempo real.

79.6. Graph Settings: Filter (Local, Remote, All)

Netgate define Local y Remote respecto a la subred primaria de la interfaz seleccionada: Local indica direcciones comprendidas en esa red y Remote las que quedan fuera; All muestra ambos grupos. «Local» no equivale automáticamente a «IP privada», «usuario corporativo» o «equipo de la sede». En WAN detrás de otro router una dirección privada puede ser Local para la WAN sin pertenecer a la LAN interna.



Figura 79.2. La pertenencia local/remota depende del prefijo de la interfaz elegida.

Filtro	Resultado	Precaución
Local	Direcciones pertenecientes a la red de la interfaz.	La red WAN puede estar detrás de NAT.
Remote	Direcciones fuera de la red de esa interfaz.	No es un detector de origen geográfico.
All	Combina ambos conjuntos visibles.	No convierte la muestra en historial exhaustivo.

79.7. Graph Settings: Display

Valor	Origen habitual del nombre mostrado
IP Address	Dirección numérica del host.
Host Name	Nombre corto conocido por mapeos DHCP estáticos u overrides de DNS.
Description	Descripción asociada a los mapeos u overrides disponibles.
FQDN	Nombre de dominio completo, si existe información correlacionable.

Estos campos dependen de los registros conocidos por el firewall. Una ausencia de nombre no implica ausencia de equipo ni error DNS; el identificador visible también puede variar tras NAT. La documentación oficial relaciona los nombres con mapeos estáticos DHCP y sobrescrituras de DNS Resolver o DNS Forwarder.

79.8. Graph Settings: Mode

rate (standard) es el modo ordinario de presentación de tasas. Algunas implementaciones han ofrecido alternativas experimentales basadas en iftop. Comprobar qué modos admite y soporta la compilación instalada antes de utilizarlos.

Para documentación de problemas de rendimiento, registrar siempre el modo exacto utilizado. Resultados procedentes de motores de muestreo distintos pueden no coincidir exactamente con los contadores persistentes de interfaz.

79.9. Controls: Background updates

Background updates regula el comportamiento cuando la visualización deja de estar en primer plano. El valor visible «Clear graphs when not visible» indica una política de limpieza de datos gráficos fuera de vista. El detalle de otras entradas de ese desplegable puede variar según versión: no debe inferirse de la captura un listado adicional concreto.

Mantener actualizaciones en segundo plano puede consumir más recursos del navegador y de la página de administración. Por el contrario, al limpiar los datos cuando se oculta la vista, se perderá continuidad visual de la traza visible; esto no elimina los registros RRD de Monitoring.

79.10. Controls: Invert in/out

Invert in/out determina la disposición visual de las dos direcciones. Con On, el flujo de salida se dibuja por debajo de cero para diferenciarlo del flujo de entrada. Es una inversión gráfica de signo: los paquetes salientes no se convierten en «tráfico negativo» ni se aplica una resta de consumo.

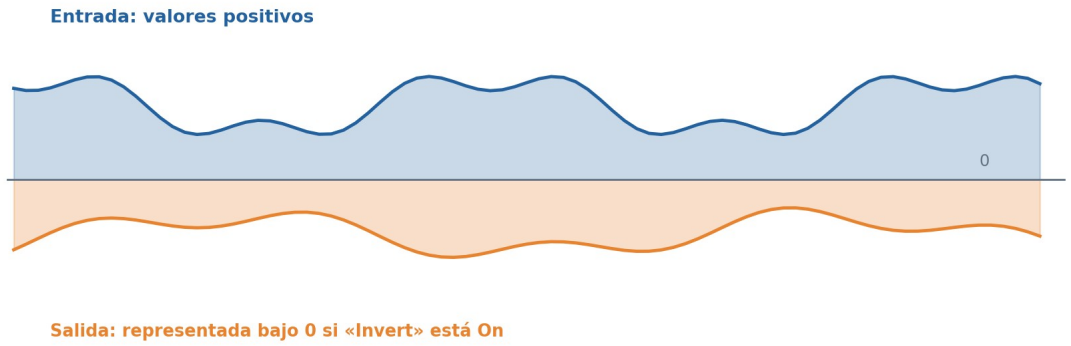


Figura 79.3. Separación de tráfico entrante y saliente al invertir la representación.

79.11. Controls: Graph Smoothing

El control deslizante Graph Smoothing ajusta el suavizado de la representación. Un trazado más suave puede hacer más legible la tendencia, pero disimular ráfagas muy breves. Para investigar picos, repetir la observación con suavizado bajo y contrastar con contadores de interfaz y captura de paquetes. No debe interpretarse el suavizado como una modificación de la red.

79.12. Save: persistencia de la vista

El botón Save guarda las preferencias de visualización. No crea reglas, no modifica el ancho de banda del enlace ni cambia rutas. Antes de guardar, verificar que la interfaz y el tipo de filtro corresponden al propósito del análisis; registrar la selección cuando se recopilen evidencias para comparar resultados.

79.13. Traffic Graph: leyenda y ejes

La leyenda identifica cada serie por su interfaz y sentido, habitualmente «(in)» y «(out)». El eje horizontal muestra tiempo; el vertical muestra una tasa de transferencia. Si está activa la inversión, uno de los sentidos se representa bajo el cero. La escala puede reajustarse automáticamente, lo que dificulta comparar dos capturas sin conocer el rango utilizado.

Una gráfica plana puede significar ausencia de tráfico, una interfaz equivocada, ventana demasiado corta, captura todavía no iniciada o problemas con la actualización de la página. La comprobación se completa en Status → Interfaces y en Diagnostics → Packet Capture.

79.14. Unidad de medida: bits, bytes, tasas y volumen

Concepto	Definición útil	Ejemplo ficticio
bit/s (bps)	Bits transmitidos por segundo; unidad habitual de la tabla.	8 Mbit/s = 8 millones de bits por segundo.
byte/s (B/s)	Bytes por segundo: 1 byte = 8 bits.	8 Mbit/s ÷ 8 = 1 MB/s decimal.
Volumen transferido	Tasa × tiempo; estimación si la tasa es estable.	50 Mbit/s × 10 s ÷ 8 = 62,5 MB.
Mbit/s frente a MiB/s	Mbit usa múltiplos decimales; MiB usa base 2.	No confundir en auditorías de capacidad.

PRECISIÓN La relación de tasa y volumen solo es exacta si se conoce la tasa instantánea a lo largo de todo el intervalo. Una captura aislada de 50 Mbit/s no permite calcular el consumo del día.

79.15. Tabla Host IP / Bandwidth In / Bandwidth Out

La tabla contigua es una instantánea de direcciones y tasas. Host IP identifica la dirección mostrada según Display; Bandwidth In y Bandwidth Out expresan las tasas de cada sentido, relativas a la interfaz. Netgate advierte que las conversaciones breves pueden no llegar a mostrarse y que la tabla no está pensada para atribución histórica exhaustiva.

Columna	Lectura	Limitación
Host IP	Dirección o representación nominal según Display.	NAT, gateway intermedio y overrides afectan a la identificación.
Bandwidth In	Tasa de entrada para la IP observada.	El sentido depende de la interfaz seleccionada.
Bandwidth Out	Tasa de salida para la IP observada.	No equivale a bytes totales ni coste mensual.

79.16. Efectos del NAT, CGNAT y tráfico en túneles

En la WAN pública, varios equipos internos pueden aparecer agregados bajo la dirección exterior del cortafuegos o del equipo aguas arriba. En un router con CGNAT, las direcciones exteriores y el puerto origen visibles pueden pertenecer a un tramo intermedio y no identificar directamente un cliente interno. Un túnel VPN añade una capa de encapsulación: la interfaz física contabiliza los paquetes exteriores y la interfaz de túnel, si es seleccionable, muestra una perspectiva distinta.

Cuando se necesite localizar al host real, correlacionar el instante de interés con Diagnostics → States, reglas NAT, DHCP Leases y, si procede, capturas de tráfico; utilizar la información con criterio de minimización y permisos administrativos.

79.17. Tiempo real frente a histórico de Monitoring

Aspecto	Traffic Graph	Status → Monitoring
Objetivo	Respuesta inmediata, segundos recientes.	Tendencia y comparación histórica.
Persistencia	No constituye registro duradero.	Series guardadas en bases RRD.
Granularidad	Muestras dinámicas de corta duración.	Resolución consolidada según antigüedad.
Detalle por host	Muestra fugaz de IP; no auditoría completa.	Por defecto métricas agregadas de interfaces y servicios.
Uso típico	Confirmar un pico activo.	Comparar horas, días o semanas.

79.18. Diseño de una comprobación segura paso a paso

1. Confirmar horario y objetivo: interfaz, destino o servicio afectado; no cambiar todavía reglas ni rutas.
2. Abrir Status → Traffic Graph y seleccionar la interfaz que realmente transporta el flujo.
3. Comenzar con Filter = All, Display = IP Address y Sort by = Bandwidth In, documentando el modo.
4. Observar varias actualizaciones; después ordenar por Bandwidth Out para identificar el sentido dominante.
5. Comparar con Status → Interfaces (contadores), Gateways (RTT/pérdida) y Monitoring (evolución).

6. Si se necesita atribución: revisar Diagnostics → pfTop / States y realizar una captura breve, con permisos.
7. Registrar hora, interfaz, tasa observada y conclusiones, distinguiendo hecho de hipótesis.

79.19. Procedimiento: detectar congestión en una WAN

Situación: la organización percibe lentitud generalizada y el gráfico de WAN presenta picos cercanos a la capacidad contratada. Primero confirmar que el enlace elegido es el activo, que el caudal del ISP se mide en unidades comparables y que no hay pérdida importante en Status → Gateways. Si hay subida saturada, revisar colas o limitadores; no proponer Traffic Shaping sin verificar la velocidad real y el comportamiento de cada dirección.

Una subida al 100 % puede elevar latencia y jitter por bufferbloat sin que el gateway aparezca inmediatamente «Down». Medir calidad con un destino conocido y, si es posible, realizar prueba controlada fuera de horario productivo.

79.20. Procedimiento: confirmar failover Multi-WAN

1. Comprobar en Status → Gateways la situación de WAN principal y secundaria, sin forzar cambios.
2. Observar la gráfica de cada interfaz por separado; buscar tráfico en la WAN que realmente se espera utilizar.
3. Correlacionar el comportamiento con reglas de policy routing, gateway groups y tabla de estados.
4. Contrastar sesiones VPN que puedan mantener rutas o gateways específicos.
5. Para pruebas planificadas, registrar un plan de reversión y una vía de administración alternativa.

79.21. Procedimiento: verificar un enlace VPN

Para una incidencia entre sedes, comparar la WAN física y la interfaz del túnel, si está expuesta como origen de gráfica. Un pico en WAN demuestra intercambio exterior, no necesariamente tráfico de aplicación hacia la red remota. Confirmar la sesión en Status → OpenVPN, IPsec o WireGuard, las rutas, las reglas y una prueba real hacia el recurso remoto de documentación 203.0.113.20.

79.22. Procedimiento: investigar envío inesperado de datos

Si destaca Bandwidth Out de forma anómala, verificar ventana horaria, destino y si es un proceso autorizado (copias de seguridad, replicación, sincronización). Revisar States y logs antes de concluir que hay exfiltración. Una IP que aparece en la muestra no equivale por sí misma a evidencia de ataque ni identifica un usuario inequívocamente.

79.23. Otras herramientas que complementan el análisis

Herramienta	Para qué sirve	Nota práctica
Diagnostics → pfTop	Visualiza estados activos y tasas de sesiones.	Útil cuando la tabla de hosts no basta.
Diagnostics → States	Relación entre conexiones, NAT y reglas.	No eliminar estados por simple inspección.
Diagnostics → Packet Capture	Observación de paquetes y protocolos.	Limitar tiempo, tamaño y exposición de datos.
Status → Interfaces	Contadores de entrada, salida y errores.	Permite distinguir flujos de fallos físicos.
Status → Gateways	RTT, pérdida de paquetes y estado de enlaces.	Importante para Multi-WAN y microcortes.
Status → Monitoring	Tendencias RRD, métricas y percentiles.	No equivale a la muestra actual.
ntopng / NetFlow / colector	Análisis persistente más detallado, si está instalado.	Requiere recursos y definición de retención.

79.24. Matriz de diagnóstico y causa probable

Observación	Posibles causas	Primera validación
No aparecen muestras	Interfaz inactiva, sin tráfico, filtro restrictivo o actualización detenida.	Cambiar a All, contrastar Interfaces y estado del navegador.
Un único host domina	NAT, host realmente activo o visibilidad limitada.	Consultar States y posición de la interfaz.
WAN saturada	Carga legítima, backups, mala política QoS o capacidad insuficiente.	Comparar uplink/downlink, gateways y duración.
El tráfico oscila	Ráfagas de aplicación, ventana de muestreo o suavizado.	Observar más tiempo y reducir smoothing.
VPN conectada sin datos	Rutas, reglas, DNS, selectores o tráfico de aplicación ausente.	Estado VPN, rutas, firewall y prueba de aplicación.
Contadores divergen	NAT, encapsulación, método de muestreo o periodos diferentes.	Normalizar unidades e interfaz/ventana comparadas.

79.25. Metodología de correlación sin modificar producción



Figura 79.4. Secuencia operativa desde el pico visible hasta la verificación de causa.

Separar el dato observado («en el intervalo se mostró un máximo de X Mbit/s») de la interpretación («podría tratarse de una transferencia de copia»). La confirmación exige otra fuente: estados, logs, paquete, aplicación o contador de destino. Evitar reinicios, deshabilitar reglas y cambios de routing sin autorización, ventana de mantenimiento y reversión documentada.

79.26. Rendimiento del propio panel de administración

El navegador renderiza una gráfica que se actualiza frecuentemente. Sesiones prolongadas, múltiples pestañas y resolución elevada pueden incrementar el trabajo del cliente y la carga de consulta. Ajustar Background updates cuando el administrador trabaje en otras pestañas; no mantener visualizaciones abiertas indefinidamente como sustituto de un sistema de monitorización dedicado.

79.27. Seguridad, privacidad y control de acceso

Las direcciones IP, nombres, volúmenes y horarios pueden constituir información operativa sensible. Otorgar acceso a Status según roles mínimos, evitar capturas o exportaciones innecesarias y publicar ejemplos desidentificados. No introducir capturas de producción, topologías privadas, tokens o nombres reales en documentación distribuida.

79.28. Escenarios empresariales resueltos

Escenario	Lectura de Traffic Graph	Acción recomendada
Sede con dos proveedores	Comprobar que el tráfico se desplaza al enlace esperado.	Revisar Gateways y grupos antes de declarar failover correcto.
Copia de seguridad nocturna	Pico de salida temporal.	Relacionar con ventana de backup y logs del servidor.

Escenario	Lectura de Traffic Graph	Acción recomendada
Teletrabajo por VPN	Tráfico físico y túnel no siempre equivalentes.	Validar túnel, rutas, NAT y acceso al servicio real.
Videoconferencia entrecortada	Variación rápida y posible saturación subida.	Correlacionar RTT, pérdida y QoS.
Sospecha de tráfico irregular	Host visible sólo en determinados instantes.	Conservar evidencias mínimas y revisar States sin atribuir automáticamente un ataque.

79.29. Comprobaciones de aceptación

1. La interfaz seleccionada se corresponde con el camino del tráfico previsto.
2. El filtro Local/Remote/All se ha entendido respecto al prefijo primario de esa interfaz.
3. Las unidades en el gráfico y los contadores comparados están normalizadas.
4. Los valores de salida bajo cero se reconocen como inversión visual, no tráfico negativo.
5. Las conclusiones por IP se corroboran con una fuente adicional cuando hay NAT o túneles.
6. No se han modificado reglas, rutas ni servicios durante la mera supervisión.

79.30. Glosario esencial

Término	Definición
Throughput	Caudal efectivo transferido por unidad de tiempo.
Ingress/Egress	Entrada o salida, siempre desde el punto de observación.
Muestreo	Observación parcial en intervalos; puede perder flujos cortos.
Suavizado	Transformación de visualización que reduce variación aparente.
NAT	Traducción de direcciones que altera qué IP se ve en cada interfaz.
RRD	Base circular con retención y consolidación de series de tiempo.
pfTop	Herramienta de visualización de estados de PF en tiempo real.

79.31. Referencias técnicas y oficiales

Netgate — Traffic Graphs

Netgate — Monitoring Graphs

Netgate — Monitoring Bandwidth Usage

Netgate — Dashboard Widgets

Netgate — Using pfTop

Netgate — Multi-WAN: Verifying Functionality

Netgate — Monitoring Status Menu

Netgate — Working with Graphs

Netgate — Graph Settings (Monitoring)

Las opciones del menú y su disponibilidad pueden variar entre versiones y paquetes de pfSense Plus. Debe verificarse la versión instalada antes de aplicar ajustes avanzados.

80 Status → UPnP IGD & PCP

Supervisión de asignaciones dinámicas · NAT automatizado · control de exposición · diagnóstico de conectividad

El panel **Status → UPnP IGD & PCP** ofrece una lectura operativa de los puertos que los dispositivos internos han solicitado abrir mediante UPnP IGD, PCP o NAT-PMP. Su utilidad es doble: verificar que existe una asignación dinámica y detectar exposiciones entrantes que no forman parte del inventario de reglas NAT creadas manualmente.

PUNTO DE PARTIDA Cuando el servicio está deshabilitado, la página no presenta asignaciones, sino un aviso con acceso directo a Services → UPnP IGD & PCP. Habilitarlo es una decisión de seguridad, no un requisito para que el cortafuegos funcione.

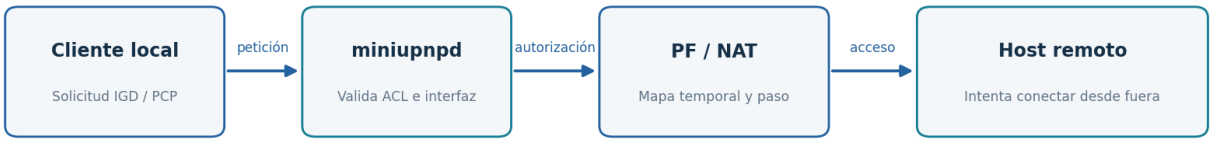


Figura 80.1. Flujo conceptual de solicitud, autorización y exposición dinámica.

80.1. Objeto del panel y ruta de acceso

Ruta exacta: Status → UPnP IGD & PCP. Esta página pertenece al área de supervisión. La configuración se realiza en **Services → UPnP IGD & PCP**; el estado del proceso de servicio se consulta también en **Status → Services**. No debe confundirse observar asignaciones con configurar qué clientes pueden solicitarlas.

Vista	Pregunta a la que responde
Status → UPnP IGD & PCP	¿Qué asignaciones dinámicas de puertos figuran actualmente?
Services → UPnP IGD & PCP	¿Quién puede pedirlas, por qué protocolo y sobre qué WAN?
Status → Services	¿El proceso miniupnpd está registrado y en ejecución?
Status → System Logs → System / Routing	¿Qué eventos o errores comunica miniupnpd?
Status → System Logs → Firewall	¿Se observan conexiones que coinciden con reglas registradas?

80.2. Lectura de la pantalla sin servicio activo

El mensaje **«Service is currently disabled. It can be enabled here: Services > UPnP IGD & PCP.»** indica que el servicio está deshabilitado en la configuración de pfSense. El enlace conduce al formulario del servicio. El icono de cerrar de la notificación oculta el aviso en la interfaz; no habilita ni modifica el daemon.

La cabecera identifica la ruta y ofrece accesos generales de pfSense, incluida la ayuda contextual. La información y las acciones disponibles dependen de las asignaciones que el servicio exponga; no debe suponerse que existan controles individuales de eliminación en todas las versiones.

INTERPRETACIÓN CORRECTA Un servicio deshabilitado no implica una avería; puede ser una decisión deliberada de endurecimiento. Tampoco equivale a que no existan redirecciones NAT manuales, reglas de firewall o servicios accesibles por otros mecanismos.

80.3. Protocolos involucrados y funcionamiento de miniupnpd

pfSense utiliza el daemon **miniupnpd** para gestionar las peticiones de mapeo de clientes autorizados. **UPnP IGD** emplea descubrimiento SSDP y consultas HTTP/SOAP; **PCP** permite controlar mapeos y es sucesor de **NAT-PMP**, con el que mantiene compatibilidad en este contexto. El resultado puede traducirse en reglas dinámicas NAT y de paso para permitir tráfico entrante desde redes remotas.

Protocolo / componente	Puerto habitual	Función y cautela
SSDP / UPnP IGD	UDP 1900	Descubrimiento; a menudo multicast. Abrir únicamente desde las interfaces internas previstas.
UPnP IGD HTTP/SOAP	TCP 2189	Consultas y órdenes al servicio, según la implementación de Netgate.
PCP y NAT-PMP	UDP 5351	Petición, renovación o eliminación de mapeos por el cliente.
Tráfico de la aplicación	Puerto variable TCP/UDP	Puerto expuesto dinámicamente; no confundirlo con el puerto de control del protocolo.

SEGURIDAD Nunca publicar los puertos de control 1900/2189/5351 desde Internet como supuesto remedio general. El servicio se diseña para solicitudes de clientes en interfaces internas autorizadas. Las reglas requeridas dependen del diseño y de la política LAN.

80.4. Qué ocurre cuando un cliente solicita abrir un puerto

1. El software local envía una petición al daemon a través de una interfaz interna donde está permitido el protocolo.
2. miniupnpd comprueba los protocolos activos, las restricciones de la ACL aplicables y la dirección WAN publicable.
3. Si la petición se admite, se crea o actualiza un mapeo externo hacia la dirección y puerto internos que procedan.
4. El administrador puede observar el mapeo en Status → UPnP IGD & PCP, cuando existe y se encuentra activo.
5. La conexión desde Internet todavía depende de la ruta exterior completa, posibles routers aguas arriba y filtrado adicional.
6. El mapeo puede renovarse, caducar o ser retirado; el ciclo concreto depende del protocolo, el cliente y la implementación.

80.5. Pantalla con asignaciones: columnas documentadas

La documentación de Netgate muestra la tabla **«Active UPnP IGD & PCP/NAT-PMP Port Maps»** cuando existen asignaciones. Los siguientes ocho encabezados proceden de esa vista oficial; no aparecen en la captura del servicio deshabilitado.

Columna	Significado operativo	Comprobación sugerida
Ext Interface	Interfaz exterior asociada a la redirección.	Confirmar que es la WAN prevista.
Ext Port	Puerto de entrada anunciado en el lado exterior.	Identificar conflictos y servicios publicados.
Int IP	Dirección interna de destino.	Vincularla al inventario autorizado.
Int Port	Puerto del servicio de destino.	Comprobar proceso escuchando y firewall local.
Protocol	Transporte (por ejemplo TCP o UDP).	No asumir que abrir TCP abre también UDP.
Source IP	Restricción de origen remoto; «any» permite cualquier IP como origen del mapeo.	No interpretarla como IP que creó la regla.
Source Port	Restricción de puerto de origen, si existe.	«any» no es el puerto de aplicación local.
Description	Etiqueta proporcionada para identificar la asignación.	Tratarla como información informativa, no fiable para auditoría de identidad.

80.6. Ejemplo didáctico de una redirección dinámica



Figura 80.2. Correspondencia puerto exterior → destino interno, con direcciones reservadas para documentación.

En este ejemplo exclusivamente documental, una petición TCP para **198.51.100.10:53020** se entrega al servicio **192.0.2.20:32400**. La coincidencia de puertos no es obligatoria: Ext Port e Int Port pueden ser distintos. La elección de puerto y protocolo debe justificarse por el servicio real y limitarse mediante políticas de acceso.

ALCANCE La presencia de una fila en Status confirma que existe una asignación reportada por el servicio; no certifica que un tercero pueda establecer una conexión ni que el equipo destinatario responda. La prueba debe hacerse desde una red externa controlada.

80.7. Diferenciar asignaciones dinámicas y NAT permanente

Aspecto	Dinámica UPnP / PCP	Redirección manual NAT
Creación	Petición de cliente local y autorización del daemon.	Configuración explícita del administrador.
Vigencia	Puede caducar o renovarse según protocolo y cliente.	Permanece hasta modificación o deshabilitación.
Cambio de destino	Un cliente autorizado puede solicitar otros puertos/destinos dentro de su alcance.	El administrador controla cada destino.
Control de seguridad	ACL del servicio y reglas de firewall complementarias.	Reglas NAT/filtro definidas y revisables.
Supervisión	Status → UPnP IGD & PCP.	Firewall → NAT y reglas asociadas.

La lista dinámica no sustituye un inventario de reglas manuales ni una auditoría de exposición. Tampoco debe entenderse como un registro histórico completo de todas las solicitudes efectuadas en días anteriores.

80.8. Activación deliberada: controles relacionados

En **Services → UPnP IGD & PCP**, el interruptor principal **Enable port mapping service** requiere que al menos uno de los protocolos **UPnP IGD** o **PCP/NAT-PMP** esté habilitado. **External Interface** debe señalar la WAN que contiene el gateway predeterminado; **Internal Interfaces** delimita dónde residen los clientes. No se recomienda habilitar el servicio de forma global para resolver una incidencia aislada sin determinar qué aplicación lo necesita.

Ajuste relacionado	Implicación para la supervisión
Enable + protocolo autorizado	Sin ambos requisitos, no hay mecanismo funcional de mapeo.
External Interface	Identifica la salida WAN destinada a anunciar mapeos; Multi-WAN requiere cautela.
Internal Interfaces	Delimita interfaces donde se escuchan peticiones de clientes.
Default Deny + ACL Entries	Reduce qué clientes IPv4 y puertos están autorizados; no controla clientes IPv6.
Enable STUN / Override WAN Address	Ayuda en diseños compatibles detrás de 1:1 NAT, no elude CGNAT restrictivo.
Firewall Logs	Registra conexiones que coinciden con reglas generadas; puede producir volumen significativo.

80.9. Seguridad: privilegio de publicar servicios

Una aplicación en un equipo con acceso a UPnP IGD & PCP puede solicitar que se permita tráfico entrante. Por ello, este mecanismo debe considerarse una **delegación de capacidad de exposición de red**. Un programa comprometido en un cliente autorizado puede aprovechar la misma capacidad que una aplicación legítima.

Preferir deshabilitado donde no exista una necesidad operativa concreta y justificada.

Cuando sea necesario, aplicar «Default Deny» y permitir solo equipos IPv4 y rangos de puertos estrictamente definidos.

Ubicar los dispositivos que requieren port mapping en una VLAN o interfaz dedicada cuando sea viable.

No confiar en la ACL IPv4 para proteger peticiones IPv6: diseñar reglas IPv6 separadas.

Comprobar las asignaciones periódicamente y correlacionarlas con el inventario y los registros.

Evitar asignaciones universales a equipos de trabajo, cámaras, NAS o servidores sin una revisión formal.

80.10. IPv6: interpretación particular y limitaciones

La implementación documentada admite IPv6, pero no todos los clientes lo utilizan. En IPv6, la conectividad no se debe explicar como una traducción NAT IPv4 tradicional: puede implicar apertura de permisos de paso para direcciones globales. Netgate advierte que los clientes IPv6 suelen comunicarse desde direcciones link-local hacia destinos multicast; por ello, las reglas predeterminadas no garantizan el paso del tráfico de control.

LIMITACIÓN DOCUMENTADA Las entradas ACL descritas para el servicio solo controlan clientes IPv4. En IPv6 debe revisarse por separado el filtrado y la exposición real. No extrapolar el comportamiento de una tabla IPv4 a todo el direccionamiento IPv6.

80.11. WAN privada, doble NAT y CGNAT

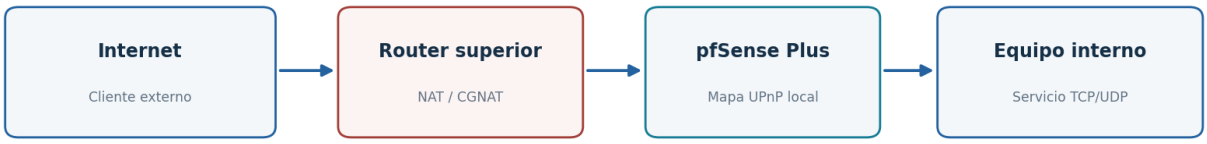


Figura 80.3. Un mapeo local no abre automáticamente el equipo anterior en una cadena de NAT.

Si pfSense recibe una WAN privada, el puerto externo que anuncia miniupnpd puede no corresponder a una dirección pública accesible. Cuando existe un router superior que efectúa NAT, este también debe entregar el tráfico hacia pfSense para completar el camino. En un CGNAT del proveedor sin redirección aguas arriba controlable, habilitar el servicio no crea por arte de magia un puerto público accesible.

Las opciones **STUN** y **Override WAN Address** documentadas por Netgate pueden servir en diseños específicos con NAT 1:1 sin filtrado y reenvío correctamente construido. STUN prueba condiciones de alcance y puede impedir mapeos si detecta que la recepción entrante no llega al firewall. Nunca sustituye una prueba completa de extremo a extremo.

80.12. Particularidades de Multi-WAN y gateways

La documentación de Netgate define una sola **External Interface**, asociada a la WAN con gateway predeterminado. Por ello, no es correcto asumir que un mapeo se traslada automáticamente a otra WAN cuando cambia la ruta de salida. Tras un failover, revisar la WAN activa, la dirección pública utilizada, la consistencia de NAT y la accesibilidad desde una red externa. No habilitar automáticamente UPnP para todas las WAN ni utilizar reglas amplias como solución provisional.

80.13. Status → Services: comprobar el daemon

1. Abrir Status → Services e identificar el servicio UPnP IGD & PCP / miniupnpd cuando esté registrado.

2. Comprobar su estado y correlacionarlo con la habilitación de Services → UPnP IGD & PCP.
3. No interpretar un proceso «Running» como prueba de que existan mapeos válidos ni accesibles.
4. Antes de reiniciar o detener, documentar las asignaciones activas y el impacto en las aplicaciones.
5. Realizar de nuevo las pruebas de registro de mapeos y conectividad externa tras la intervención.

OPERACIÓN CON IMPACTO Reiniciar o detener el daemon puede retirar o alterar asignaciones activas y dejar aplicaciones sin puertos entrantes hasta su renovación. En producción, cualquier cambio debe contar con ventana y plan de reversión.

80.14. System Logs: dónde buscar errores útiles

El subsistema **Routing** del registro **Status → System Logs → System** incorpora mensajes de **miniupnpd**. Netgate documenta errores de inicio, pruebas STUN, fallos al añadir reglas —por ejemplo, «Failed to add»— y otros eventos relacionados con la conectividad WAN. Por otro lado, cuando se habilita **Firewall Logs** en el servicio, las conexiones que coincidan con reglas dinámicas registrables pueden observarse en **Status → System Logs → Firewall**.

Síntoma observado	Lugar de comprobación	Lectura inicial
No aparecen asignaciones	Status / Services / Routing	Servicio, protocolos, peticiones y ACL.
«Failed to add»	System Logs → Routing	Dirección WAN, STUN, NAT superior y autorizaciones.
Cliente recibe error o timeout	Firewall Logs / Packet Capture	Puertos de control y llegada de solicitud.
Asignación creada, servicio inaccesible	Firewall / NAT / captura externa	Tráfico externo, ruta de retorno y servicio de destino.
Asignación desaparece	Estado y registros del cliente	Caducidad, renovación o reinicio del servicio.

80.15. Firewall: reglas dinámicas y visibilidad

Las reglas generadas por UPnP IGD & PCP existen fuera de las reglas definidas manualmente y no se editan con el mismo flujo que un port forward estático. La opción de colas ALTQ se define desde el servicio cuando procede. La presencia de una regla dinámica no implica que todos los paquetes estén registrados: el ajuste **Firewall Logs** debe activarse si se requiere trazabilidad de conexiones coincidentes, teniendo en cuenta el volumen de eventos y la política de retención.

80.16. Comprobación guiada de un puerto publicado

1. Identificar la aplicación y el puerto requerido; registrar aprobación, dispositivo responsable y alcance.
2. Confirmar en el panel Status que la regla activa corresponde a la interfaz, IP interna, puertos y protocolo esperados.
3. Verificar la dirección WAN publicable y si existe doble NAT, filtrado de ISP o CGNAT.
4. Comprobar que el servicio de destino escucha en el puerto interno y que el firewall del sistema operativo permite conexiones.
5. Desde un cliente externo autorizado, probar el protocolo y puerto real; no confiar en un test ejecutado desde la propia LAN.
6. Correlacionar el intento con Logs de firewall y Routing, así como con captura de paquetes donde corresponda.
7. Retirar la necesidad temporal y verificar que el mapeo desaparece o se revoca mediante el flujo permitido por el cliente.

80.17. Captura de paquetes y pruebas sin modificar la configuración

La captura selectiva permite determinar si se reciben solicitudes de control y paquetes del servicio publicado. Para una prueba puntual puede utilizarse **Diagnostics → Packet Capture**, seleccionando la interfaz correcta y filtros limitados. Si se emplea consola, estos comandos tienen finalidad de observación y requieren permisos administrativos:

Objetivo	Ejemplo de observación (no ejecuta cambios)
Ver peticiones de control en LAN	tcpdump -ni <interfaz_interna> "udp port 1900 or udp port 5351"
Ver conexión exterior de prueba	tcpdump -ni <interfaz_wan> "tcp port 53020"
Inspeccionar redirecciones NAT en pf	pfctl -sn (filtrar después la salida por el puerto de prueba)
Consultar reglas PF aplicadas	pfctl -sr (lectura de reglas; no modifica el firewall)

PRIVACIDAD Las capturas de paquetes, incluso las limitadas por puerto, pueden contener direcciones, nombres de servicios y metadatos sensibles. Guardar evidencias solo en repositorios autorizados y anonimizar antes de publicar ejemplos.

80.18. Diagnóstico progresivo: sin cambios prematuros

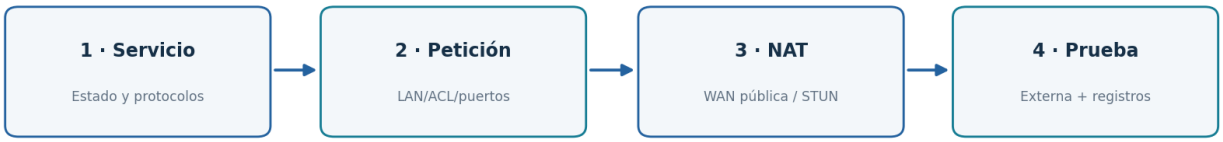


Figura 80.4. Secuencia de diagnóstico de menor a mayor alcance operativo.

Cuando la prueba externa no funciona, conservar el orden de comprobación. **Primero** verificar si la petición se recibió; **después**, si fue autorizada y produjo un mapeo; **por último**, si el camino de ida y vuelta permite alcanzar la aplicación. Alterar indiscriminadamente firewall, NAT y gateways a la vez dificulta identificar la causa y aumenta el riesgo de abrir servicios de forma innecesaria.

80.19. Matriz de incidencias y medidas de corrección

Problema	Causas probables	Acción segura inicial
Servicio disabled	Deshabilitación intencional / sin necesidad operativa.	Confirmar requisitos antes de habilitarlo.
Daemon activo, lista vacía	No hay clientes solicitando mapeos; ACL o puertos bloqueados.	Generar petición controlada y revisar Routing.
Cliente no descubre IGD	SSDP UDP/1900 bloqueado o interfaz equivocada.	Captura local y verificación de reglas LAN.
PCP no responde	UDP/5351 bloqueado o protocolo no habilitado.	Comprobar servicio, ACL y red interna.
WAN con IP privada	Doble NAT, CGNAT o STUN no compatible.	Comprobar redirección superior y dirección pública.
Asignación visible, sin conexión	Servicio no escucha, retorno mal encaminado o NAT superior.	Probar desde fuera y capturar ambos lados.
Puerto abierto hacia un equipo no esperado	Cliente con autorización excesiva, endpoint comprometido.	Identificar dispositivo, aislar según procedimiento y cerrar exposición.
Mapping tras cambio de WAN falla	IP exterior distinta y rutas o NAT inconsistentes.	Revisar WAN predeterminada y reconstruir prueba controlada.

80.20. Procedimiento 1 — Verificar servicio inactivo sin habilitarlo

1. Confirmar el mensaje «Service is currently disabled» en Status.
2. Verificar la política prevista en Services → UPnP IGD & PCP sin cambiarla.
3. Revisar por separado si hay NAT manual o servicios expuestos autorizados.

4. Documentar el estado como «deshabilitado por configuración», no como «incidente», salvo contradicción con el diseño esperado.

80.21. Procedimiento 2 — Activación controlada en laboratorio

1. Definir un único segmento de prueba y un dispositivo autorizado que necesite un mapeo temporal.
2. Seleccionar una sola External Interface que satisfaga los requisitos de Netgate y una Internal Interface de laboratorio.
3. Habilitar únicamente el protocolo necesario; activar Default Deny y una ACL IPv4 restrictiva, si procede.
4. Guardar, comprobar estado de miniupnpd y obtener un mapeo mediante la aplicación aprobada.
5. Validar la fila de Status y probar acceso desde red externa controlada.
6. Al finalizar, retirar la autorización o deshabilitar el servicio y comprobar la desaparición del mapeo.

80.22. Procedimiento 3 — Auditoría de exposición dinámica

1. Definir ventana y responsable de la revisión, con mínimo privilegio.
2. Inventariar Ext Interface, Ext Port, Int IP, Int Port, Protocol y Description.
3. Correlacionar cada destino con su activo autorizado y el propietario de la aplicación.
4. Revisar cualquier regla con Source IP = any o puertos sensibles, y validar su justificación.
5. Comprobar el ajuste Default Deny, las ACL IPv4 y las reglas IPv6 independientes.
6. Registrar diferencias y ejecutar correcciones aprobadas; documentar resultado de prueba desde exterior.

80.23. Procedimiento 4 — Doble NAT o fallo STUN

1. Confirmar si la WAN de pfSense tiene una dirección global enrutable o una dirección privada.
2. Identificar si existe un dispositivo anterior con NAT 1:1 y reenvío controlado, o CGNAT no administrable.
3. Comprobar en Routing si el daemon ha rechazado el mapeo o STUN informa fallo en recepción de tráfico.
4. Si existe infraestructura superior administrable, verificar por separado el trayecto externo hasta pfSense.
5. No utilizar Override WAN Address para disfrazar una falta real de conectividad entrante.
6. Repetir la prueba externa y registrar resultados antes de aprobar el cambio.

80.24. Escenarios empresariales de referencia

Escenario	Enfoque recomendado
Red corporativa con estaciones y servidores	Mantener deshabilitado salvo necesidad documentada; priorizar NAT estático y reglas auditables.
VLAN dedicada a laboratorio o pruebas audiovisuales	Permitir clientes concretos y puertos delimitados; mantener supervisión y pruebas periódicas.
Red Wi-Fi invitados	No habilitar automáticamente: equipos no confiables podrían publicar servicios por petición.
Sede con WAN principal y enlace alternativo	Evaluar si el mapeo depende de la WAN predeterminada; validar después de conmutación.
Cortafuegos tras router 4G / CGNAT	Comprobar el alcance externo real; considerar arquitectura VPN inversa cuando no se controlan puertos públicos.

80.25. Hoja de comprobación para cambios en producción

Control	Evidencia mínima
Necesidad y aprobación	Servicio, dispositivo, puerto, tiempo de uso y responsable autorizados.
Mínimo privilegio	ACL por equipo / rango y segmentación de red; IPv6 evaluado por separado.

Control	Evidencia mínima
WAN y NAT superior	Dirección accesible desde Internet y ruta completa verificada.
Visibilidad	Capturas anonimizadas del estado y entradas de logs pertinentes.
Prueba externa	Resultado reproducible con fecha, protocolo, origen de prueba y destino.
Reversión	Procedimiento probado para retirar el permiso sin afectar a servicios ajenos.

80.26. Riesgos, rendimiento y registro de evidencias

Los mapeos automatizados pueden mejorar la interoperabilidad de aplicaciones, pero también crear superficies de exposición difíciles de auditar. En redes empresariales debe evitarse que un cliente sin controles anuncie servicios a toda Internet. Si se activan logs de conexión, medir volumen, retención y espacio disponible. La supervisión de este panel es una instantánea operativa: para trazabilidad longitudinal integrar registros y procesos de auditoría autorizados.

Cuando la política de seguridad exija reglas inmutables, cambio documentado o listas de orígenes remotos controladas, la publicación manual es generalmente más administrable que permitir mapeos automáticos extensivos.

80.27. Glosario técnico

Término	Definición resumida
UPnP IGD	Protocolo de control de gateway para descubrimiento y redirecciones.
PCP	Port Control Protocol; solicita control de mapeos en dispositivos de red.
NAT-PMP	Antecesor de PCP, utilizado para solicitar mapeos NAT.
SSDP	Protocolo de descubrimiento en red local usado por UPnP.
miniupnpd	Daemon responsable de los servicios de mapeo UPnP IGD y PCP/NAT-PMP.
STUN	Mecanismo para averiguar información pública y características de NAT.
CGNAT	Traducción de direcciones compartida en infraestructura del proveedor.
ACL	Lista de control de accesos; aquí delimita solicitudes IPv4 autorizadas.
Lease / lifetime	Periodo de vigencia de una asignación sujeto a renovación/caducidad.

80.28. Referencias técnicas verificables

01 Netgate — UPnP IGD & PCP: servicio, puertos, ACL y estado

02 Netgate — Guía del menú Status

03 Netgate — Diagnóstico de NAT Port Forwards

04 Netgate — Routing Logs y miniupnpd

05 Netgate — Troubleshooting Firewall Rules

06 Netgate — UPnP IGD & PCP y Traffic Shaping

07 Netgate — Port Forwarding y control automático

08 Netgate — Notas de versión pfSense Plus 25.07 (aviso disabled)

09 IETF — RFC 6886 (NAT-PMP), referencia normativa

NOTA SOBRE VERSIONES Los nombres y controles pueden cambiar con las revisiones de pfSense Plus. Contrastar las diferencias con las notas de versión y la ayuda del formulario instalado antes de aplicar un procedimiento.

Parte VII Diagnostics

81 Diagnostics → Introducción general

Herramientas de diagnóstico · redes y firewall · seguridad · evidencias · recuperación operativa

Diagnostics reúne herramientas para comprobar la conectividad, investigar reglas y estados, inspeccionar procesos y preparar acciones de recuperación sobre pfSense Plus. Su utilidad depende de seleccionar la herramienta correcta y de interpretar qué datos observa cada una, evitando cambios prematuros en sistemas de producción.

CRITERIO TÉCNICO Un resultado positivo de Ping no demuestra que una aplicación funcione; un puerto TCP accesible no demuestra que la autenticación sea válida; una sesión de estado no prueba que la respuesta regrese. Cada herramienta verifica una parte distinta del camino.

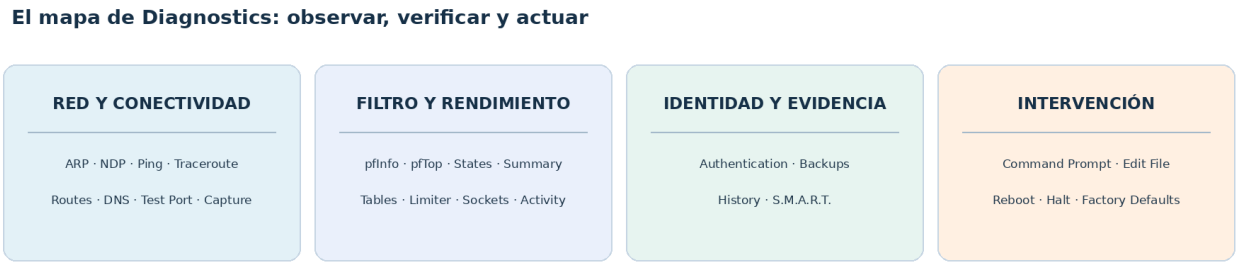


Figura 81.1. Las 25 entradas del menú agrupadas por finalidad operacional.

81.1. Alcance y ruta de acceso

Ruta exacta: Diagnostics. El menú proporciona accesos directos a páginas de prueba, inspección, gestión de configuración y operaciones sobre el propio firewall. La disponibilidad de determinadas opciones depende del hardware, de la instalación y de la versión de pfSense Plus.

El menú reúne 25 herramientas. Debe distinguirse entre las funciones de lectura —que habitualmente no alteran la configuración—, las que modifican tablas o estados dinámicos y las que pueden reiniciar, apagar o restablecer el firewall.

81.2. Inventario completo del menú Diagnostics

La tabla conserva el orden del menú. Cada descripción aclara su finalidad y su principal criterio de interpretación, sin atribuir opciones a formularios cuya presentación depende de la versión.

N.º	Herramienta	Finalidad concreta	Impacto
01	ARP Table	Vecinos IPv4 y correspondencia IP–MAC en enlaces locales.	Lectura / borrado ARP
02	Authentication	Prueba de autenticación contra servidores externos definidos (LDAP/RADIUS).	Prueba controlada
03	Backup & Restore	Exportación y restauración de la configuración.	Cambio crítico
04	Command Prompt	Ejecución de órdenes shell/PHP y operaciones de ficheros.	Privilegiado
05	Configuration History	Consulta de revisiones y recuperación de configuraciones anteriores.	Reversión crítica
06	DNS Lookup	Resolución de nombres desde el propio firewall.	Lectura
07	Edit File	Edición directa de archivos del sistema.	Cambio crítico
08	Factory Defaults	Restablecimiento de la configuración predeterminada.	Destructivo
09	Halt System	Apagado ordenado del equipo.	Interrupción
10	Limiter Info	Inspección del funcionamiento de limitadores dummynet.	Lectura

N.º	Herramienta	Finalidad concreta	Impacto
11	NDP Table	Vecinos IPv6 vistos localmente y sus direcciones de enlace.	Lectura / borrado NDP
12	Packet Capture	Captura de paquetes en interfaces elegidas.	Lectura sensible
13	pfInfo	Contadores del filtro PF y de sus tablas.	Lectura
14	pfTop	Vista dinámica de estados y tráfico de conexiones.	Lectura
15	Ping	Pruebas de alcance ICMP desde el firewall.	Prueba activa
16	Reboot	Reinicio del equipo y de los servicios dependientes.	Interrupción
17	Routes	Inspección de tablas de encaminamiento.	Lectura
18	S.M.A.R.T. Status	Salud y autodiagnóstico de discos compatibles.	Condicional
19	Sockets	Puertos/procesos y conexiones de red originadas o atendidas por el equipo.	Lectura
20	States	Inspección y eliminación selectiva de estados de conexiones PF.	Lectura / cambio
21	States Summary	Agregados de estados por origen, destino y pares de IP.	Lectura intensiva
22	System Activity	Consumo de CPU, memoria, procesos e hilos.	Lectura
23	Tables	Inspección y edición de tablas PF / alias activos.	Lectura / cambio
24	Test Port	Prueba de conexión TCP desde el firewall a un destino.	Prueba activa
25	Traceroute	Exploración de saltos hacia un destino.	Prueba activa

81.3. El método profesional: de la evidencia a la intervención



Figura 81.2. Secuencia que reduce el riesgo operativo y favorece un diagnóstico reproducible.

El objetivo no es ejecutar todas las herramientas, sino construir una hipótesis verificable. Antes de iniciar: identificar el servicio afectado, la dirección del tráfico, el momento del fallo, el origen de la prueba y el último cambio conocido.

Definir el síntoma: una estación sin acceso web no equivale a un firewall sin Internet; delimitar equipos, protocolos y sedes afectadas.

Recoger indicios de menor impacto: estados, rutas, mensajes de System Logs y estadísticas antes de borrar sesiones, modificar reglas o reiniciar.

Reproducir con precisión: indicar origen, interfaz, nombre o IP del destino, puerto, familia IPv4/IPv6 y hora de prueba.

Aplicar un único cambio reversible, autorizado y documentado cuando la evidencia señale una causa concreta.

Validar conectividad, experiencia del usuario, registros y retorno al estado esperado; conservar evidencias y registrar el cierre.

81.4. Herramientas de red y conectividad

81.4.1. ARP Table y NDP Table

ARP relaciona direcciones IPv4 y MAC en el segmento local. NDP cumple funciones equivalentes de descubrimiento de vecinos IPv6 mediante ICMPv6. Sus tablas son cachés temporales, no inventarios exhaustivos; un cliente que no ha intercambiado tráfico recientemente puede no figurar. Una entrada incompleta de ARP indica que se emitió una búsqueda sin recibir respuesta válida.

Usos: detectar conflictos de direccionamiento, movimientos de equipos, problemas L2, fallos de VLAN y direcciones de vecino caducadas. Borrar una entrada obliga al firewall a reaprender la información y puede provocar una interrupción breve, por lo que debe realizarse de manera selectiva.

81.4.2. DNS Lookup, Ping, Traceroute y Test Port

Herramienta	Qué confirma	Qué NO confirma
DNS Lookup	El firewall puede consultar un nombre con un resolutor concreto.	Que el cliente use el mismo DNS o que el servicio responda.
Ping	Existe respuesta ICMP desde el origen/ interfaz utilizados.	Que el puerto de la aplicación esté abierto.
Traceroute	Saltos que responden a una técnica de trazado.	Todos los saltos reales; puede haber filtrado o asimetría.
Test Port	Se establece o rechaza una conexión TCP a un puerto.	Servicios UDP ni el éxito de la autenticación de aplicación.

En túneles, Multi-WAN y policy routing es determinante el origen: un Ping enviado desde la propia WAN puede seguir una ruta distinta a la de un cliente LAN. La prueba debe documentarse con interfaz, dirección fuente y destino exactos. Un traceroute incompleto no demuestra una interrupción en el último salto mostrado.

81.4.3. Routes y Packet Capture

Routes muestra la tabla de rutas que utiliza el sistema y permite reconocer redes directamente conectadas, rutas estáticas y vías por defecto. Debe contrastarse con las reglas de policy routing y gateways, porque el tráfico reenviado con una política específica puede no seguir el gateway predeterminado observado en la tabla general.

Packet Capture recoge paquetes reales en un punto de observación. Una captura WAN puede mostrar un paquete entrante antes de que PF lo permita, mientras que la captura de salida observa el tráfico tras las transformaciones aplicadas en ese extremo. Comparar entrada y salida, junto con States y reglas, ayuda a ubicar dónde deja de circular un flujo.



Figura 81.3. Correlación de puntos de captura, filtrado, NAT y respuesta del destino.

ADVERTENCIA Los archivos PCAP pueden contener direcciones, nombres, tokens, credenciales e incluso datos de aplicaciones sin cifrar. Limitar el filtro y duración, custodiar el archivo y anonimizarlo antes de compartirlo.

81.5. Diagnóstico del cortafuegos, estados y rendimiento

81.5.1. pfInfo y pfTop

pfInfo expone estadísticas internas del filtro PF: contadores de paquetes, búsquedas e inserciones de estados, límites y anomalías. pfTop permite observar conexiones vivas y ordenarlas para localizar consumo, antigüedad o ritmo de actividad. Un aumento de inserciones no demuestra por sí solo un ataque: debe cotejarse con aplicaciones y registros.

81.5.2. States y States Summary

States contiene conexiones reconocidas por PF, sus extremos y traducciones NAT. El resumen agrega actividad por IP origen, destino o par, útil para detectar concentraciones de sesiones. Una entrada establecida puede mantenerse después de modificar una regla, por lo que conviene distinguir la política vigente del estado que se creó anteriormente.

ADVERTENCIA Eliminar un estado concreto puede facilitar una nueva negociación de ruta o NAT, pero también corta esa sesión. Vaciar todos los estados afecta a múltiples aplicaciones y VPN: reservarlo para intervención autorizada. Las consultas globales de States Summary pueden consumir recursos en firewalls con tablas grandes.

81.5.3. Tables, Limiter Info, Sockets y System Activity

Entrada	Lectura técnica	Aplicación
Tables	Entradas efectivas de alias/tablas PF, incluidas listas dinámicas y FQDN resueltos.	Confirmar si el objeto que evalúa el firewall contiene la IP esperada.
Limiter Info	Estado y tráfico de limitadores dummynet.	Distinguir política de ancho de banda de congestión del enlace.
Sockets	Sockets de procesos locales: escucha y conexiones del propio firewall.	Detectar si DNS, SSH u otro servicio escucha en el puerto previsto.
System Activity	Procesos, hilos, CPU y consumo de memoria.	Relacionar lentitud de GUI o VPN con carga sostenida.

Editar una tabla de PF puede producir un cambio operativo inmediato; conviene revisar primero el origen del alias y su posterior regeneración. Por el contrario, Limiter Info es una vista de control de limitadores y no sustituye Status → Queues, dedicado a colas ALTQ.

81.6. Identidad, backups y diagnóstico de hardware

81.6.1. Authentication

Permite comprobar credenciales en un servidor de autenticación configurado, con especial interés en LDAP y RADIUS. Un resultado correcto demuestra una autenticación básica; no valida necesariamente protocolos avanzados como EAP, asignación de privilegios finales ni el funcionamiento completo de una VPN.

81.6.2. Backup & Restore y Configuration History

Backup & Restore descarga y restaura configuraciones. Configuration History permite comparar revisiones y recuperar una configuración anterior. En el menú de esta versión figura como entrada independiente; la documentación de Netgate también la sitúa bajo Diagnostics → Backup & Restore → Config History. La ubicación concreta puede variar según la compilación.

Antes de una restauración debe comprobarse compatibilidad de versión y paquetes, conservar un respaldo actual y disponer de consola fuera de banda. Restaurar cambia parámetros de red, reglas, autenticación o VPN y puede desconectar la GUI. Una restauración desde el historial no implica que todas las modificaciones se apliquen automáticamente sin recargar servicios o reiniciar cuando sea necesario.

81.6.3. S.M.A.R.T. Status

La herramienta presenta información de autodiagnóstico y, en hardware compatible, pruebas de discos. La disponibilidad no es universal: depende del controlador, interfaz de almacenamiento, unidad física y soporte del firmware. Una prueba S.M.A.R.T. correcta no sustituye copias de seguridad ni valida por completo un sistema de archivos.

81.7. Acciones con impacto elevado y herramientas de administración

Entrada	Potencia	Riesgo principal y salvaguarda
Command Prompt	Órdenes shell/PHP y transferencia de ficheros.	Puede modificar el sistema y ejecutar tareas sin retorno. Usar solo órdenes acotadas y comprender su efecto.
Edit File	Acceso directo a ficheros del firewall.	Una edición sintáctica o en el lugar incorrecto puede inutilizar servicios; conservar original y validar.
Reboot	Reinicio ordenado del equipo.	Se interrumpen servicios y sesiones; ventana de mantenimiento, HA y acceso alternativo.
Halt System	Apagado ordenado.	Pérdida de conectividad hasta encendido físico/remoto seguro.
Factory Defaults	Retorno a configuración de fábrica.	Pérdida de ajustes operativos. Requiere plan de recuperación, copia y autorización.

La ejecución de comandos desde la GUI no es una consola interactiva. Netgate recomienda evitar procesos que no terminen y comandos de edición interactiva. Factory Defaults se centra en la configuración; no constituye por sí mismo un borrado seguro de datos de almacenamiento ni una desinstalación completa de todos los archivos de paquetes.

> **ADVERTENCIA** En un firewall remoto y sin vía de consola, Factory Defaults, Halt System, ciertos cambios de Edit File y algunas acciones de Reboot pueden dejar el equipo inaccesible. Antes de actuar: backup, ventana, plan de reversión, autorización y confirmación de acceso alternativo.

81.8. Procedimientos prácticos de diagnóstico

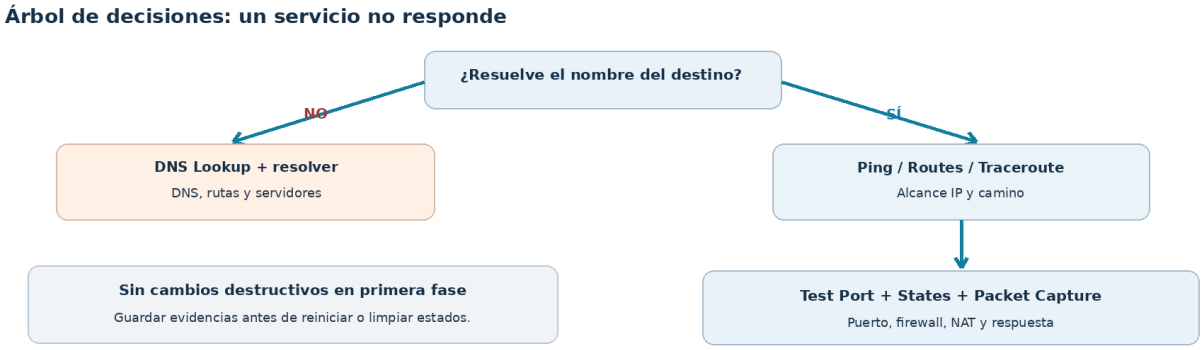


Figura 81.4. Selección progresiva de pruebas según el síntoma observable.

81.8.1. No hay navegación desde una red interna

Registrar hora, usuario/segmento y si el fallo afecta a un único dispositivo o a todos.

Comprobar Interfaces y Gateways; consultar Routes y la salida WAN esperada.

Ejecutar DNS Lookup y una prueba Ping con origen apropiado; diferenciar DNS de conectividad IP.

Buscar en States el flujo y revisar reglas/registro de firewall; capturar paquetes en LAN y WAN si persiste.

Corregir solo la causa verificada y validar navegador y aplicación, no únicamente el ping.

81.8.2. Una conexión TCP publicada no responde

Identificar origen externo, destino público y puerto documentado.

Consultar NAT y regla asociada, luego States; evitar pruebas desde dentro que dependan de reflexión NAT.

Realizar Packet Capture en WAN y después en la interfaz interna para seguir el SYN y el retorno.

Comprobar servicio final, gateway del host y firewall del sistema operativo; registrar conclusión con evidencias.

81.8.3. VPN conectada pero aplicación inaccesible

Confirmar sesión VPN y dirección virtual asignada.

Revisar rutas y tablas de estado del tráfico interno; contrastar redes superpuestas.

Capturar en interfaz virtual y destino cuando sea posible; comprobar firewall, NAT y DNS interno.

Validar respuesta del host y permisos de aplicación; no reiniciar la VPN por una respuesta ICMP fallida aislada.

81.8.4. Lentitud o alto número de sesiones

Revisar System Activity y pfInfo; documentar CPU, memoria y contadores de estados.

Abrir pfTop y States Summary para identificar dirección IP, puerto o servicio con mayor carga.

Consultar Limiter Info si hay políticas dummynet y compararlo con Monitoring.

Correlacionar eventos con horarios, cambios recientes y carga real antes de modificar límites.

81.9. Tabla de decisión: síntoma, herramienta y siguiente prueba

Síntoma observado	Primer instrumento	Segunda comprobación
Nombre no resuelve	DNS Lookup	Estado de Unbound, servidores y ruta DNS.
IPv4 local no llega	ARP Table	VLAN, enlace, Ping y captura de ARP.
IPv6 local no llega	NDP Table	RA/DHCPv6 y captura ICMPv6.
Servicio TCP inalcanzable	Test Port	Packet Capture / States / proceso destino.
Desvío de tráfico	Routes	Policy routing, firewall y traceroute.
Bloqueos inesperados	States y Tables	Reglas PF, alias y logs.
CPU elevada	System Activity	pfInfo, pfTop y procesos específicos.
Después de un cambio	Configuration History	Comparar configuración y rollback planificado.
Posible fallo de disco	S.M.A.R.T. Status	Logs, backups y pruebas de disco apropiadas.

81.10. Evidencias, privacidad y reproducibilidad

Un informe de diagnóstico útil identifica: fecha/hora y zona horaria, síntoma, alcance, origen y destino de la prueba, interfaz, protocolo/puerto, herramienta aplicada, resultado antes/después y decisión. Es importante diferenciar un hecho observado de una hipótesis: «no llega SYN a WAN» es evidencia; «lo bloquea el operador» es una posible causa pendiente de contraste.

Los resultados de diagnóstico pueden revelar topología, direcciones, MAC, claves, identificadores de usuario, sesiones y contenidos. Antes de compartir registros, backups, capturas o archivos generados por utilidades de soporte, inspeccionar y anonimizar cada elemento. Una máscara de pantalla no protege un archivo PCAP o XML adjunto: los datos subyacentes deben sanitizarse.

> **CRITERIO TÉCNICO** No publicar configuraciones, capturas ni archivos de soporte sin revisión específica. Netgate advierte que incluso los paquetes de diagnóstico que intentan ocultar secretos pueden conservar información sensible.

81.11. Buenas prácticas operativas y glosario

El orden recomendado es observación → prueba acotada → correlación → cambio reversible → validación. Siempre que sea posible, probar desde el origen real del problema, registrar resultados negativos y limitar capturas de paquetes por interfaz, filtro, tamaño y tiempo.

Término	Significado
ARP / NDP	Resolución de vecinos a nivel de enlace en IPv4 / IPv6.
PF	Motor de filtrado de paquetes y seguimiento de conexiones del cortafuegos.
State	Entrada dinámica que identifica y procesa una conexión reconocida.
NAT	Traducción de direcciones/puertos aplicada al flujo.
PCAP	Formato de archivo de captura de paquetes.
dummynet	Subsistema usado por limitadores de tráfico en pfSense.

Término	Significado
Policy routing	Selección de un gateway por una regla específica, no solo por la ruta por defecto.
Rollback	Reversión controlada a una configuración previa conocida.

81.12. Lista operativa antes de actuar en producción

El diagnóstico no finaliza cuando desaparece el error visual. Debe existir una comprobación funcional de extremo a extremo y un registro de cómo se ha recuperado el servicio. Este control resulta especialmente relevante en equipos que concentran DNS, DHCP, VPN y varias salidas WAN.

Control	Comprobación imprescindible
Alcance	¿Se conoce qué usuarios, aplicaciones e interfaces están afectados?
Evidencia previa	¿Se han recogido estados, rutas, logs y hora exacta antes del cambio?
Riesgo	¿La acción puede borrar estados, alterar rutas, apagar el equipo o cambiar reglas?
Recuperación	¿Existe copia válida de configuración y acceso de consola alternativo?
Validación	¿Se comprobaron los servicios reales, el retorno del tráfico y los logs posteriores?
Cierre	¿Se documentó la causa, el cambio aplicado y la reversión si procede?

81.13. Documentación oficial y referencias

[01] Menú Diagnostics: catálogo general

[02] ARP Table: funcionamiento y límites

[03] Troubleshooting Authentication

[04] Command Prompt: funciones y advertencias

[05] Packet Capture GUI: filtros y controles

[06] Packet Capturing: orden de observación

[07] pfInfo: contadores de PF

[08] pfTop: estados y rendimiento

[09] States Summary: agregados y limitaciones

[10] Tables: contenido de las tablas PF

[11] Configuration History: restauración

[12] Diagnóstico de NAT y redirecciones

[13] Diagnostic Data: protección de evidencias

82 Diagnostics → ARP Table

Resolución de vecinos IPv4 · caché IP–MAC · búsqueda · Wake-on-LAN · diagnóstico de capa 2

La tabla ARP muestra las asociaciones IPv4↔MAC que conoce el firewall en segmentos alcanzables directamente. Su lectura facilita investigar fallos de conectividad, conflictos de direcciones y cambios de dispositivo sin confundir una caché temporal con un inventario completo de la red.

CRITERIO TÉCNICO ARP es una evidencia de vecindad IPv4, no una prueba de que un equipo esté encendido, accesible por ICMP o con sus aplicaciones operativas.

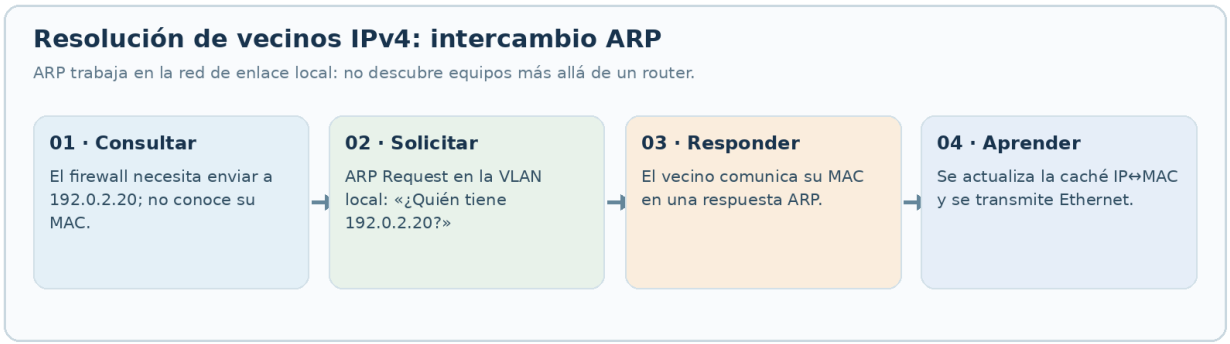


Figura 82.1. Secuencia conceptual de petición, respuesta y aprendizaje ARP en el dominio de broadcast.

82.1. Finalidad, alcance y ubicación

Ruta exacta: Diagnostics → ARP Table. La función consulta la tabla de vecinos IPv4 del sistema y permite buscar entradas, abrir destinos Wake-on-LAN y eliminar asociaciones de la caché. No configura el servidor DHCP, no crea reglas NAT y no sustituye una auditoría de inventario.

Una entrada suele aparecer cuando el firewall necesita resolver la MAC de un vecino en un enlace local. Un equipo activo que no haya comunicado con el firewall recientemente puede faltar de la lista; los dispositivos alcanzables a través de un router remoto aparecen asociados al siguiente salto local, no individualmente.

82.2. Fundamentos: qué ocurre cuando pfSense envía un paquete

82.2.1. ARP Request, ARP Reply y trama Ethernet

Para enviar un paquete IPv4 a un destino de su mismo segmento, el firewall selecciona primero la interfaz de salida mediante su tabla de rutas. Si desconoce la dirección MAC correspondiente a la IP del siguiente salto, transmite una solicitud ARP de difusión dentro de esa red de capa 2. El equipo propietario de la dirección responde con su MAC y el firewall puede encapsular el paquete IPv4 en una trama Ethernet unicast.

82.2.2. Lo que ARP no hace

ARP no utiliza el servicio DNS ni proporciona cifrado o autenticación criptográfica. No atraviesa routers convencionales como una difusión ARP normal y no sirve para resolver direcciones IPv6: los vecinos IPv6 usan Neighbor Discovery Protocol (NDP), basado en ICMPv6. En presencia de Proxy ARP o direcciones virtuales pueden intervenir otros elementos, por lo que la MAC mostrada no siempre pertenece al host final.

82.3. Sección Search: cada campo y control

Control visible	Función y comportamiento
Search Term	Texto o patrón para filtrar filas de la tabla. La ayuda lo presenta como expresión regular tipo Unix; el código de la página usa expresiones regulares del navegador.
Selector All	Busca en todas las columnas textuales representadas.
Selector de campo	Opciones verificadas en el código: All, Interface, IP Address, MAC Address, Hostname, Status y Link Type.

Control visible	Función y comportamiento
Search	Aplica el filtro a las filas que el navegador ya muestra; no fuerza un nuevo descubrimiento ARP.
Clear	Restablece el cuadro de búsqueda, selecciona All y vuelve a mostrar las filas ocultas; no borra la caché del sistema.
Icono – en Search	Contrae o despliega el panel de búsqueda; es una preferencia de presentación.

Ejemplos ficticios: buscar `192\.0\.2\.` para identificar un prefijo concreto, `^Permanent$` en Status para localizar entradas permanentes o `^LAN$` en Interface para limitar la tabla a esa etiqueta. La sintaxis avanzada depende de las expresiones regulares admitidas por el navegador, y los patrones mal construidos pueden provocar errores de búsqueda.

82.4. Columnas de ARP Table

Columna	Interpretación operativa y precauciones
Interface	Interfaz lógica o física donde se encuentra el vecino. En enlaces VLAN la relación entre nombre asignado, VLAN y puerto físico debe comprobarse en Interfaces.
IP Address	Dirección IPv4 de la entrada. No debe suponerse que haya sido entregada por DHCP.
MAC Address	Dirección de enlace del vecino o la indicación (Incomplete). Puede incluir fabricante si se instaló Nmap y existe información OUI.
Hostname	Nombre recuperado por concesiones DHCP o resolución inversa DNS. Puede ser antiguo, incompleto o no existir.
Status	Permanent para entradas estáticas/locales; Expires in N seconds para dinámicas. (Incomplete) refleja ARP no resuelto.
Link Type	Tipo de enlace indicado por el sistema, por ejemplo vlan o ethernet; no identifica la velocidad ni calidad del enlace.
Actions	Añadir destino WOL (+), enviar Magic Packet (encendido) y eliminar entrada ARP (papelera).

82.5. Interpretación de estados y temporizadores



Figura 82.2. Tres clases de observación y sus limitaciones como indicador de disponibilidad.

82.5.1. Permanent

Describe una asociación estática o propia del firewall, como la IP de una interfaz y, según el tipo de configuración, determinadas IP virtuales. No implica que una máquina remota esté respondiendo; tampoco significa que el servidor DHCP posea una reserva. Si se intenta borrar una asociación local indispensable, el sistema puede impedirlo o volver a crearla.

82.5.2. Expires in N seconds

Indica el tiempo restante de una entrada dinámica. La documentación de Netgate menciona 1.200 segundos (20 minutos) como edad máxima predeterminada de referencia. El temporizador y el mecanismo de mantenimiento pueden variar con la versión del sistema; un contador cercano a cero no demuestra desconexión.

82.5.3. (Incomplete)

El firewall intentó obtener una MAC para una IP pero todavía no recibió una respuesta ARP válida. Puede indicar que el host está apagado, que hay un puerto o VLAN equivocado, que la IP no corresponde a ningún equipo del segmento, o una anomalía de capa 2. Es una pista, no un diagnóstico definitivo.

82.6. Acciones: iconos por fila y botón global

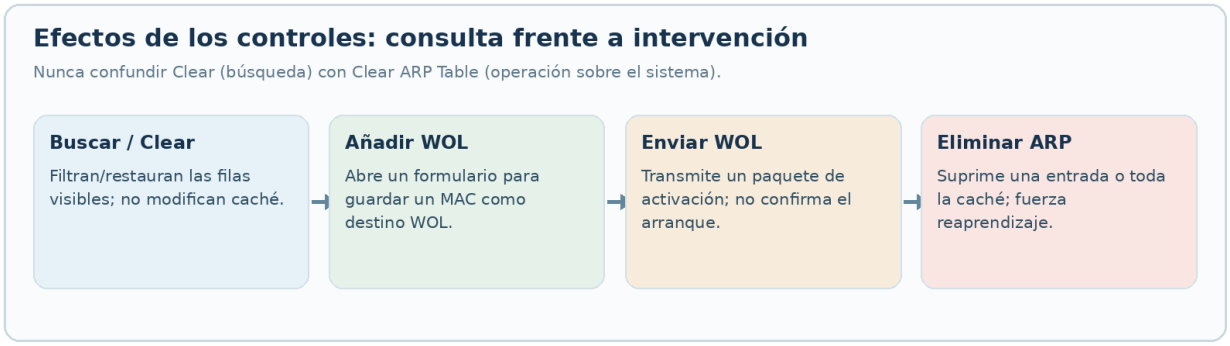


Figura 82.3. Comparación entre acciones de filtrado local, Wake-on-LAN y modificación de la caché.

Acción	Qué realiza	Riesgo/alcance
+ (Add WOL mapping)	Abre Services → Wake-on-LAN para crear una entrada con interfaz, MAC y descripción precargadas cuando se dispone de ellas.	No crea una reserva DHCP ni una entrada ARP estática.
Power (Send WOL packet)	Envía un Magic Packet por la interfaz de destino seleccionada.	No asegura que el equipo admita WOL ni que arranque.
Papelera por fila	Solicita eliminar una entrada IP→MAC de la caché; el siguiente tráfico puede originar una nueva consulta ARP.	Puede introducir latencia o pérdida temporal de paquetes hacia ese vecino.
Clear ARP Table	Solicita confirmación y purga las entradas de la caché mediante una operación global.	Mayor impacto; puede afectar temporalmente a múltiples conexiones.
Clear (Search)	Limpia el filtro de búsqueda de la página.	Sin modificación de ARP, DHCP o reglas.

ADVERTENCIA La papelera ARP no elimina un host de la red, no revoca una concesión DHCP y no bloquea tráfico. Si el origen sigue respondiendo, la asociación puede reaparecer inmediatamente.

82.7. Relaciones con otras pantallas de pfSense

Pantalla	Qué aporta al diagnóstico
Status → DHCP Leases	Muestra concesiones y asociaciones configuradas; la presencia de una MAC en ARP influye en cómo se representa la disponibilidad de ciertas concesiones.
Diagnostics → NDP Table	Equivalente funcional para vecinos IPv6, con semántica y estados propios de NDP.
Diagnostics → Ping	Provoca actividad dirigida y puede desencadenar una búsqueda ARP; un fallo ICMP no implica necesariamente un fallo de ARP.
Diagnostics → Packet Capture	Permite observar solicitudes y respuestas ARP en la interfaz correcta.
Status → System Logs	Permite investigar movimientos de IP entre MAC, cambios de enlace y eventos de red.
Services → Wake-on-LAN	Almacena equipos, emite Magic Packets y administra destinos de activación.
Interfaces / Switch / VLAN	Aporta la correspondencia entre subred, interfaz lógica, VLAN y puerto físico real.

82.8. Diagnóstico guiado: de ARP incompleto a la causa raíz

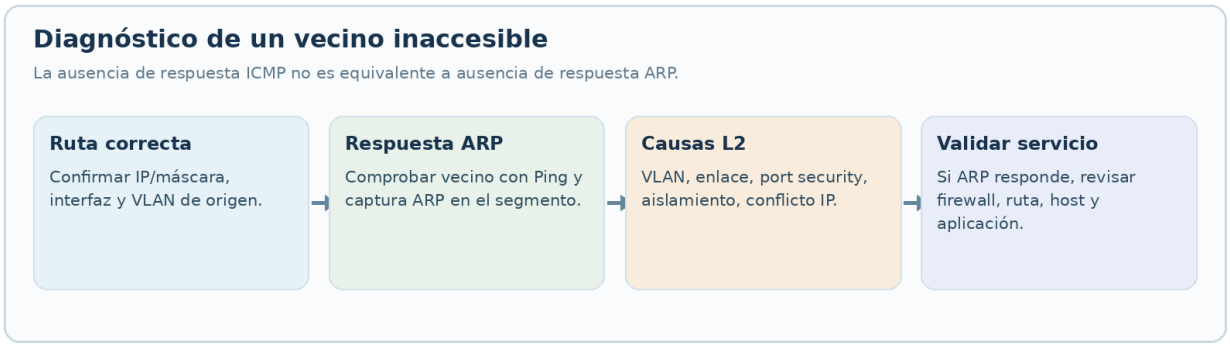


Figura 82.4. Secuencia de comprobación escalonada antes de borrar asociaciones o modificar VLAN.

Procedimiento de menor a mayor impacto:

Identificar el alcance: ¿un único host, una VLAN completa o varias sedes? Registrar la IP ficticia, la interfaz esperada y la hora.

Verificar máscara, ruta e interfaz de salida. ARP solo se utilizará hacia un vecino del enlace; para redes remotas se resuelve la MAC del gateway local.

Consultar la tabla ARP y anotar si la entrada falta, es dinámica, permanente o incompleta.

Enviar una prueba controlada con Diagnostics → Ping usando el origen correcto. Observar si se crea o modifica la entrada.

Capturar ARP en la interfaz adecuada: comprobar solicitudes, VLAN esperada, respuesta y dirección MAC de origen.

Revisar el switch, el etiquetado VLAN, estado físico, aislamiento L2, seguridad del puerto y configuración del equipo.

Solo con evidencia de asociación obsoleta, eliminar esa entrada ARP concreta; repetir las pruebas y registrar el resultado.

82.9. Comandos FreeBSD de inspección y validación

Comando de referencia	Finalidad y seguridad
arp -an	Lista asociaciones IPv4 de la caché sin ejecutar cambios.
arp -n 192.0.2.20	Consulta la asociación de una dirección de ejemplo; revisar sintaxis según versión.
tcpdump -eni <if> arp	Captura ARP con direcciones de enlace; sustituir <if> por la interfaz real desde la consola autorizada.
arp -d 192.0.2.20	Elimina una única entrada; acción con riesgo de pérdida transitoria de conectividad.
arp -d -a	Borra múltiples asociaciones; NO usar como prueba rutinaria ni desde sesión remota sin reversión.

Los comandos se proporcionan como referencia del entorno FreeBSD subyacente. Para un procedimiento auditado es preferible comenzar por las páginas GUI y Packet Capture; la sintaxis exacta y permisos se comprobarán en la versión instalada. No utilizar comodines ni copiar comandos de borrado sin revisar el objetivo.

82.10. Escenarios empresariales reproducibles

82.10.1. Nueva estación de trabajo sin acceso al gateway

Síntoma: el equipo 192.0.2.20/24 no se comunica con su firewall 192.0.2.1. Si aparece (Incomplete), verificar primero la VLAN del puerto, etiquetado y máscara. Capturar ARP en el firewall. Una respuesta correcta con MAC aprendida desplaza la investigación hacia reglas, host y capa superior.

82.10.2. Sustitución de un servidor con la misma IP

Al migrar un servidor a otra tarjeta de red puede cambiar la MAC asociada. Si persiste una entrada dinámica antigua, es razonable eliminar solo esa asociación tras registrar la dirección observada. Verificar que el servidor nuevo anuncia su IP sin conflicto y que el tráfico reaprende la MAC correcta.

82.10.3. Dos equipos con la misma IPv4

Si la IP cambia repetidamente entre dos MAC y el sistema registra mensajes de movimiento ARP, contrastar con DHCP, switch y equipos implicados antes de calificarlo como ataque. Puede tratarse de duplicidad de IP, clustering, teaming, un proxy o una sustitución legítima. Eliminar la caché no corrige la causa de la duplicidad.

82.10.4. Router de otra VLAN sin respuesta

Un firewall que consulta la MAC del siguiente salto en una VLAN equivocada mostrará entradas ausentes o incompletas. Comprobar rutas, puerto trunk, pertenencia VLAN y enrutamiento antes de editar políticas de firewall. En redes remotas no se deben esperar MAC individuales de cada estación.

82.10.5. Wake-on-LAN de un equipo administrado

Guardar un destino WOL desde el icono + puede ahorrar transcripción de la MAC. La prueba de encendido necesita comprobar configuración del adaptador y firmware, disponibilidad eléctrica, segmento de difusión y arranque posterior; el envío del paquete no es confirmación de éxito.

82.11. ARP spoofing, movimientos y seguridad

Las respuestas ARP pueden falsificarse: un host malicioso puede anunciar una asociación IP→MAC indebida. Los síntomas incluyen cambios no esperados, intermitencias y errores de comunicación; pero también los producen eventos legítimos de HA, balanceo, virtualización o cambios de NIC. Conviene correlacionar los eventos con inventario de puertos, DHCP, registros y capturas, evitando acusaciones basadas únicamente en una MAC cambiante.

Para reducir riesgos se utilizan controles de acceso físico, segmentación VLAN, protección L2 del switching (según fabricante), inventario coherente, gestión del direccionamiento y vigilancia de eventos de movimiento ARP. Deshabilitar el registro de movimientos sin análisis previo elimina evidencias valiosas; cualquier ajuste de tunables debe justificarse y documentarse.

82.12. Advertencias de operación remota, HA y Multi-WAN

ADVERTENCIA Vaciar la tabla ARP puede causar interrupciones breves mientras se resuelven de nuevo vecinos esenciales, como el gateway WAN, servidores y equipos de administración. Planificar una ventana cuando exista criticidad y disponer de consola local o fuera de banda.

En redes con CARP, la presencia de IP virtuales puede crear entradas permanentes o asociaciones que cambian durante el failover. En Multi-WAN se deben estudiar por separado los vecinos de cada interfaz y los efectos de NAT o rutas. No interpretar una dirección MAC vista en WAN como la identidad del servidor remoto final: normalmente es el siguiente salto local.

82.13. Matriz de incidencias y validación

Síntoma	Hipótesis principal	Prueba prioritaria
(Incomplete) persistente	Equipo sin ARP Reply; VLAN errónea; enlace caído; IP inadecuada.	Captura ARP + switch + subred.
IP cambia entre MAC	Conflicto, NIC teaming, proxy o cambios legítimos.	Logs de movimiento + control de puertos.
Host no aparece	No comunicó recientemente con firewall.	Ping desde origen correcto; observar ARP.
Permanent sin respuesta	Entrada local/estática, no estado de host remoto.	Confirmar propiedad de IP y ruta.
Ping falla y ARP funciona	Bloqueo ICMP, ruta, firewall host o aplicación.	Packet Capture + firewall + pruebas TCP.

Síntoma	Hipótesis principal	Prueba prioritaria
Reaparece tras borrar	Entrada reconstruida por actividad/ARP legítimo.	Examinar origen y consistencia de MAC.

82.14. Lista de comprobación antes de cerrar una incidencia

Asociación IP/MAC, interfaz y VLAN verificadas sin reproducir información confidencial en informes destinados a terceros.

Prueba ARP documentada y diferenciada de ping, DNS y disponibilidad de la aplicación.

Causas alternativas consideradas: DHCP, duplicidad IP, firewall host, troncales, gateway y alta disponibilidad.

Cambios autorizados anotados: eliminación de entrada concreta o limpieza global, con hora y motivo.

Conectividad restablecida y confirmada desde ambos extremos cuando corresponda.

Registros, capturas y pruebas conservados conforme a la política corporativa de protección de datos.

82.15. Glosario técnico

Término	Definición
ARP	Address Resolution Protocol: descubrimiento de MAC para un siguiente salto IPv4 en el enlace local.
MAC	Identificador de enlace de red utilizado en Ethernet.
Caché ARP	Tabla temporal de asociaciones IPv4–MAC conocidas por el sistema.
Incomplete	Entrada pendiente de resolución ARP sin respuesta válida.
Broadcast domain	Conjunto de interfaces que reciben una difusión de capa 2.
Proxy ARP	Equipo que responde consultas ARP en nombre de otro destino.
NDP	Neighbor Discovery Protocol: descubrimiento de vecinos IPv6 mediante ICMPv6.
WOL	Wake-on-LAN: activación de una máquina mediante Magic Packet.
OUI	Prefijo de MAC que puede permitir identificar un fabricante, con limitaciones.

82.16. Referencias oficiales y verificables

Netgate — ARP Table

Netgate — Diagnostics (menú)

Netgate — Troubleshooting Offline DHCP Leases

Netgate — Wake on LAN

Netgate — Troubleshooting ARP Move Log Messages

Netgate — Nmap package

Netgate — Arping package

Netgate — Advanced Networking

Netgate — Troubleshooting Network Connectivity

Netgate — pfSense GUI: diag_arp.php (fuente)

Nota de aplicabilidad: nombres y comportamientos se han contrastado con la documentación vigente y el código público de pfSense. La disponibilidad de controles adicionales puede variar por versión, paquete y configuración.

83 Diagnostics → Authentication

Pruebas de identidad · base local · LDAP · RADIUS · depuración · grupos y permisos

La comprobación de credenciales es el primer paso de un diagnóstico de identidad, pero no sustituye las pruebas de autorización ni la validación completa del servicio que utilizará esas credenciales.

LÍMITE ESENCIAL Un resultado correcto en esta pantalla verifica autenticación básica. No garantiza por sí solo que funcionen EAP, MFA, un túnel VPN, un portal cautivo ni los permisos de la GUI.

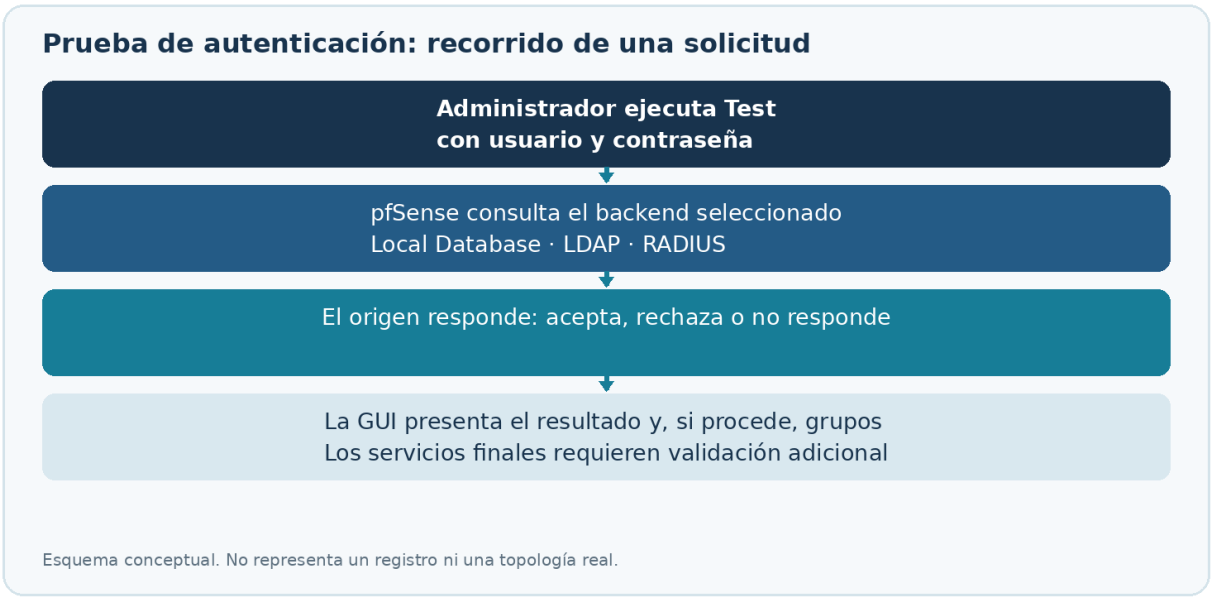


Figura 83.1. Flujo conceptual de una prueba de autenticación, sin datos de entornos reales.

83.1. Finalidad, alcance y ubicación

Ruta exacta: Diagnostics → Authentication. El formulario permite solicitar a pfSense Plus que compruebe un nombre de usuario y una contraseña contra un origen disponible en el administrador de usuarios. El resultado se presenta en la propia página. No crea cuentas, no cambia por sí mismo las credenciales y no sustituye la configuración de los servicios consumidores.

La pantalla utiliza el selector Authentication Server, los campos Username y Password, la casilla Set debug flag y el botón Test. Los servidores LDAP/RADIUS externos deben configurarse previamente en System → User Manager → Authentication Servers. En la pantalla examinada, el origen seleccionado es Local Database; no se deduce que existan orígenes externos configurados.

Elemento de la pantalla	Papel técnico
Ruta superior y ayuda contextual	Identifica la herramienta; la ayuda conduce a documentación relativa a la pantalla.
Authentication Test	Sección que agrupa el formulario y la ejecución de la prueba.
Icono de ajustes de cabecera	Acceso contextual de la interfaz; su destino exacto depende de la versión y no es un campo de autenticación.
Test	Envía la prueba y muestra una respuesta positiva o un fallo; no equivale a iniciar sesión en otro servicio.

83.2. Modelo de autenticación: identidad, autorización y servicio

Conviene separar tres conceptos. Identificación es declarar quién desea acceder; autenticación es demostrarlo (por ejemplo, contraseña); autorización es determinar qué puede hacer esa identidad. Una

prueba positiva solo demuestra el paso que se ha comprobado. Un usuario puede autenticar correctamente y carecer de permisos para la GUI o para conectarse a una VPN concreta.

83.2.1. Backend local y servicios externos

Local Database valida las credenciales de las cuentas locales del User Manager. Los orígenes externos LDAP y RADIUS delegan la comprobación a un servicio directorio o AAA. LDAP puede realizar búsquedas de directorio y operaciones de bind; RADIUS intercambia mensajes de petición y respuesta, con políticas y posibles atributos de grupo.

83.2.2. EAP y MFA: dónde termina la prueba

Netgate advierte que ciertos mecanismos especiales, entre ellos EAP, no quedan cubiertos por este test. Si una solución utiliza EAP-TLS, EAP-RADIUS, certificados de cliente, MFA o un cliente VPN, debe ejecutarse después una prueba real extremo a extremo con el método y servicio previstos. Un resultado negativo tampoco identifica por sí mismo la causa; pueden intervenir red, configuración o política.

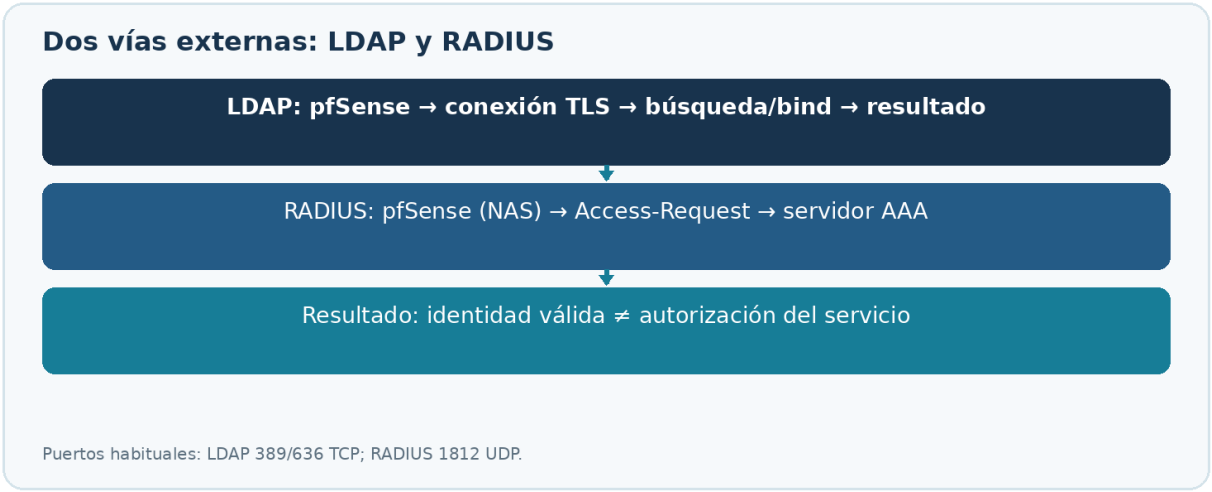


Figura 83.2. Comparación conceptual entre autenticación LDAP y RADIUS.

83.3. Campos y controles del formulario: explicación exhaustiva

Los siguientes nombres corresponden a controles visibles en la página, diferenciados de los parámetros que se configuran en otras rutas de pfSense Plus.

Campo/control	Opciones y comportamiento	Precaución
Authentication Server	Selector de origen; en la pantalla aparece Local Database. Servidores externos añadidos pueden aparecer como alternativas.	Seleccionar el origen equivocado puede producir falsos diagnósticos.
Username	Nombre de usuario que el backend verificará. El formato esperado depende del origen y de su configuración.	No introducir una cuenta administrativa si basta una cuenta de pruebas de mínimos privilegios.
Password	Contraseña correspondiente a la identidad. Se usa para solicitar la autenticación.	No registrar, copiar ni compartir el valor en capturas o documentos.
Debug — Set debug flag	Activa trazas diagnósticas adicionales al probar desde esta página. Netgate documenta su uso en el camino LDAP.	El detalle puede revelar información del directorio; no asumir que depura RADIUS o la base local.
Test	Ejecuta la comprobación y muestra el resultado; permite observar grupos devueltos cuando coinciden con grupos locales.	No prueba todos los permisos, protocolos ni el funcionamiento de la aplicación final.

83.3.1. Qué no aparece en el formulario

Los puertos, servidores, secretos compartidos de RADIUS, bases DN, transporte TLS, CA y atributos de grupo se definen en System → User Manager → Authentication Servers, no en esta pantalla. Tampoco existe en la captura un selector de método EAP o una opción para conceder permisos automáticamente.

83.4. Interpretación de resultados

El resultado normalmente identifica una autenticación aceptada o fallida. Es indispensable completar el diagnóstico con registros y una prueba del servicio de destino. Algunos errores de conexión pueden confundirse con credenciales incorrectas desde el punto de vista del usuario.

Observación	Lectura prudente	Siguiente comprobación
Autenticación correcta	El origen ha aceptado la credencial en esta prueba básica.	Comprobar grupos, privilegios y servicio final.
Autenticación fallida	Credenciales, política, búsqueda, bind o contacto con el servidor podrían fallar.	Revisar origen seleccionado y registros de ambos extremos.
Grupos visibles	El origen devolvió grupos reconocidos localmente con el mismo nombre.	Revisar mapeos de privilegios y autorización concreta.
Grupos ausentes	No es prueba suficiente de fallo de autenticación.	Verificar los atributos devueltos y los grupos locales.
Respuesta muy lenta	Posible timeout, DNS, conectividad, MFA o carga del backend.	Medir tiempo y revisar parámetros de timeout del origen.

SEGURIDAD No compartir capturas del resultado sin revisar si aparecen usuarios, grupos, direcciones de servidores, nombres internos o detalles de diagnóstico.

83.5. Local Database: prueba y límites

Es el origen integrado de identidades locales. Resulta útil para comprobar si una contraseña es aceptada sin depender de DNS o de servidores LDAP/RADIUS externos. No obstante, tener credenciales válidas no implica que una cuenta posea el privilegio de administrar el firewall.

83.5.1. Procedimiento — comprobar una cuenta local

1. Entrar en Diagnostics → Authentication desde una sesión de administración autorizada.
2. Seleccionar Local Database en Authentication Server.
3. Escribir el usuario de prueba y su contraseña sin mostrarla ni registrarla.
4. Dejar Debug desmarcado, salvo que una comprobación específica y documentada indique lo contrario.
5. Pulsar Test y registrar solo resultado, fecha y cuenta pseudonimizada.
6. Confirmar, mediante el servicio de destino, que los permisos y el inicio de sesión reales son correctos.

83.6. LDAP: consultas, certificados y grupos

LDAP permite consultar directorios como Microsoft Active Directory, OpenLDAP o FreeIPA. La configuración y su estructura dependen del proveedor. En pfSense, un fallo puede proceder del nombre del servidor, resolución DNS, certificado, cuenta de bind, base DN, contenedor de autenticación, ámbito de búsqueda o filtro extendido.

83.6.1. Transportes y puertos habituales

LDAP estándar usa normalmente TCP/389 sin cifrado; STARTTLS negocia cifrado sobre TCP/389; LDAPS utiliza TLS desde el inicio sobre TCP/636. Netgate recomienda cifrar el tráfico LDAP porque puede contener credenciales y otros datos confidenciales. La CA emisora del certificado del servidor debe ser confiable para el firewall.

Ajuste externo	Validación	Error frecuente
Hostname	FQDN que resuelve y coincide con SAN/certificado.	Usar una IP que no figura en el certificado TLS.

Ajuste externo	Validación	Error frecuente
Transport / Port	STARTTLS TCP/389; LDAPS TCP/636, según servidor.	Confundir LDAPS y STARTTLS.
Peer Certificate Authority	CA o cadena emisora importada y seleccionada.	Falta de CA intermedia o certificado vencido.
Bind credentials	Cuenta de consulta con privilegios mínimos y alcance adecuado.	Contraseña caducada o cuenta sin permisos de búsqueda.
Base DN y Search Scope	Árbol correcto; a menudo es necesario Entire Subtree.	Buscar en OU equivocada o limitar el ámbito.
Extended Query	Filtro correcto según atributos/grupos del directorio.	Filtro LDAP mal formado o atributo inexistente.

83.6.2. Efecto y límites de Set debug flag

Netgate documenta que el depurado de esta página es reconocido actualmente por la ruta LDAP. Añade detalles de consultas y resultados al registro general del sistema. Activarlo únicamente durante una prueba controlada, recoger evidencia mínima y desactivarlo inmediatamente; no supone que el tráfico TLS pueda examinarse en una captura de red.

83.6.3. Procedimiento — probar LDAP con TLS

1. Confirmar que el servidor LDAP se ha definido en User Manager y que el transporte cifrado está habilitado.
2. Comprobar DNS, conectividad TCP/389 o TCP/636 y fecha/hora del firewall y del servidor.
3. Verificar cadena CA, nombre DNS y vigencia del certificado TLS.
4. Seleccionar la entrada LDAP en Diagnostics → Authentication.
5. Probar con una cuenta de alcance limitado y examinar el resultado.
6. Si falla, activar Debug para una segunda prueba puntual y leer Status → System Logs → System; desactivarlo al concluir.
7. Validar el grupo y el inicio de sesión final en el servicio que usará LDAP.

83.7. RADIUS: AAA, puertos y decisiones de política

RADIUS es habitual con VPN, Wi-Fi empresarial y controles AAA. Para que pfSense utilice un servidor, debe existir como cliente/NAS autorizado, con un secreto compartido coincidente y con reglas de red que permitan el intercambio.

83.7.1. Autenticación y accounting

El puerto habitual de autenticación es UDP/1812 y el de accounting es UDP/1813; esta página ejecuta una prueba de autenticación, no un ciclo completo de accounting. La documentación recomienda proteger el tráfico RADIUS mediante red de gestión confiable o VPN si cruza redes externas.

83.7.2. Grupos, Class y límites de atributos

Netgate describe la devolución de grupos mediante el atributo RADIUS Class como una cadena delimitada por punto y coma. Las entradas deben coincidir con grupos locales para aparecer en el resultado de Diagnostics → Authentication. La biblioteca cliente documentada tiene un límite de respuesta de 4.096 bytes: listas grandes de atributos pueden truncarse, por lo que conviene verificar esa limitación en situaciones complejas.

Caso	Posible causa	Verificación práctica
Timeout	Puerto, ruta, firewall, servidor caído o NAS no permitido.	Captura UDP/1812 en ambos extremos; comprobar timeout.
Access-Reject	Contraseña, política, horario, grupo, estado de cuenta o método incompatible.	Consultar log del RADIUS/NPS y razón de rechazo.

Caso	Posible causa	Verificación práctica
Respuesta aceptada pero VPN falla	EAP, certificados, perfil VPN o autorización adicional.	Prueba de conexión real del servicio y su log.
Grupos no listados	Class ausente, formato incorrecto o grupos locales inexistentes.	Comparar respuesta y nombres de grupos.
Retardo por MFA	Tiempo para aprobar segundo factor superior al timeout.	Revisar ventana del método y parámetro externo de timeout.

83.7.3. Procedimiento — validar RADIUS de forma segura

1. Confirmar que el firewall está registrado como cliente/NAS y que el secreto compartido coincide.
2. Comprobar ruta y puerto UDP/1812 desde la interfaz de origen pertinente.
3. Seleccionar la entrada RADIUS y usar credenciales de una cuenta de pruebas autorizada.
4. Pulsar Test y correlacionar hora y resultado con el registro del servidor RADIUS.
5. Verificar grupos devueltos, privilegios y política del servicio consumidor.
6. Repetir la prueba en el servicio real cuando exista EAP, MFA o certificados.

83.8. Metodología escalonada de resolución de incidencias

Antes de modificar un backend, seguir una secuencia que permita distinguir errores de credenciales, transporte, consulta y autorización. Evitar reinicios del firewall o cambios masivos de contraseña como primera reacción.

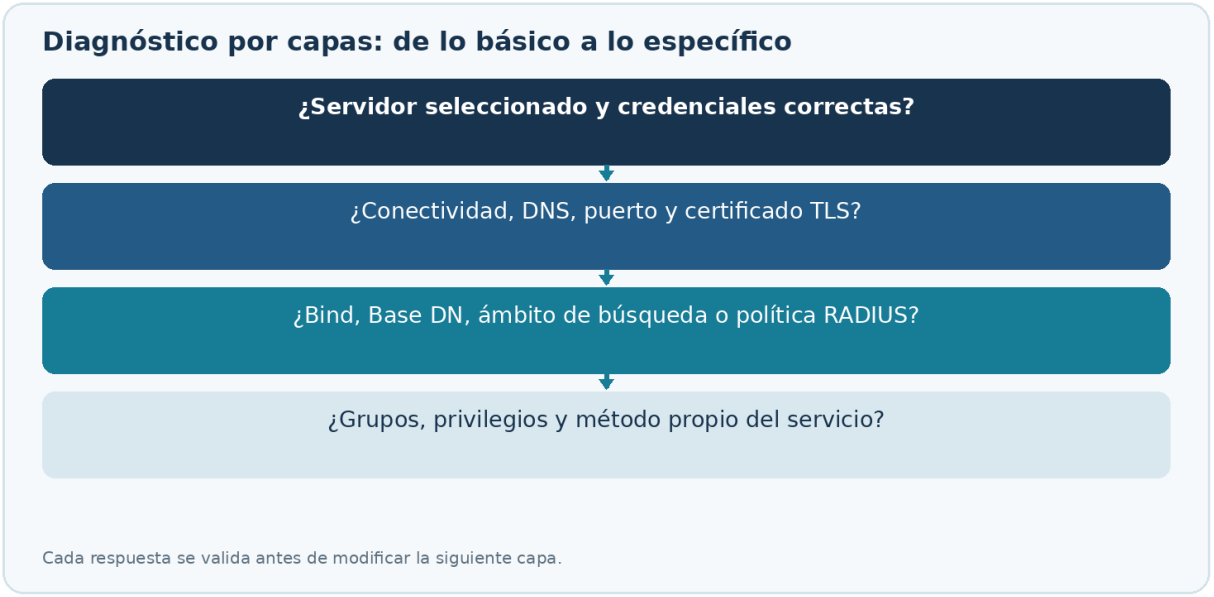


Figura 83.3. Cuatro capas para clasificar un fallo de autenticación.

Síntoma	Hipótesis inicial	Comprobación de menor impacto
No hay respuesta	Red, DNS, puerto, proceso o ACL.	DNS Lookup, Test Port para TCP y Packet Capture con autorización.
LDAP falla por certificado	CA, SAN o reloj desalineado.	Examinar cadena y fecha; no desactivar validación.
LDAP encuentra al usuario pero no lo admite	Bind, Base DN, scope, filtro o credencial.	Debug LDAP en una ventana controlada.
RADIUS rechaza	Política NPS/FreeRADIUS, método o cuenta.	Comprobar reason code en logs del servidor.
Login básico OK y VPN no	EAP, certificado, red del cliente o regla de servicio.	Seguir la secuencia completa del protocolo VPN.

Síntoma	Hipótesis inicial	Comprobación de menor impacto
GUI rechaza usuario válido	Permisos locales faltantes o diferencias en el backend.	Revisar grupos y permisos de User Manager.

83.8.1. Capturas de red y límites de visibilidad

Una captura puede confirmar paquetes, destinos, puertos y tiempos; no permite descifrar LDAP/TLS. No difundir capturas con RADIUS/LDAP sin auditoría previa, puesto que pueden revelar identidades o atributos. Si el servidor es externo, coordinar la comprobación con su administrador y contrastar hora, IP de origen y resultado.

83.8.2. Comprobaciones complementarias de pfSense

System → User Manager → Authentication Servers verifica el origen; Diagnostics → DNS Lookup prueba resolución; Diagnostics → Test Port ofrece pruebas TCP útiles para LDAP; Diagnostics → Packet Capture examina intercambio de paquetes; Status → System Logs muestra mensajes del sistema; el servidor LDAP/RADIUS proporciona la causa detallada cuando el firewall solo informa error genérico.

83.9. Escenarios empresariales reproducibles

Los ejemplos siguientes utilizan nombres y rangos reservados para documentación. Son modelos didácticos, no recomendaciones de publicar servicios de autenticación en Internet.

83.9.1. Directorio corporativo por LDAPS

Un firewall consulta ldap.example.com (192.0.2.50) por TCP/636. La CA raíz e intermedia están importadas; el usuario de bind tiene permisos de lectura mínimos. Una cuenta de prueba autentica correctamente, pero el acceso GUI se deniega por falta de grupo local adecuado. Solución: revisar el mapeo y privilegios, sin tocar certificados válidos.

83.9.2. Servidor RADIUS/NPS para VPN

Una instancia NPS de ejemplo en 198.51.100.30 escucha UDP/1812. El Test acepta el usuario, pero la conexión VPN real falla por una configuración EAP distinta. El administrador mantiene la prueba básica, revisa políticas NPS y ejecuta el cliente VPN para encontrar el punto exacto de rechazo.

83.9.3. MFA y tiempo de espera insuficiente

Un backend AAA solicita una aprobación externa; la respuesta puede tardar más que el timeout. La prueba muestra demora o error, aunque las credenciales sean válidas. La respuesta correcta es verificar la configuración del proveedor, la ventana de MFA y el timeout del servidor antes de cambiar los métodos de seguridad.

83.9.4. Contenedores y permisos LDAP

Una cuenta de directorio se encuentra en una OU diferente. Con Search Scope demasiado limitado, la búsqueda no devuelve al usuario; ampliar el ámbito de manera controlada y depurar el filtro permite resolver la consulta. Debe evitarse dar permisos excesivos al usuario de bind.

83.10. Protección de credenciales y continuidad administrativa

La herramienta concentra datos sensibles. La gestión operativa debe aplicar mínimo privilegio, cifrado de transporte, acceso restringido a la GUI y trazabilidad. Probar primero con identidades autorizadas y conservar siempre un mecanismo de administración local y consola para contingencias.

INTERVENCIONES DE ALTO RIESGO No desactivar la validación de certificados, abrir LDAP a redes públicas, cambiar secretos RADIUS en producción sin coordinación ni utilizar cuentas de administrador en capturas de prueba. Los cambios en la autenticación de GUI pueden causar bloqueo administrativo.

83.10.1. Seguridad de logs y evidencias

Un log ampliado puede incluir DN, nombres de cuentas, atributos de directorio y detalles de servidor. Conservar únicamente lo imprescindible y anonimizar antes de usarlo en incidencias, formación o documentación. Limitar accesos, aplicar retención proporcionada y asegurar los sistemas remotos que reciben syslog.

83.10.2. Reversión y acceso de emergencia

Antes de modificar el origen de autenticación de la GUI, verificar una cuenta local de emergencia y el acceso a consola. En caso de fallo del backend externo, estudiar los mecanismos de recuperación descritos por Netgate. No reiniciar ni restablecer credenciales indiscriminadamente durante una incidencia menor.

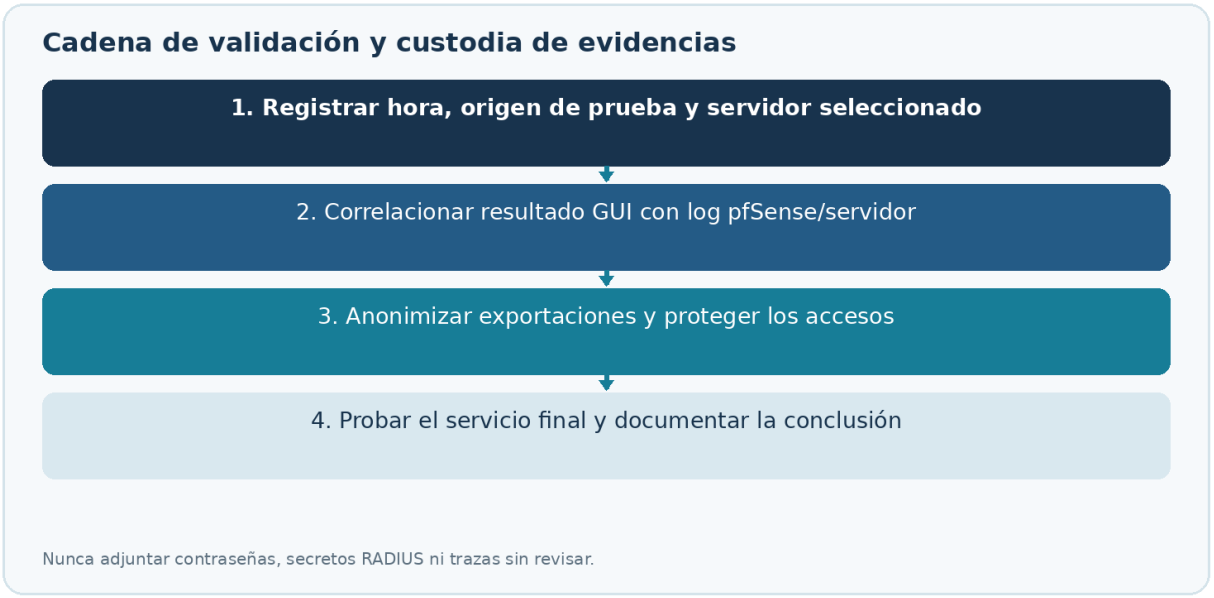


Figura 83.4. Ciclo de validación y custodia de evidencias de autenticación.

83.11. Procedimiento de aceptación de un origen nuevo

Una incorporación a producción se considera validada solo si la prueba básica y las comprobaciones del servicio consumidor pasan con una cuenta de ensayo y quedan documentadas con fecha y responsable.

Control de aceptación	Evidencia mínima esperada
Origen configurado	Nombre funcional, tipo, destino y responsable; sin secretos en acta.
Transporte seguro	Verificación de cifrado y CA en LDAP; canal protegido para RADIUS.
Conectividad	Resolución/puerto y respuesta del backend dentro de la ventana prevista.
Identidad válida	Resultado positivo de Diagnostics → Authentication.
Identidad no autorizada	Prueba negativa controlada, sin bloquear cuentas reales.
Grupos y permisos	Autorización conforme a política de mínimo privilegio.
Servicio consumidor	Prueba funcional de GUI, VPN o portal cautivo, según corresponda.
Registro y rollback	Referencia a logs anonimizados y plan de recuperación aprobado.

83.12. Relaciones con otras funciones de pfSense Plus

Diagnostics → Authentication se conecta funcionalmente con System → User Manager; con los servicios VPN y Captive Portal; con System Logs para el diagnóstico; y con DNS, rutas y reglas PF cuando el backend se aloja en otra red. Separar cada capa impide confundir una caída de conectividad con un problema de contraseña.

Función relacionada	Relación con la autenticación
System → User Manager	Cuentas locales, grupos, privilegios y orígenes externos.

Función relacionada	Relación con la autenticación
Status → System Logs	Pistas de LDAP, eventos de servicio y auditoría.
VPN → OpenVPN / IPsec	Autenticación real, certificados, EAP y perfiles del cliente.
Services → Captive Portal	Aplicación final de autenticación y autorizaciones.
Diagnostics → Packet Capture	Conectividad, retransmisiones y mensajes de red visibles.
Diagnostics → DNS Lookup / Test Port	Verificaciones previas de nombre y transporte TCP.

83.13. Glosario esencial

Los siguientes términos ayudan a interpretar los resultados sin confundir autenticación con concesión de permisos.

Término	Definición
AAA	Authentication, Authorization and Accounting; familia de funciones de identidad.
Bind LDAP	Operación de asociación/autenticación frente al servicio de directorio.
DN / Base DN	Nombre distinguido y punto de partida de búsqueda LDAP.
SAN / CA	Identidad incluida en certificado y autoridad emisora de confianza.
RADIUS NAS	Dispositivo cliente de RADIUS que envía peticiones al servidor.
Access-Accept / Reject	Respuesta RADIUS que acepta o rechaza una solicitud.
EAP	Marco de métodos de autenticación no cubierto íntegramente por este test.
MFA	Segundo o más factores de verificación de identidad.
Minimum privilege	Concesión de solo los permisos imprescindibles.

83.14. Referencias oficiales y documentación técnica

Documentación oficial de Netgate consultada para la verificación de campos, límites y procedimientos. Las opciones de servidores externos se desarrollan como contexto técnico y no se atribuyen a la pantalla Diagnostics → Authentication.

Netgate · Troubleshooting Authentication

Netgate · Authentication Servers

Netgate · LDAP Authentication Servers

Netgate · RADIUS Authentication Servers

Netgate · User Management and Authentication

Netgate · Active Directory con RADIUS/NPS

Netgate · Testing the FreeRADIUS Package

Netgate · OpenVPN Users with FreeRADIUS

Netgate · Troubleshooting Access when Locked Out

Netgate · Diagnostics Menu Guide

84 Diagnostics → Backup & Restore

Copias XML · recuperación · historial · cifrado · switch integrado · paquetes

La recuperación de un cortafuegos depende menos de disponer de un archivo que de saber qué contiene, cómo se protege y qué alterará al restaurarse. Esta herramienta reúne la exportación de configuración, su reposición, la recuperación de versiones previas y funciones asociadas a los paquetes.

REGLA OPERATIVA Antes de restaurar o reinstalar paquetes, conserve un respaldo completo comprobado fuera del firewall, asegure acceso por consola y programe una ventana de cambio. Una restauración integral reinicia el dispositivo.



Figura 84.1. Relación entre configuración, copia protegida y recuperación.

84.1. Finalidad, ruta y alcance de la herramienta

Ruta exacta: Diagnostics → Backup & Restore. En la interfaz presentada aparecen dos pestañas: Backup & Restore y Configuration History. La primera contiene Backup Configuration, Restore Backup y Package Functions; la segunda consulta revisiones y permite recuperar cambios anteriores. La ubicación y algunos controles pueden variar con la versión de pfSense Plus y la plataforma de hardware.

La configuración general reside en /conf/config.xml. Describe reglas, interfaces, servicios, usuarios y parámetros de paquetes. Los servicios generan sus archivos de ejecución a partir de ella; por tanto, guardar la configuración no equivale a copiar íntegramente el disco, los parches manuales o los archivos externos de todas las aplicaciones.

84.2. Mapa de los controles visibles y navegación

Zona / control	Papel en la página	Precaución
Backup area	Selecciona All o un área para exportación parcial	Una copia parcial no permite recuperar por sí sola todo el equipo.
Skip packages / Skip RRD data	Excluye información de paquetes o métricas históricas	Comprobar qué quedará fuera antes de descargar.
Include extra data / Backup SSH keys	Añade bases auxiliares y claves de host SSH	Puede aumentar tamaño y sensibilidad del fichero.
Encryption / Download configuration as XML	Protege opcionalmente y exporta la copia	Sin Encryption, el XML se descarga en texto claro.
Restore area / Configuration file	Determina alcance y archivo de origen	El área restaurada debe corresponder al tipo de copia.
Switch / Encryption / Restore Configuration	Preserva switch, descifra y restaura	La restauración integral puede cambiar LAN y reiniciar.
Reinstall Packages	Lanza la reinstalación de paquetes configurados	Puede interrumpir servicios de paquetes y requerir red.
Configuration History	Consulta, compara y recupera revisiones	La recuperación desde historial no reinicia automáticamente.

84.3. Qué se guarda y qué puede quedar fuera

En un despliegue habitual, config.xml contiene prácticamente toda la configuración del firewall. No obstante, los datos RRD, bases volátiles, registros, archivos modificados manualmente y determinados contenidos de paquetes requieren atención particular. En procedimientos de recuperación total debe mantenerse un inventario de recursos que no proceden del XML.

Elemento	¿Suele estar en el XML?	Criterio de recuperación
Reglas PF, NAT, interfaces, DHCP y VPN	Sí, como configuración	Validar aplicación y conectividad después de importar.
Paquetes y parámetros guardados en pfSense	Sí, salvo exclusión	Reinstalar binarios; comprobar compatibilidad y dependencias.
RRD de Monitoring	Opcional	Incluir solo si necesita históricos locales.
Leases y bases volátiles auxiliares	Opcional: extra data	No considerarlas inventario persistente.
Claves de host SSH	Opcional: Backup SSH keys	Preservan identidad SSH; custodia estricta.
Ficheros o parches manuales externos	No necesariamente	Procedimiento propio o paquete Backup Files/Dir.
SO, kernel y estado completo del disco	No	Instalador, ZFS Boot Environment o imagen independiente.



Figura 84.2. Elección del alcance, contenido, cifrado y custodia de la exportación.

84.4. Backup Configuration: Backup area

All es el valor visible en el selector y representa una copia completa de las áreas de configuración. Seleccionar un área reduce el archivo a la parte prevista para recuperación selectiva; la lista exacta de áreas depende de la versión y de los paquetes, por lo que no debe darse por fija sin abrir el desplegable. Para recuperación ante desastre o migración se recomienda All, antes de plantear respaldos parciales adicionales.

COMPATIBILIDAD Una restauración parcial exige seleccionar en Restore area el área correspondiente al archivo parcial y utilizar una revisión de configuración compatible. No es posible elegir una sección de un XML completo y restaurarla directamente mediante la restauración parcial.

84.5. Skip packages: información de paquetes

Al marcar Do not backup package information, la exportación omite datos de instalación y configuración de los paquetes. Es útil para aislar un fallo relacionado con un paquete, pero transforma el valor del archivo como respaldo integral. Netgate advierte que, al restaurar una copia sin estos datos, será necesario reinstalar y reconfigurar los paquetes afectados.

Sin marcar es el valor predeterminado documentado y el recomendable para una copia general de continuidad. La conservación de su configuración no garantiza que los archivos binarios se encuentren ya instalados en el destino ni que la versión del paquete sea compatible.

84.6. Skip RRD data: métricas y volumen

La casilla Do not backup RRD data aparece marcada. Así se excluyen las bases de datos de supervisión histórica RRD, lo que reduce el tamaño del XML. Desmarcarla puede preservar gráficas de CPU, redes y

gateways, pero añade carga y duración a la exportación e importación; el formulario advierte que pueden consumirse varios megabytes adicionales.

Para un plan de continuidad, la decisión depende del objetivo: restaurar configuración y servicio suele ser prioritario; conservar evidencias de tendencia puede justificar una copia específica de RRD fuera del archivo principal.

84.7. Include extra data: bases auxiliares y datos volátiles

Backup extra data está desmarcado en la pantalla. Su activación añade información adicional de ciertos servicios, entre ellos bases de datos de Captive Portal y concesiones DHCP/DHCPv6 cuando proceda. Es útil en migraciones controladas, pero puede ampliar el archivo y no sustituye los mecanismos de auditoría ni las copias de las bases propias de algunos paquetes.

El icono informativo junto a la opción identifica una ayuda contextual; las clases exactas de datos incluidos deben contrastarse con las características instaladas y las notas de la versión.

84.8. Backup SSH keys y continuidad de la identidad

La opción Backup SSH keys se muestra activada. Incluye las claves de host SSH utilizadas para identificar al firewall ante clientes remotos. Si se restauran, los administradores no reciben un cambio inesperado de huella SSH. También ayudan a preservar la continuidad de identificación de dispositivos en mecanismos de respaldo asociados a Netgate, sujeto al formato y la versión empleados.

SEGURIDAD Las claves privadas de host son secretos. Su conservación facilita migraciones legítimas, pero su exposición permitiría suplantar al equipo. En caso de compromiso, deben regenerarse y verificarse las huellas en los clientes.

84.9. Encryption: protección del archivo XML

La casilla Encrypt this configuration file aparece desmarcada. Si se activa, el formulario solicita una contraseña y su confirmación y cifra el archivo exportado con AES-256. En una copia sin cifrar, el XML puede contener material sensible, como secretos RADIUS, credenciales LDAP de enlace, certificados, claves VPN y contraseñas recuperables. La contraseña de cifrado debe gestionarse fuera del propio equipo y probarse en un entorno seguro.

El cifrado de un XML descargado no equivale a habilitar AutoConfigBackup: son flujos distintos. El transporte del archivo debe realizarse igualmente a través de una conexión HTTPS de confianza o una red de administración protegida.

84.10. Download configuration as XML: procedimiento de exportación

01. Acceder a Diagnostics → Backup & Restore desde una cuenta administrativa autorizada y comprobar versión, hora y nombre lógico del equipo sin incorporarlos a documentación pública.
02. Seleccionar Backup area = All para el respaldo de recuperación integral.
03. Revisar Skip packages, Skip RRD data, Include extra data y Backup SSH keys conforme a la política de respaldo.
04. Activar Encryption y utilizar una contraseña robusta custodiada en el gestor corporativo de secretos; no introducirla en tickets.
05. Pulsar Download configuration as XML, guardar el fichero en ubicación segura y comprobar su existencia e integridad sin publicarlo.
06. Registrar identificador de copia, revisión compatible, fecha y procedimiento de restauración; conservar al menos una copia externa probada.

84.11. Restore Backup: campos principales y comportamiento

La zona Restore Backup permite seleccionar Restore area, cargar Configuration file, preservar opcionalmente el switch integrado y descifrar el archivo cuando sea necesario. El botón Restore Configuration aplica la restauración. En una restauración completa el firewall se reinicia; una restauración de área individual no provoca reinicio ni actualización automática de todos los subsistemas.

Campo	Valor/acción visible	Consecuencia técnica
Restore area	All	Restauración completa al importar copia completa; para parcial, seleccionar área correspondiente.
Configuration file	Selector local de archivo	Sube el XML al firewall para validación y aplicación.
Switch	Preserve switch configuration	Mantiene configuración del switch integrado de la plataforma cuando está disponible.
Encryption	Configuration file is encrypted	Solicita contraseña para descifrar antes de restaurar.
Restore Configuration	Botón de acción	Modifica el estado del firewall; con copia completa reinicia automáticamente.

84.12. Preserve switch configuration: alcance y límites

En ciertos dispositivos Netgate con switch Ethernet integrado, la casilla Preserve switch configuration copia la configuración del conmutador activo al contenido restaurado. Es especialmente relevante al trasladar una configuración creada en una plataforma distinta. Esta opción no conserva ni recrea por sí sola todas las interfaces VLAN y LAGG relacionadas: debe validarse la asignación de puertos, la conectividad y la correspondencia lógica de interfaces tras recuperar.

PÉRDIDA DE ACCESO Un cambio de mapeo WAN/LAN, VLAN o puertos del switch puede impedir el acceso de administración después del reinicio. Antes de una restauración en hardware diferente, disponer de consola local o acceso fuera de banda.

84.13. Contraseña de archivos cifrados en la restauración

Cuando el archivo XML se exportó cifrado, hay que marcar Configuration file is encrypted y proporcionar su contraseña. La GUI determina el método de descifrado de copias compatibles. Si la clave no se conoce, la recuperación del contenido no debe considerarse viable; tampoco deben enviarse archivos ni contraseñas por correo sin cifrado.

84.14. Restauración completa: procedimiento controlado

01. Registrar estado previo del sistema: versión, revisión de configuración, gateways, interfaces, VPN, servicios y accesos administrativos de contingencia.
02. Comparar la revisión del XML con la versión de destino. Si procede de una revisión más reciente que el destino, detener el cambio y planificar una actualización compatible.
03. Comprobar si existe switch integrado, cambio de NIC, VLAN/LAGG o diferencia de puertos; obtener un respaldo vigente del equipo destino.
04. En Restore Backup, dejar Restore area = All, seleccionar el XML y activar Encryption si corresponde.
05. Decidir de forma explícita si se preserva el switch; ejecutar Restore Configuration dentro de la ventana aprobada.
06. Esperar la secuencia de recuperación y reinicio; comprobar por consola y GUI el acceso, las interfaces, DHCP/DNS, reglas, VPN y NAT.
07. Confirmar la recuperación con una prueba funcional y documentar incidencias; no borrar el respaldo anterior hasta finalizar la aceptación.



Figura 84.3. Ruta principal de una recuperación integral y comprobaciones tras el reinicio.

84.15. Restauración parcial: reglas prácticas

Solo debe utilizarse una copia que contenga exactamente la sección elegida, con revisión de configuración compatible. Netgate explica que la operación parcial no inicia un reinicio ni fuerza la relectura del subsistema: según el caso será preciso guardar/aplicar desde su página, volver a cargar el filtro o reiniciar el servicio correspondiente. Tampoco se debe asumir que funcionará cruzando versiones con revisiones de configuración diferentes.

01. Exportar una copia completa de seguridad del estado vigente, aun cuando la actuación vaya a ser parcial.
02. Verificar que el archivo de origen es un XML de copia parcial de la sección deseada y no un respaldo All.
03. Seleccionar Restore area correspondiente, elegir el XML y restaurar.
04. Reaplicar manualmente el componente afectado (por ejemplo, recargar PF cuando cambian reglas), de forma controlada.
05. Comprobar el resultado funcional y registrar los cambios en el historial y las evidencias de intervención.

84.16. Compatibilidad de revisiones y migraciones de plataforma

Origen → destino	Viabilidad documentada	Acción recomendable
Misma revisión de configuración	Completa y parcial compatibles	Probar en laboratorio si el destino es crítico.
Revisión anterior → versión más nueva	Copia completa suele migrarse mediante actualización interna	Probar con la versión de destino; comprobar paquetes.
Revisión nueva → versión más antigua	No compatible cuando el formato cambió	Actualizar destino, nunca asumir downgrade.
Parcial con revisión diferente	No hay mecanismo de conversión de área	Migrar la copia completa en laboratorio y extraer área compatible.
CE ↔ Plus / hardware distinto	Posible en algunos casos, no garantizado	Revisar NIC, switch integrado, drivers y licencias.

La coincidencia del número comercial de versión no sustituye el análisis de Configuration Revision. La restauración de hardware diferente requiere confirmar correspondencias de interfaces y disponibilidad de paquetes; algunas dependencias externas, como directorios de autenticación o redes remotas, no están incorporadas al fichero XML.

84.17. Configuration History: finalidad de la segunda pestaña

La pestaña Configuration History conserva revisiones anteriores guardadas localmente al modificar la configuración. Netgate documenta un historial predeterminado de 30 versiones anteriores más la vigente, configurable según versión. Es una herramienta de reversión de cambios accidentales, no una alternativa suficiente a las copias externas: un fallo de disco puede eliminar todo el historial local.

84.18. Columnas, acciones y filtros de Configuration History

Elemento documentado	Interpretación / uso	Precaución
Selección A y B	Elige dos versiones para Compare/Diff	Seleccionar antes/después según cronología.
Date	Fecha y hora de la revisión	Depende de reloj NTP y zona horaria correctos.
Configuration Change	Usuario/proceso y descripción del cambio	La descripción puede ser genérica; revisar diferencias reales.
Version/Revision	Número de formato de configuración	Clave para compatibilidad y recuperación.
Size	Tamaño del archivo XML	No refleja por sí solo la criticidad del cambio.
Restore / Download / Delete	Recupera, guarda o elimina una revisión	Restore desde historial no reinicia automáticamente.
Checkbox + Delete (Plus)	Selección múltiple de revisiones para eliminar	No es necesario vaciar historial para recuperar espacio.
Backup Count	Número de copias internas retenidas	Adecuar al volumen de cambios y espacio disponible.

En instalaciones Plus con ZFS Boot Environments puede aparecer un selector de entornos de arranque, con Base Version, Created y Last Booted. Cada entorno puede aportar su propio historial. La existencia de dicho selector depende del diseño del almacenamiento; no debe confundirse con una copia externa completa.

84.19. Comparar dos revisiones y revertir una modificación

01. Entrar en Configuration History y localizar las dos revisiones alrededor del incidente.
02. Seleccionar con los indicadores A/B la versión anterior y la posterior y ejecutar Compare/Diff.
03. Examinar cambios de reglas, interfaces, rutas y certificados; evitar exponer el diff en documentación abierta.
04. Descargar la revisión adecuada si se necesita una evidencia o una copia externa de seguridad.
05. Utilizar Restore sobre la revisión elegida, sabiendo que esta operación no provoca reinicio automático.
06. Volver a aplicar el subsistema necesario o reiniciar de forma planificada si el cambio lo exige; verificar el acceso y servicio.



Figura 84.4. Secuencia de diagnóstico, comparación y recuperación de un cambio fallido.

84.20. Recuperación por consola cuando la interfaz web falla

Netgate documenta la opción 15 del menú de consola: Restore recent configuration. Permite seleccionar una copia previa del historial si el cambio ha impedido entrar a la GUI. Exige acceso físico, consola serie o un canal de administración fuera de banda, y por ello forma parte del plan de contingencia. Los cambios de interfaz o de firewall que corten la gestión remota no pueden solucionarse con garantías desde la misma sesión afectada.

84.21. Package Functions: Reinstall Packages

El botón Reinstall Packages aparece cuando existen paquetes configurados y redirige al proceso de reinstalación de los paquetes del sistema. No equivale a restaurar todo el firmware, ni a reparar automáticamente configuraciones externas omitidas del XML. Puede depender de repositorios y conectividad y ocasionar reinicios de procesos que prestan servicios, por ejemplo IDS, proxy o VPN complementarias.

OPERACIÓN DISRUPTIVA No usar Reinstall Packages como paso rutinario ante cualquier incidencia. Primero verificar repositorios, espacio libre, versión y logs, exportar un XML completo y disponer de un plan de reversión. La operación puede dejar temporalmente inoperativos servicios dependientes de paquetes.

84.22. Diferencia entre XML local, historial, ACB y ZFS

Mecanismo	Qué protege principalmente	Límite clave
Exportar XML	Configuración en archivo portable	Requiere custodia y pruebas de restauración.
Configuration History	Cambios recientes en el propio firewall	Se pierde con fallo de almacenamiento.
AutoConfigBackup	Copias cifradas remotas asociadas a clave de dispositivo	Requiere contraseña y clave; no sustituye otros datos.
ZFS Boot Environment (Plus)	Entorno de arranque del SO y reversión de actualizaciones	No es copia externa de todo el sistema.
Backup Files/Dir (paquete)	Ficheros y directorios seleccionados	Depende del paquete y configuración concreta.

84.23. Protección de credenciales, certificados y datos sensibles

El archivo puede incluir claves privadas, secretos de túneles, identificadores de redes, credenciales de integración y parámetros completos de la topología. La copia se debe clasificar como información confidencial de máxima sensibilidad. Se aconseja cifrar antes de abandonar el firewall, aplicar almacenamiento segregado con permisos mínimos, control de versiones, acceso MFA y registro de descargas y restauraciones.

Para compartir fragmentos con soporte o colaboradores hay que anonimizar direcciones, hostnames, MAC, usuarios, certificados y claves; no basta con ocultar una IP visible. Nunca se debe adjuntar el config.xml original a un documento formativo ni reutilizar el fichero completo en un laboratorio no aislado.

84.24. Procedimiento de prueba periódica de recuperación

1. Crear y cifrar una copia completa y comprobar su checksum mediante una herramienta de estación autorizada.
2. Implantar una VM o dispositivo de pruebas con versión compatible y red aislada; evitar conflictos DHCP, CARP y VPN con producción.
3. Restaurar el XML, corrigiendo las correspondencias de interfaces para el entorno de pruebas.
4. Verificar apertura de GUI, autenticación, reglas PF, DHCP/DNS, VPN, NTP y demás servicios que apliquen.
5. Documentar tiempo real de recuperación, problemas detectados y elementos fuera del XML.
6. Cerrar la prueba desactivando o destruyendo el laboratorio y protegiendo todas las copias temporales.

84.25. Escenarios empresariales y elección de método

Escenario	Método más apropiado	Evidencia exigida
Regla errónea bloquea administración	Consola: historial reciente / reversión	Acceso GUI, regla PF verificada, log.
Fallo de almacenamiento principal	Reinstalación + XML/ACB externo	WAN/LAN, VPN, paquetes y servicios recuperados.

Escenario	Método más apropiado	Evidencia exigida
Migración a otro equipo Netgate	XML completo + revisión de switch e interfaces	Puertos, VLAN, rutas, MAC y políticas verificadas.
Error tras cambio de servidor DHCP	Historial o copia parcial compatible	Concesiones, DNS y alcance correcto del servicio.
Paquete crítico dañado	Reinstall Packages tras backup y revisión	Paquete y servicio operativo, registros limpios.

84.26. Matriz de incidencias y actuación segura

Síntoma	Causa probable	Primera actuación
El XML no se importa	Cifrado, revisión incompatible o fichero truncado	Validar origen, contraseña e integridad; no forzar.
Tras restaurar no entra la GUI	Cambio de interfaz/ACL/VLAN/switch	Usar consola y revisar asignación y filtros.
Restauración parcial sin efecto	Área no reaplicada	Guardar/aplicar componente o programar reinicio.
Faltan paquetes al recuperar	Backup sin datos o repositorio inaccesible	Revisar Installed Packages y registros.
Alertas SSH tras migración	Claves de host cambiadas	Verificar nueva huella por canal seguro.
No aparecen históricos RRD	Skip RRD data habilitado	Aceptar omisión o recuperar RRD alternativos.
Falta historial en ZFS	Boot Environment distinto	Seleccionar entorno correcto si está disponible.

84.27. Lista de comprobación antes y después de restaurar

Momento	Comprobación / evidencia	Resultado esperado
Antes	Copia All cifrada externa y clave disponible	Archivo íntegro y contraseña probada.
Antes	Compatibilidad, hardware, VLAN y puertos	Plan de retorno y acceso de consola.
Durante	Registro de acción, ventana y responsable	Control del cambio, sin secretos en actas.
Después	Acceso GUI, rutas, DHCP, DNS, NAT y VPN	Servicios críticos disponibles.
Después	Monitorización, logs y estado de paquetes	Operación estable y documentada.

84.28. Glosario técnico de recuperación

Término	Definición operativa
config.xml	Archivo XML de configuración central de pfSense.
Configuration Revision	Versión del formato interno de la configuración.
Backup Area	Ámbito del archivo exportado o de la restauración parcial.
RRD	Base histórica de datos para gráficos de Monitoring.
ZFS Boot Environment	Instantánea de entorno de arranque que permite reversión de sistema.

Término	Definición operativa
ACB	AutoConfigBackup: respaldo remoto cifrado de configuración.
SSH host key	Clave que identifica criptográficamente al servidor SSH.
VLAN / LAGG	Segmentación de capa 2 / agregación lógica de interfaces.

84.29. Ficha operativa para documentar una restauración

La trazabilidad ayuda a comprobar que una recuperación devuelve los servicios y no solo la interfaz administrativa. Esta ficha puede adaptarse al registro corporativo de cambios sin almacenar contraseñas, claves o XML de producción en el acta.

Campo de control	Registro recomendado
Identificador y motivo	Código del cambio, incidencia y nivel de urgencia.
Respaldo de origen	Fecha, revisión de configuración y checksum; sin copiar secretos.
Alcance	All / área parcial; indicar si afecta a switch, VLAN, paquetes o RRD.
Plan de recuperación	Consola disponible, persona autorizada, tiempo de interrupción aceptado.
Comprobación funcional	Pruebas de WAN/LAN, GUI, DHCP, DNS, VPN, NAT, rutas y servicios.
Resultado y cierre	Conforme/no conforme; incidencias, reversión y evidencias conservadas.

Un simulacro satisfactorio deja constancia del tiempo necesario para recuperar la administración, del orden de comprobaciones y de las dependencias externas que quedaron fuera del archivo. Debe repetirse cuando cambien significativamente el hardware, las interfaces, los paquetes o la política de seguridad.

84.30. Referencias oficiales y lecturas complementarias

[1] Netgate — Making Backups in the GUI
[2] Netgate — Restoring from Backups / Configuration History
[3] Netgate — Backup and Recovery
[4] Netgate — Backup Compatibility / Different Version
[5] Netgate — Caveats and Gotchas
[6] Netgate — Password Storage Security Policies
[7] Netgate — XML Configuration File
[8] Netgate — Automatic Configuration Backup Service
[9] Netgate — AutoConfigBackup Configuration
[10] Netgate — Recover During Installation
[11] Netgate — Package Manager
[12] Netgate — Console Menu Basics
[13] Netgate — Backing Up External Files and Directories
[14] Netgate — Pre-Upgrade Tasks

Las rutas, controles y requisitos reflejan el comportamiento descrito por Netgate y los campos visibles de la interfaz tratada. Las diferencias entre versiones o paquetes deben verificarse en el firewall de destino antes de una operación de recuperación.

85 Diagnostics → Command Prompt

Shell · transferencia de archivos · PHP · administración segura · diagnóstico

Una consola web es un instrumento excepcional de diagnóstico, pero también una vía directa para alterar el sistema. Este capítulo establece cuándo utilizarla, cómo interpretar su respuesta y cómo preservar la continuidad del cortafuegos.

CONTROL DE RIESGO La ejecución de comandos y código PHP puede modificar reglas, servicios, archivos o credenciales. Antes de utilizar funciones con efectos, preparar un respaldo, disponer de acceso fuera de banda y revisar cuidadosamente la instrucción.

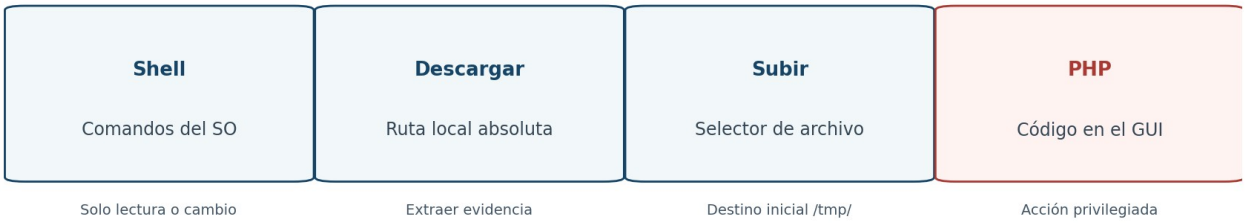


Figura 85.1. Cuatro capacidades de administración reunidas en una misma página.

85.1. Finalidad, alcance y ruta exacta

Ruta: Diagnostics → Command Prompt. La página permite ejecutar comandos de la shell del sistema, descargar archivos del firewall, cargar archivos desde el equipo del administrador y ejecutar código PHP. Netgate advierte que no es una herramienta de mantenimiento ordinario ni una alternativa segura a los formularios de configuración: se reserva para administradores experimentados o indicaciones de soporte técnico.

A diferencia de una terminal interactiva tradicional, la GUI devuelve los resultados cuando el comando finaliza. El proceso tiene el contexto y los privilegios que le permite el mecanismo del firewall; por ello, no debe tratarse como un entorno aislado o sin consecuencias.

85.2. Anatomía de la pantalla e identificación de controles

Bloque / elemento	Función visible	Comportamiento / cautela
Advanced Users Only	Advertencia de uso avanzado.	El mensaje es preventivo; no es un control de activación.
Execute Shell Command · Command	Caja de texto de una instrucción Shell.	Se envía para ejecución en el sistema.
« / »	Recuperar órdenes anteriores de la sesión web.	Historial local de la página; no equivale a auditoría persistente.
Execute (Shell)	Ejecutar el comando escrito.	Esperar retorno; evitar tareas que no terminan.
Clear	Limpiar el campo o resultado mostrado en ese control.	No deshace un comando ya ejecutado.
Download File	Ruta absoluta del archivo a obtener.	La descarga debe tratarse como posible información sensible.
Download	Enviar el archivo al navegador.	No produce una copia de respaldo integral por sí solo.
Upload File · Seleccionar archivo	Elegir archivo del equipo local.	Su contenido se coloca inicialmente en /tmp/.
Upload	Transferir el archivo al sistema.	No significa ejecutarlo ni instalarlo.
Execute PHP Commands · Command	Área multilínea para instrucciones PHP.	Puede acceder a funciones internas: alto riesgo.

Bloque / elemento	Función visible	Comportamiento / cautela
Execute (PHP)	Ejecutar el código PHP indicado.	El resultado o error aparece en la interfaz.

85.3. Por qué esta herramienta requiere privilegios especiales

La ventana no aplica las garantías de los asistentes: una instrucción puede saltarse validaciones de campos o alterar archivos sin crear una entrada clara en Configuration History. Las operaciones de lectura también pueden revelar claves, identificadores, IP, rutas, usuarios o configuraciones privadas. La autorización de acceso a Diagnostics y los permisos individuales deben aplicarse por mínimo privilegio.

NO EQUIPARAR Poder abrir la página no significa que cualquier comando esté recomendado o soportado. Netgate aconseja utilizarla solamente con conocimientos suficientes o bajo guía de TAC.

85.4. Ejecutar comandos Shell: secuencia de funcionamiento

01. Identificar el síntoma y seleccionar preferentemente una herramienta específica del menú Diagnostics.

02. Confirmar el impacto esperado; para diagnósticos iniciales usar comandos acotados y de solo lectura.

03. Escribir la instrucción en Command, verificar sintaxis, argumentos, ruta y duración.

04. Pulsar Execute una sola vez y esperar a que finalice. Registrar resultado sin copiar datos sensibles a terceros.

05. Correlacionar la salida con Status → Services, System Logs y el estado real de las conexiones.

Netgate explica que la interfaz necesita que el comando termine para mostrar la salida. Herramientas como ping sin número de paquetes, tcpdump sin límite o editores interactivos (vi) no deben ejecutarse desde esta página: pueden quedar en marcha sin producir una respuesta utilizable.

85.5. Historial efímero de comandos y botón Clear

Las flechas dobles izquierda y derecha recuperan los comandos introducidos previamente durante la sesión en la página. El navegador pierde esa lista cuando el administrador abandona la página, según la documentación oficial. No es un control para «deshacer»: una recarga del formulario o la limpieza del campo no revierte acciones sobre procesos, archivos, PF o rutas.

Para auditorías, la evidencia debe registrarse en el sistema de cambios corporativo y contrastarse con los logs pertinentes. La existencia y detalle de registros de actividad administrativa pueden variar con la acción ejecutada y la versión.

85.6. Comandos de inspección de bajo impacto

Comando	Qué muestra	Interpretación correcta
date	Fecha/hora de sistema.	Un reloj incorrecto dificulta correlacionar eventos; consultar NTP.
uptime	Tiempo encendido y carga media.	La carga no es porcentaje directo de CPU.
df -h	Ocupación de sistemas de archivos.	Vigilar tendencias y montajes; sin eliminar archivos.
netstat -rn	Tabla de rutas numérica.	La ruta presente no prueba la conectividad bidireccional.
pfctl -s info	Estado y contadores generales de PF.	Consultivo; diferenciar de acciones de recarga.
pfctl -sr	Reglas de filtrado cargadas en PF.	Puede mostrar reglas auto-generadas; no editar su salida.
sockstat -4 -l	Sockets IPv4 escuchando.	Un puerto abierto localmente no garantiza acceso desde WAN.
ping -c 3 192.0.2.10	Tres solicitudes ICMP a una IP de ejemplo.	Cambiar el destino por uno autorizado en una prueba real.

USO DIDÁCTICO 192.0.2.10 pertenece a TEST-NET-1 y no representa un destino de producción. No todos los binarios están disponibles en todas las versiones ni todos los comandos se comportan igual en todos los paquetes.

85.7. Diagnóstico acotado frente a procesos persistentes

Un comando que se mantiene activo consume recursos y puede bloquear la respuesta de la página o seguir ejecutándose tras abandonar la vista. Limitar por número de muestras, paquetes, duración o volumen, y preferir las herramientas GUI especializadas. Si el proceso queda sin retorno, no repetirlo indefinidamente; comprobar el estado mediante consola fuera de banda.

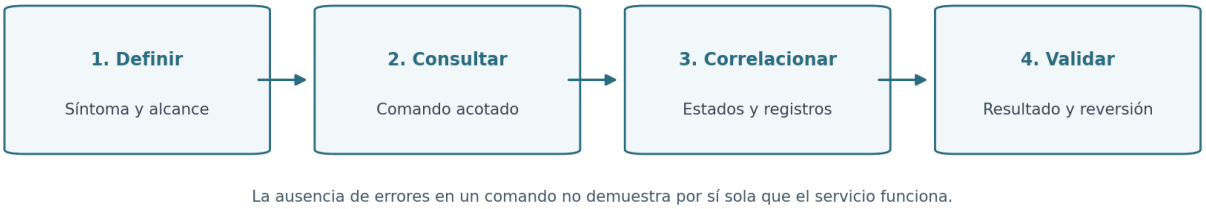


Figura 85.2. Flujo de diagnóstico seguro basado en evidencias y verificación.

85.8. Descarga de archivos: ruta y comportamiento

El bloque Download File recibe un nombre de ruta completo del sistema de archivos del firewall. Tras pulsar Download, el navegador solicita la descarga del archivo disponible. Es útil para recopilar una evidencia previamente generada, pero se debe comprobar su clasificación, tamaño y necesidad antes de extraerla.

01. Determinar qué archivo es necesario y asegurarse de que su descarga está autorizada.

02. Confirmar que el archivo existe y que no contiene secretos, datos personales ni una configuración completa innecesaria.

03. Introducir su ruta absoluta en File to download; por ejemplo, /tmp/status_output.tgz, si previamente se generó un paquete de diagnóstico.

04. Pulsar Download y custodiar la copia en almacenamiento cifrado con acceso restringido.

05. Registrar el origen, la fecha y el responsable; eliminar copias temporales según política corporativa.

DATOS SENSIBLES Los archivos de soporte pueden contener detalles de red, credenciales o tokens. La documentación de Netgate señala que incluso el archivo de diagnóstico que intenta ocultar secretos debe inspeccionarse antes de compartirlo.

85.9. Subida de archivos: ubicación temporal y riesgos

En Upload File se pulsa Seleccionar archivo, se elige un fichero local y se confirma con Upload. Netgate especifica que los archivos subidos se depositan en /tmp/. Desde allí, otras funciones podrían moverlos, pero subirlos no los instala, no los valida automáticamente y no habilita un servicio.

/tmp/ es una ubicación temporal y no un repositorio de configuraciones. La persistencia y el espacio disponible dependen de la plataforma; no almacenar allí el único ejemplar de una evidencia o respaldo. Verificar procedencia, formato, extensión y contenido antes de permitir cambios posteriores.

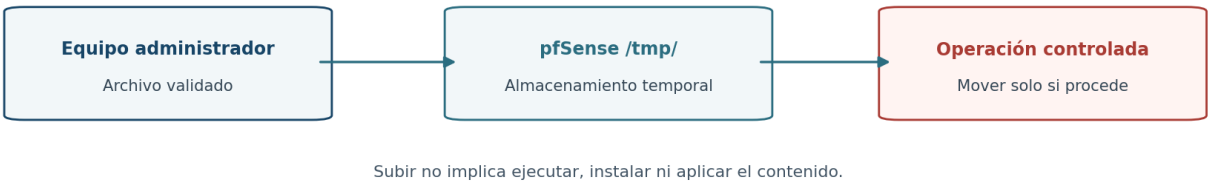


Figura 85.3. Ciclo de subida de archivos y separación entre transferencia y aplicación.

85.10. Ejecución PHP: qué aporta y por qué es especialmente delicada

El área Execute PHP Commands ejecuta código PHP dentro del contexto de pfSense. Su finalidad es el diagnóstico o reparación avanzada, no el desarrollo rutinario de scripts a través del navegador. Según

Netgate, el resultado o mensaje de error aparece en la misma página. El ejemplo visible de la interfaz únicamente imprime un mensaje.

Ejemplo inocuo y reproducible de salida, sin leer configuración ni ejecutar cambios:

```
print('Comprobación de PHP completada.');
```

Un script PHP podría invocar funciones internas, alterar la configuración o producir efectos equivalentes a comandos administrativos. No copiar fragmentos encontrados en Internet sin revisar su procedencia, alcance y compatibilidad; un error sintáctico puede simplemente fallar, pero un error lógico puede dejar el firewall inoperativo.

DISTINCIÓN Execute PHP Commands en la GUI y el desarrollador PHP Shell de consola (pfSsh.php) son mecanismos diferentes. Algunos comandos de playback de consola no están diseñados para ejecutarse en el formulario web.

85.11. Shell web, PHP web y consola de pfSense: diferencias

Mecanismo	Interacción	Uso recomendado
Execute Shell Command	No interactivo; devuelve salida al terminar.	Lecturas breves, comandadas por diagnóstico concreto.
Execute PHP Commands	Código PHP desde webConfigurator.	Solo procedimientos revisados o soporte especializado.
Consola local / SSH · opción 8	Shell interactiva de FreeBSD.	Diagnóstico que requiere terminal o trabajo controlado.
Consola · opción 12	PHP Shell y herramientas pfSense.	Administración experta; playback específicos.
Diagnostics → Packet Capture	Captura desde GUI, con límites y filtros.	Preferible a tcpdump libre para casos habituales.

85.12. Sustituir comandos genéricos por herramientas especializadas

Antes de utilizar esta página, buscar la función específica: Diagnostics → Ping y Traceroute para conectividad, DNS Lookup para resolución, Packet Capture para captura controlada, pfTop para estados PF, Status → Services para operación de demonios y Backup & Restore para configuraciones. Esas interfaces reducen errores de sintaxis y ayudan a documentar la acción.

85.13. Caso práctico 1: pérdida intermitente de acceso exterior

01. Anotar periodo de incidencia, interfaz, gateway y síntomas sin intervenir sobre reglas.

02. Consultar Status → Gateways y System Logs → Gateways, además de los eventos de WAN.

03. En Command Prompt ejecutar netstat -rn y pfctl -s info, ambos de consulta.

04. Contrastar rutas con el gateway seleccionado y realizar pruebas de DNS/ping desde las páginas específicas.

05. Documentar si la incidencia procede de enlace, ruta, DNS o reglas antes de aplicar una corrección.

85.14. Caso práctico 2: DNS Resolver operativo pero sin resolución

01. Verificar en Status → Services si unbound está iniciado.

02. Usar Diagnostics → DNS Lookup para comparar respuesta de distintos resolvers.

03. Si es preciso, revisar sockstat -4 -l para observar sockets en escucha; no confundir escucha con respuesta correcta.

04. Consultar System Logs → DNS Resolver y contrastar una consulta local y otra a través del cortafuegos.

05. Reiniciar el servicio solo tras identificar el motivo y disponer de autorización para interrumpir resolución.

85.15. Caso práctico 3: reglas PF y cambios aparentemente inefectivos

01. Registrar qué tráfico debería pasar o bloquearse y desde qué interfaz entra.

02. Consultar reglas en la GUI y, como comprobación adicional, ejecutar pfctl -sr sin parámetros modificadores.
03. Revisar Status → System Logs → Firewall y la tabla de estados en Diagnostics → States.
04. Recordar que una regla cambiada no anula necesariamente conexiones establecidas previamente.
05. Solo si está justificado, planificar una recarga del filtro y validar tráfico nuevo y existente por separado.

85.16. Caso práctico 4: entrega de evidencias al soporte

La utilidad de datos de diagnóstico de Netgate crea, cuando se utiliza según su procedimiento, un archivo /tmp/status_output.tgz. Puede descargarse desde Command Prompt si ya existe. Este archivo debe revisarse antes de enviarlo, porque puede contener IP, certificados, datos de clientes o detalles del entorno. Para una incidencia simple conviene compartir un extracto mínimo y anonimizado, no necesariamente un archivo de diagnóstico completo.

85.17. Clasificación del riesgo de comandos

Clase	Ejemplos conceptuales	Control mínimo
Consulta · bajo	Reloj, uptime, rutas, contadores.	Destino/volumen acotado; revisión de resultados.
Extracción · medio	Descargar logs o un archivo de diagnóstico.	Autorización, minimización y cifrado de evidencias.
Carga · medio/alto	Subir fichero a /tmp/ con fines de mantenimiento.	Procedencia validada, hash y aprobación.
Cambio de estado · alto	Reiniciar servicios, manipular reglas o rutas.	Ventana de cambio, consola y reversión.
Modificación persistente · crítico	Editar configuración, eliminar archivos o ejecutar PHP no revisado.	Respaldo probado y supervisión especializada.

85.18. Qué no debe hacerse desde esta página

No lanzar procesos infinitos o interactivos; no copiar comandos destructivos de terceros; no consultar y divulgar claves privadas por comodidad; no alterar directamente config.xml sin metodología de recuperación; no ejecutar cargas PHP desconocidas; no utilizar Upload para instalar paquetes no aprobados; no reiniciar indiscriminadamente servicios críticos para «probar».

EFECTO DEL BOTÓN CLEAR Clear actúa sobre la representación de la página, no sobre cambios realizados en el firewall. Un comando que ya modificó la configuración seguirá teniendo efecto hasta que se revierta explícitamente.

85.19. Reversión, pérdida de acceso y recuperación segura

La primera prioridad ante una ejecución que afecte a la administración remota es conservar evidencias y obtener acceso por consola local o por gestión fuera de banda. Si el error se limita a un servicio, valorar su estado y dependencias. Si se alteró la configuración, considerar Configuration History o una copia externa validada, siguiendo los procedimientos de recuperación de Netgate.

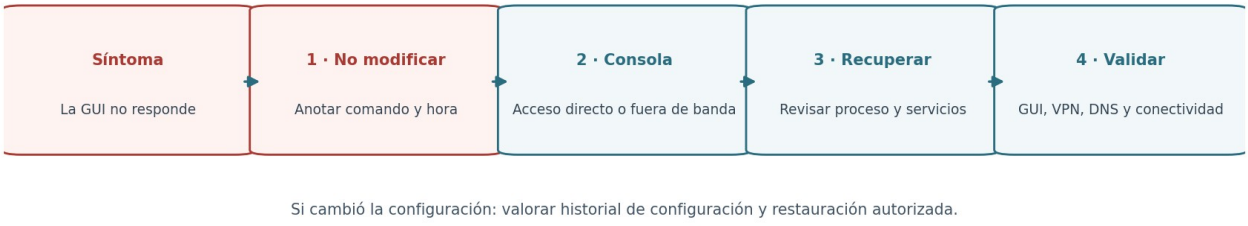


Figura 85.4. Escalera de recuperación ante una ejecución incorrecta.

85.20. Recomendaciones de seguridad del puesto administrador

Utilizar HTTPS, autenticación robusta y permisos limitados; operar desde una red de administración segregada y no publicar la GUI en Internet. Mantener credenciales fuera de campos de comando, capturas y tickets. En accesos compartidos, cerrar sesión después de trabajar y no confiar en el historial temporal de la página para trazabilidad. Proteger los ficheros descargados y destruir copias locales sin justificación de retención.

85.21. Compatibilidad con pfSense Plus, plataforma y versión

La ruta y las cuatro áreas mostradas corresponden a la interfaz examinada de pfSense Plus. El inventario de binarios, el resultado de utilidades, las rutas internas y determinadas funciones de PHP pueden variar según versión, arquitectura y paquetes instalados. No se debe presuponer que un procedimiento válido en pfSense CE o en otra versión de Plus es idéntico en un dispositivo actual.

85.22. Interpretación de errores y señales de alerta

Resultado	Causas posibles	Comprobación siguiente
Comando desconocido	Binario ausente, ruta o sintaxis equivocada.	Verificar versión y alternativa GUI; no instalar a ciegas.
Sin salida aparente	Proceso prolongado, red no responde o espera interactiva.	No repetir; consultar consola y límites de ejecución.
Permission denied	Privilegios, ruta, volumen solo lectura.	Revisar permisos; no forzar protecciones.
Archivo no disponible	Ruta incorrecta, evidencia no generada, caducidad temporal.	Confirmar existencia y ubicación del archivo.
Error PHP	Sintaxis, funciones o diferencias de versión.	No reintentar código mutador sin revisar.
GUI no responde	Proceso bloqueado o dependencia afectada.	Consola fuera de banda y revisión de servicios.

85.23. Procedimiento general de intervención en producción

01. Obtener aprobación del cambio o del diagnóstico y asignar responsable técnico.
02. Verificar copia de seguridad reciente y canal de administración fuera de banda.
03. Definir comandos, alcance, duración máxima y resultados esperados; evitar operaciones no revisadas.
04. Registrar inicio, contexto y líneas ejecutadas, excluyendo secretos de cualquier evidencia compartida.
05. Comparar resultados con las herramientas GUI y con la percepción del usuario final.
06. Aplicar plan de reversión si falla la validación y cerrar la incidencia con evidencias mínimas.

85.24. Matriz de validación posterior

Dimensión	Prueba mínima	Criterio esperado
Acceso	WebConfigurator por canal autorizado.	Acceso normal; cuentas y permisos intactos.
Red	Gateway y rutas de referencia.	Sin rutas inesperadas ni pérdida de salida.
Resolución	Consulta DNS local y remota.	Respuesta coherente dentro de tiempos esperados.
Seguridad	Reglas PF y logs recientes.	Sin reglas permisivas introducidas accidentalmente.
VPN	Estado de túneles críticos.	Sesiones y rutas conforme al diseño.
Evidencias	Inventario de artefactos en /tmp/.	Solo archivos autorizados, sin residuos sensibles.

85.25. Buenas prácticas documentales y custodia de evidencias

El informe técnico debe responder qué se pretendía comprobar, qué comando o función se utilizó, cuál fue el resultado, quién autorizó la acción y cómo se comprobó que el servicio continuó operativo. Evitar copiar el texto íntegro de salidas con direcciones reales o secretos a documentos generales. Si se necesita una muestra editorial, generar otra con rangos TEST-NET y nombres de example.com.

85.26. Glosario técnico

Término	Definición
CLI / Shell	Interfaz de ejecución de comandos del sistema operativo.
WebConfigurator	Interfaz de administración web de pfSense.
PHP	Lenguaje utilizado por funciones internas y páginas de administración.
stdout / stderr	Canales de salida estándar y errores de un proceso.
Proceso no interactivo	Tarea que no requiere intercambio continuo con una terminal.
/tmp/	Directorio temporal utilizado, entre otros fines, para cargas desde esta herramienta.
Fuera de banda	Acceso de administración independiente de la conectividad habitual.
Artefacto de diagnóstico	Archivo o salida recopilada para estudiar una incidencia.

85.27. Lista de comprobación antes de una orden administrativa

Antes de ejecutar	Verificación que debe constar en el ticket
Alcance	Síntoma identificado y objetivo concreto de diagnóstico.
Autorización	Responsable, ventana y criticidad de la actuación.
Seguridad	La orden no revela secretos ni altera permisos sin justificación.
Duración	El comando termina sin interacción y tiene límites de salida.
Recuperación	Consola disponible y copia/restauración compatibles.
Trazabilidad	Resultado esperado, hora, observación y evidencia anonimizada.
Cierre	Prueba funcional satisfactoria y limpieza de ficheros temporales.

85.28. Cuándo debe intervenir soporte especializado

Escalar a personal experto o a Netgate TAC si no se comprende el efecto de una instrucción, si se detectan errores del sistema de archivos, reinicios repetitivos, corrupción de la configuración, procesos persistentes que impiden responder a la GUI o discrepancias entre el estado de PF y las reglas aplicadas. También corresponde escalar cualquier ejecución PHP que necesite manipular funciones internas del producto sin un procedimiento validado.

PRUEBA DE RECUPERACIÓN La conclusión de un diagnóstico no es la ausencia de errores al ejecutar un comando, sino la restauración de la funcionalidad observable y la constancia de que no se han introducido cambios adicionales.

85.29. Referencias y documentación técnica oficial

- Command Prompt
- Diagnostics Menu Guide
- Console Menu Basics
- Using the PHP Shell
- Diagnostic Data
- XML Configuration File
- Backup and Recovery
- Restoring from Backups
- System Activity
- Troubleshooting Firewall Rules

Consultar siempre la documentación correspondiente al firmware instalado.

86 Diagnostics → Edit File

Editor de archivos del firewall · rutas · validación · persistencia · recuperación

Una utilidad capaz de leer, modificar y crear archivos en el sistema debe tratarse como una intervención privilegiada. El objetivo no es editar por editar, sino identificar con precisión cuándo la acción está justificada, qué archivo controla realmente el comportamiento y cómo recuperar el servicio si el cambio falla.

PRECAUCIÓN PRIORITARIA Netgate advierte que modificar un archivo equivocado o introducir errores en código y configuración puede inutilizar el firewall. Utilizar únicamente con conocimiento suficiente o siguiendo instrucciones de Netgate TAC.

86.1. Finalidad, alcance y ruta exacta

Ruta de navegación: Diagnostics → Edit File. La página integra un editor de texto que permite cargar y guardar contenido en el sistema de archivos del dispositivo pfSense Plus. La documentación oficial confirma dos operaciones principales: editar un archivo existente y crear uno nuevo a partir de una ruta y su contenido.

La herramienta no sustituye a un IDE, un shell interactivo, un sistema de control de versiones ni a los asistentes de configuración. Permite alterar archivos sin las validaciones específicas que normalmente ofrece la GUI, por lo que exige comprobación previa de cada cambio y una vía de reversión independiente de la propia página.

86.2. Identificación exhaustiva de la pantalla

Elemento visible	Función	Consecuencia o cautela
Advanced Users Only	Advertencia de riesgo en la cabecera.	No es un botón ni una protección técnica contra errores.
Save / Load a File from the Filesystem	Bloque único de lectura y escritura de archivos.	La operación afecta al archivo elegido en el firewall.
Path to file to be edited	Ruta completa del destino u origen.	Confirmar ruta, nombre y extensión; no usar rutas relativas.
Load	Carga el contenido del archivo indicado al editor.	No sustituye a Save; comprobar qué archivo se ha cargado.
Browse	Ayuda a localizar un archivo del firewall.	No es la selección de un archivo del equipo local.
Save	Escribe el contenido del área de edición.	Puede sobrescribir un archivo o crear uno nuevo.
GoTo Line # / número	Desplaza el foco de edición a la línea solicitada.	Control de navegación mostrado en la captura; el formato exacto de validación depende de la GUI.
Área grande de texto	Muestra y permite modificar el contenido textual.	No es un editor binario ni valida la lógica de los servicios.
Ayuda (?)	Acceso a ayuda contextual o documentación.	Usar para confirmar instrucciones antes de intervenir.

NAVEGACIÓN POR LÍNEAS GoTo Line # permite indicar una línea del archivo cuando la versión incorpora ese control. Load, Browse y Save gestionan la carga, selección y guardado. Comprobar el destino y conservar una copia antes de modificar archivos.

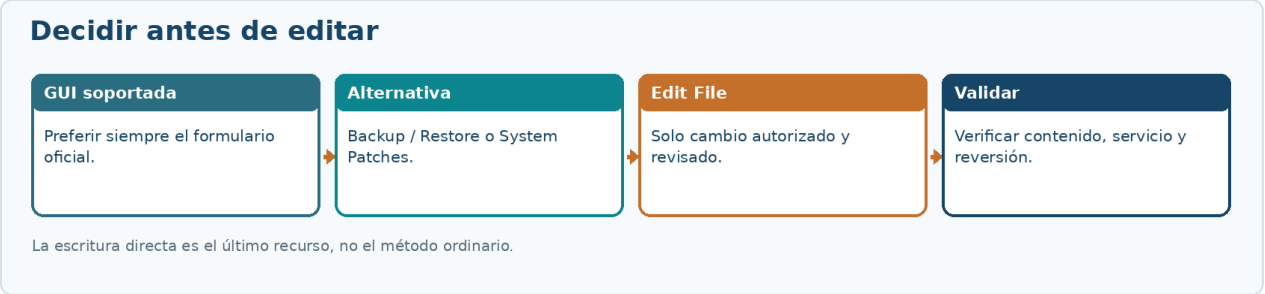


Figura 86.1. Criterio de decisión: GUI, alternativas soportadas y edición directa excepcional.

86.3. Qué significa Load, Browse, Save y GoTo Line

Load solicita la lectura del archivo cuya ruta se ha indicado; no constituye una copia de seguridad. Browse facilita seleccionar un elemento del sistema de archivos del propio firewall. Save guarda el texto editado en la ruta especificada. El control GoTo Line # actúa como ayuda de localización al trabajar sobre archivos extensos; no guarda ni aplica modificaciones por sí mismo.

La existencia de un mensaje de guardado correcto solo permite concluir que la operación de escritura fue aceptada. No demuestra que la sintaxis sea válida, que el servicio haya consumido el nuevo contenido o que el cambio sobreviva a una regeneración posterior.

86.4. Ruta absoluta, permisos y formatos

Una ruta absoluta comienza en la raíz del sistema, por ejemplo /tmp/ejemplo-editor.txt. En pfSense Plus 26.03, Netgate incorporó la exigencia de ruta absoluta al guardar desde diag_edit.php. La versión exacta del firewall de referencia no se asume: se explica este comportamiento como cambio documentado y se recomienda utilizar siempre rutas absolutas.

El archivo debe ser apropiado para edición textual y el sistema debe permitir la escritura. Un error al abrir o guardar puede deberse a una ruta inexistente, permisos insuficientes, sistema de archivos no escribible o contenido no compatible con un editor de texto. No es correcto deducir una causa concreta solo por la aparición de un error genérico.

86.5. Procedimiento seguro de lectura sin modificar el sistema

01. Delimitar el objetivo de consulta y escoger un archivo no confidencial, de texto y autorizado.
02. Anotar la ruta absoluta y comprobar por un canal seguro que es el archivo correcto.
03. Introducir la ruta en el campo y pulsar Load, o usar Browse y después Load.
04. Revisar el contenido sin pulsar Save; utilizar GoTo Line # para localizar una sección si fuera necesario.
05. Salir sin cambios y registrar la evidencia obtenida de forma anonimizada.

LECTURA PRUDENTE No copiar en informes completos archivos que contengan secretos, parámetros VPN, claves privadas, certificados o tokens; extraer únicamente la parte necesaria y anonimizarla.

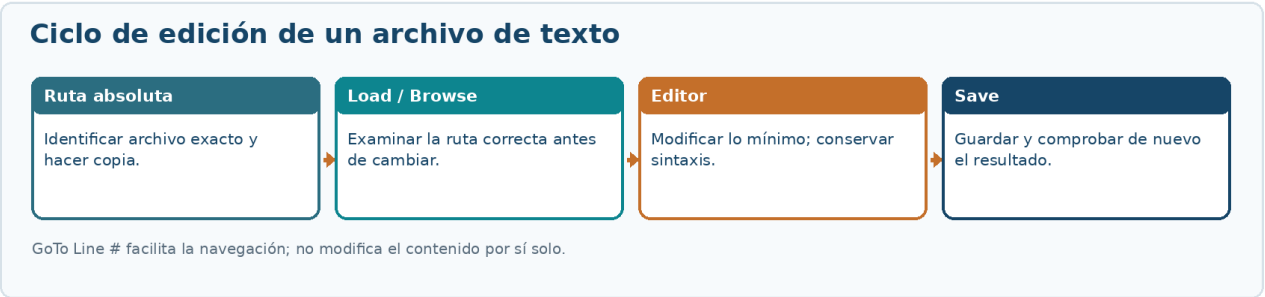


Figura 86.2. Operación de lectura/escritura y función auxiliar de navegación por líneas.

86.6. Edición de un archivo existente: procedimiento controlado

01. Obtener autorización, registrar versión, motivo y ventana de cambio. Verificar acceso alternativo por consola.

02. Hacer una copia del archivo concreto y, si afecta a la configuración, una copia completa de pfSense Plus.

03. Confirmar si el archivo es persistente, generado automáticamente, temporal o parte del software base.

04. Cargarlo, modificar únicamente las líneas necesarias y revisar sintaxis, saltos de línea y codificación.

05. Guardar una sola vez; recargar el archivo para verificar que el contenido escrito coincide con lo previsto.

06. Validar el servicio con el método específico y registrar el resultado, sin asumir que Save activa la modificación.

07. Si falla la prueba, restaurar la copia y ejecutar las medidas de reactivación documentadas para ese componente.

No realizar estas acciones sobre archivos de servicio críticos si el acceso al firewall depende del propio servicio. La restauración y activación pueden requerir consola, recarga específica o reinicio, según la clase de archivo.

86.7. Creación de un archivo nuevo

Para crear un archivo, la documentación oficial prescribe introducir una ruta nueva, redactar su contenido y pulsar Save. Por ejemplo, en un entorno de pruebas y con autorización, /tmp/ejemplo-editor.txt con el texto «Prueba documental sin datos operativos». Este ejemplo evita editar componentes funcionales de pfSense. El directorio /tmp es temporal: no debe utilizarse como almacenamiento durable ni como mecanismo de persistencia de configuraciones.

Antes de crear un archivo fuera de áreas temporales, verificar las convenciones del producto, la documentación del paquete que lo utilizará, los permisos requeridos y si el sistema lo eliminará, sobrescribirá o ignorará al reiniciar.

86.8. Persistencia: cuatro categorías que no deben confundirse

Clase	Ejemplo neutro	Riesgo de edición directa
Configuración central	/conf/config.xml	La caché y los servicios pueden no reflejar el cambio sin intervención adicional.
Configuración generada	Archivos operativos regenerados a partir del XML.	Una recarga, guardado o reinicio puede sobrescribir la modificación.
Archivo personalizado	Plantillas o datos específicos de una extensión.	No siempre se incluyen en la copia XML estándar.
Archivo temporal	/tmp/ejemplo-editor.txt	Puede desaparecer al reiniciar o por labores de limpieza.

Netgate documenta que el archivo config.xml es la fuente central de configuración y que muchos archivos de tiempo de ejecución son generados a partir de él. Modificar un archivo generado suele ser una solución inestable. Para cambios de código, System Patches es una alternativa controlable, aplicable y reversible.

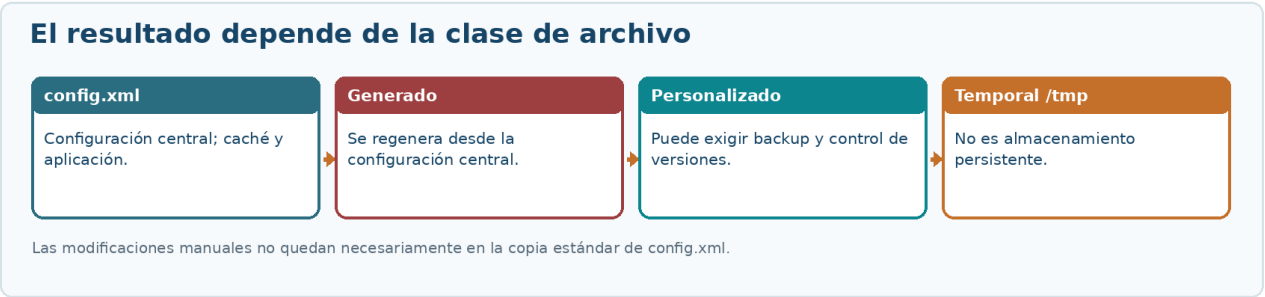


Figura 86.3. Persistencia de los cambios: XML central, archivos regenerados, personalizados y temporales.

86.9. Por qué no se debe editar config.xml sin un plan de recuperación

La configuración se almacena en /conf/config.xml. Si se modifica directamente desde Diagnostics → Edit File, no basta con pulsar Save: Netgate indica que debe tratarse la caché /tmp/config.cache y reactivar la

parte afectada mediante un guardado/recarga o reinicio. La edición en vivo también puede provocar errores de sintaxis, pérdida de conectividad o estados inconsistentes.

El procedimiento preferente para cambios manuales de XML, cuando sean imprescindibles, es exportar la configuración, editar la copia con un editor que respete finales de línea UNIX y formato XML, y restaurarla mediante Backup & Restore. Esta restauración completa conlleva reinicio; debe planificarse. La consola ofrece viconfig, que limpia la caché automáticamente, pero su uso también exige pericia.

NO EJECUTAR A CIEGAS La referencia oficial menciona limpiar /tmp/config.cache cuando se edita el XML en vivo. Esto se documenta como mecanismo técnico, no como instrucción universal para producción: hacerlo exige una estrategia de validación y recuperación específica.

86.10. Comparativa con otras herramientas de pfSense Plus

Herramienta	Finalidad principal	Cuándo elegirla
GUI de configuración	Cambiar parámetros soportados y validados.	Opción por defecto.
Diagnostics → Edit File	Leer/editar archivo textual del firewall.	Intervención excepcional autorizada.
Diagnostics → Command Prompt	Consultar sistema o ejecutar comandos.	Diagnóstico acotado y salida controlada.
Backup & Restore	Respaldar y recuperar configuración XML.	Cambios de configuración y recuperación.
System Patches	Aplicar/revertir parches de forma gestionada.	Cambios de código mantenibles o recomendaciones oficiales.
Consola / viconfig	Edición de XML y recuperación local.	Cuando la GUI está inaccesible y existe procedimiento validado.

86.11. Gestión de riesgos según archivo y acción

Acción	Riesgo	Medida mínima
Consultar un archivo informativo	Bajo/medio	Evitar exposición de información sensible.
Editar nota propia temporal	Medio	Crear copia y verificar ruta / contenido.
Cambiar ajuste de servicio regenerado	Alto	Usar interfaz de configuración; no editar manualmente.
Cambiar /conf/config.xml	Crítico	Copia completa, consola de rescate y ventana aprobada.
Editar código PHP o servicios base	Crítico	Soporte especializado; System Patches si corresponde.
Guardar ruta equivocada	Crítico	Validar nombre completo antes de pulsar Save.

GARANTÍA OPERATIVA Los cambios manuales en archivos del sistema pueden quedar fuera de las copias XML normales; hay que respaldarlos separadamente o emplear mecanismos oficialmente documentados para su persistencia.

86.12. Diagnóstico: el archivo se carga, pero el servicio no cambia

Secuencia de comprobación: identificar si el archivo editado es realmente utilizado por el proceso; comprobar si lo regenera la configuración de pfSense; verificar si requiere un recargado específico; revisar los logs; y evaluar si la configuración es válida y compatible con la versión instalada. Es incorrecto insistir en Save o reiniciar arbitrariamente: primero debe identificarse el mecanismo de aplicación.

86.13. Diagnóstico: error al cargar o guardar

Síntoma	Causas posibles	Comprobación recomendada
No se abre el archivo	Ruta incorrecta, inexistente o sin permisos.	Comprobar ruta absoluta y existencia por método de solo lectura.
Save no produce el efecto esperado	Archivo regenerado, caché o servicio sin recargar.	Revisar tipo de archivo y documentación del componente.

Síntoma	Causas posibles	Comprobación recomendada
Archivo nuevo no se encuentra	Ruta distinta o guardado rechazado.	Reabrir el destino exacto; no asumir creación.
El cambio desaparece	Regeneración por GUI, reinicio o actualización.	Migrar el cambio a GUI, XML o parche gestionado.
GUI deja de responder	Error en archivo crítico o servicio web.	Usar consola y copia de recuperación; evitar cambios acumulativos.
Caracteres alterados	Codificación o finales de línea no adecuados.	Comparar con copia; usar editor compatible con texto UNIX.

86.14. Escenario empresarial I: inspección de un archivo de diagnóstico

Un administrador necesita comprobar una salida generada previamente por una herramienta autorizada. Selecciona un archivo de texto sin secretos, lo carga, utiliza la navegación por líneas y recoge una evidencia mínima. No pulsa Save. El resultado es una consulta reproducible que no modifica la configuración ni el estado de los servicios.

86.15. Escenario empresarial II: archivo personalizado con control de cambios

En un laboratorio se necesita crear una nota de prueba temporal. Se registra la ruta absoluta y se crea en /tmp, se vuelve a cargar para confirmar el contenido y se comprueba que no interfiera con configuraciones operativas. Si el archivo debe persistir, el diseño se cambia antes de implantarlo: se elige un mecanismo respaldado y se prueba su recuperación.

86.16. Escenario empresarial III: corrección guiada por soporte

Netgate TAC facilita un procedimiento excepcional para corregir un archivo específico. Antes de actuar se conservan la copia original, versión, hash del archivo si procede y pasos de reversión. Se ejecuta el cambio mínimo indicado, se validan los servicios afectados y se evita extender la solución a otras versiones sin confirmación. Para parches de código repetibles se evalúa System Patches.

86.17. Escenario empresarial IV: pérdida de acceso tras una modificación

Después de alterar un archivo crítico, la interfaz web deja de funcionar. El objetivo no es efectuar más cambios remotos, sino recuperar el estado anterior desde consola o soporte autorizado. Se devuelve el archivo desde una copia íntegra, se comprueban los servicios y se documenta la causa raíz. Si el cambio afectaba a config.xml, se utiliza el procedimiento oficial de recuperación de configuración en vez de improvisar sobre archivos relacionados.

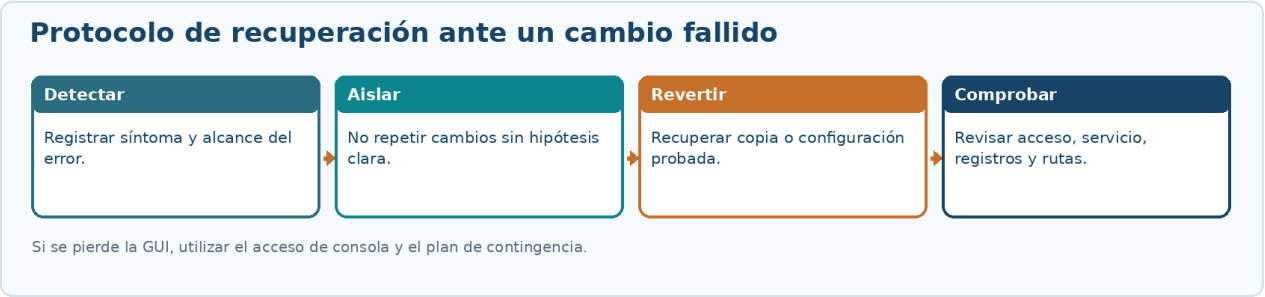


Figura 86.4. Recuperación ordenada tras un fallo de edición: detectar, aislar, revertir y comprobar.

86.18. Pruebas de aceptación posteriores a una modificación

Control	Resultado aceptable
Integridad del archivo	Ruta y contenido final coinciden con el cambio aprobado.
Servicio afectado	Iniciado y funcional, no solo con indicador de proceso activo.
Gestión	Acceso HTTPS o consola probado con una sesión independiente.
Red	Gateways, DNS, NAT y VPN críticos verificados si están implicados.

Control	Resultado aceptable
Persistencia	Comportamiento esperado tras recarga/reinicio, si está autorizado comprobarlo.
Reversión	Copia original recuperable y procedimiento probado o documentado.
Trazabilidad	Ticket de cambio sin secretos y con fecha, responsable y resultado.

86.19. Recomendaciones de seguridad y administración

Aplicar mínimo privilegio a la GUI, restringir la administración a redes de confianza y utilizar HTTPS. Auditar el acceso a herramientas avanzadas y evitar compartir pantallas o capturas que muestren secretos. Nunca cargar archivos con claves privadas en editores externos sin controles de custodia. Probar primero en laboratorio, no editar ficheros de sistema base como práctica rutinaria y evitar que una actualización sobrescriba cambios no documentados.

Para revertir modificaciones, recurrir a copias verificadas, versiones documentadas y soporte especializado. La ausencia de un historial de versiones dentro de Edit File no debe suplirse suponiendo que Configuration History conserva cualquier archivo del sistema: ese historial se centra en la configuración pfSense.

86.20. Glosario técnico

Término	Definición
Ruta absoluta	Localización completa desde la raíz del sistema de archivos.
config.xml	Archivo principal de parámetros persistentes de pfSense.
Archivo generado	Fichero creado dinámicamente a partir de otra fuente de configuración.
Cache de configuración	Representación temporal de datos para acelerar operaciones.
System Patches	Mecanismo gestionado de aplicación y reversión de parches.
viconfig	Herramienta de consola para editar la configuración central y limpiar su caché.
TAC	Servicio de soporte técnico de Netgate.
Rollback	Retorno controlado a una versión previa válida.

86.21. Lista de comprobación antes de guardar

01. ¿Existe realmente una razón técnica para evitar la GUI ordinaria?
02. ¿La ruta de destino se ha validado carácter por carácter y es absoluta?
03. ¿Hay copia íntegra, acceso por consola y procedimiento de reversión?
04. ¿Está confirmado si el archivo es fuente persistente o salida regenerada?
05. ¿Se ha revisado sintaxis, codificación, alcance y compatibilidad de versión?
06. ¿Existe una prueba funcional posterior y un plan de contingencia?

86.22. Referencias oficiales verificables

01. Netgate · Editing Files on the Firewall
02. Netgate · Diagnostics Menu Guide
03. Netgate · XML Configuration File
04. Netgate · Making Backups in the GUI
05. Netgate · Restoring from Backups
06. Netgate · Backup and Recovery
07. Netgate · Caveats and Gotchas
08. Netgate · 26.03 New Features and Changes
09. Netgate · System Patches Package

87 Diagnostics → Factory Defaults

Restablecimiento de configuración · control del cambio · recuperación · seguridad

El restablecimiento a valores de fábrica es una intervención de alto impacto que modifica el comportamiento de red y puede dejar inaccesible un firewall remoto. Dominar la pantalla exige entender qué vuelve a su estado inicial, qué permanece y cómo recuperar la administración sin exponer la red.

ADVERTENCIA PRIORITARIA Factory Reset no es una acción de diagnóstico inocua: elimina la configuración de usuario, intenta retirar paquetes y reinicia el equipo. Debe realizarse únicamente con autorización, copia externa verificable y acceso físico o consola previsto.

87.1. Finalidad técnica, alcance y ruta exacta

Ruta: Diagnostics → Factory Defaults. Esta página permite devolver la configuración de pfSense Plus a los valores iniciales mediante una confirmación expresa. Es útil para un equipo de laboratorio, una recuperación planificada o una reconfiguración desde cero; no es el procedimiento adecuado para una simple avería puntual que pueda corregirse restaurando una revisión o reparando un servicio.

La operación restablece el archivo de configuración y desencadena el arranque con valores predeterminados; Netgate indica que también trata de quitar los paquetes instalados. No reinstala el firmware, no sustituye una actualización ni garantiza la eliminación de modificaciones del sistema de archivos. La versión concreta y el modelo físico pueden influir en los detalles resultantes.

87.2. Identificación de todos los elementos visibles

Elemento de la pantalla	Función y resultado	Precaución
Diagnostics / Factory Defaults	Ruta y título de la página administrativa.	La ruta no indica el estado actual de los servicios.
Factory Defaults Reset	Panel explicativo de los cambios previstos.	Leer todos los efectos antes de confirmar.
Lista de ajustes predeterminados	Resume LAN, DHCP, WAN, credenciales y reinicio.	Es una lista informativa, no casillas editables.
Are you sure you want to proceed?	Pregunta final previa a la decisión.	El reinicio interrumpirá sesiones activas.
Factory Reset (rojo)	Inicia el procedimiento y solicita confirmación.	Acción destructiva sobre la configuración.
Keep Configuration (verde)	Abandona el restablecimiento y conserva la configuración.	No representa una copia ni una restauración.
Icono ? de ayuda	Acceso a ayuda contextual de la interfaz.	No modifica los parámetros.

Los procedimientos por consola, las diferencias por plataforma y la restauración XML se explican por separado. No son controles adicionales de la página Factory Defaults.

87.3. Cambios anunciados en el restablecimiento

Componente	Valor indicado	Implicación operativa
Configuración	Restablecimiento a valores iniciales.	Se pierden reglas, enlaces, VPN y parámetros personalizados.
LAN IPv4	192.168.1.1/24.	La gestión cambia de subred; riesgo de conflicto con otra red.
DHCP en LAN	Servidor DHCP habilitado.	Unirlo a una red corporativa puede introducir DHCP no deseado.
WAN IPv4	Cliente DHCP.	Una línea que exija PPPoE, IP fija o VLAN puede quedar inoperativa.

Componente	Valor indicado	Implicación operativa
Administración	Cuenta inicial admin / clave predeterminada pfsense.	Cambiar la contraseña inmediatamente; Plus moderno lo exige al primer acceso.
Reinicio	Se reinicia después de aplicar los cambios.	Las conexiones existentes se interrumpen.

La configuración inicial general también contempla el bloqueo de conexiones entrantes no solicitadas por WAN, salida permitida desde LAN, NAT IPv4 de salida y DNS Resolver habilitado. La documentación de instalación añade opciones IPv6 condicionales (delegación de prefijos, SLAAC y DHCPv6) que no deben interpretarse como promesas de conectividad sin un proveedor y configuración compatibles.



Figura 87.1. Secuencia controlada de restablecimiento y validación posterior.

87.4. Distinguir reset, reboot, restore y reinstalación

Operación	Qué hace	Qué no debe presumirse
Reboot	Reinicia el sistema con su configuración vigente.	No vuelve a fábrica.
Factory Reset	Sustituye la configuración por la predeterminada e intenta eliminar paquetes.	No constituye borrado seguro del soporte.
Restore Configuration	Carga un XML de respaldo y puede reiniciar el firewall.	Depende de compatibilidad y de datos auxiliares.
Reinstalación	Vuelve a instalar archivos del software desde el instalador.	No restaura por sí sola redes/VPN previas.
Recuperar revisión	Recupera un estado de configuración anterior.	No soluciona necesariamente corrupción de archivos del sistema.

87.5. Qué se pierde, qué puede persistir y qué no se garantiza

El restablecimiento elimina la configuración personalizada de interfaces, VLAN, reglas de firewall/NAT, VPN, certificados y usuarios configurados, así como la mayoría de los parámetros administrados desde la GUI. Los paquetes instalados se intentan retirar durante el proceso, pero no debe asumirse la eliminación perfecta de cualquier archivo agregado por ellos.

Netgate advierte que Factory Defaults no revierte necesariamente cambios practicados en el sistema de archivos. Por tanto, archivos personalizados, parches manuales, datos de paquetes y restos operativos pueden permanecer según la instalación. En ningún caso debe presentarse como eliminación criptográfica o borrado forense del dispositivo.



Figura 87.2. Ámbitos afectados por Factory Reset y límites del procedimiento.

87.6. Dependencia de versión, plataforma y puertos físicos

La versión pfSense Plus instalada no cambia a una edición antigua por ejecutar Factory Reset. Los parámetros iniciales deben comprobarse en la documentación vigente para esa versión. En pfSense Plus 24.03 y posteriores, el primer acceso requiere cambiar la contraseña de fábrica.

En equipos con switch integrado, las asociaciones entre conectores físicos y puertos lógicos pueden no coincidir con el esquema intuitivo de un PC de varias tarjetas. Los procedimientos mediante botones físicos también difieren: algunos dispositivos no disponen de botón de reset de configuración y el botón rotulado Reset puede ser solamente un reinicio de hardware. Antes de pulsarlo debe consultarse el manual del modelo concreto.

87.7. Impacto sobre servicios y dependencias

Área	Efecto probable	Validación necesaria
WAN / enlace de respaldo	Pérdida de PPPoE, dirección fija, etiquetado u otras opciones personalizadas.	Ver enlace, DHCP, gateway, DNS y salida real.
LAN / VLAN	Cambio de IP, subred y topología lógica.	Comprobar puerto LAN correcto y ausencia de conflictos.
DHCP / DNS	Restauración de servicios por defecto en redes iniciales.	Verificar concesión, gateway y resolución.
Firewall / NAT	Se pierden excepciones, redirecciones y reglas específicas.	Probar aplicaciones y publicación de servicios.
VPN	Desaparecen túneles y accesos remotos configurados.	No depender de VPN para finalizar la intervención.
HA / CARP / pfsync	Se pierden parámetros de clúster y sincronización.	Aislar, coordinar y documentar el rol de cada nodo.
Usuarios / SSH	Se reponen valores administrativos iniciales; SSH suele estar deshabilitado.	Cambiar contraseña y revisar usuarios/roles.
Paquetes	Se intenta su retirada; posibles restos en disco.	Reinstalar solo lo necesario y validar versiones.

CAMBIO DE RED PELIGROSO Si la subred LAN predeterminada coincide con una red existente o la WAN se conecta a la misma subred, la recuperación puede fallar por solapamiento. Realizar el primer acceso en una red aislada.

87.8. Preparación obligatoria antes de intervenir

01. Obtener autorización expresa, motivo técnico y ventana de mantenimiento; identificar servicios empresariales dependientes y responsables.

02. Descargar y guardar fuera del firewall un backup completo de config.xml; confirmar que el archivo es legible y que se conoce su contraseña si está cifrado.

03. Guardar por separado los datos no cubiertos por el XML: claves/archivos adicionales, información de paquetes, licencias y material necesario para reinstalar según el caso.

04. Anotar versión de pfSense Plus, esquema lógico de interfaces, acceso de consola autorizado y procedimiento de recuperación sin exponer identificadores en informes públicos.

05. Asegurar una estación de administración en una LAN aislada y el cable/puerto físico adecuados; prever que WAN y VPN desaparecerán.

06. Comunicar la interrupción, registrar un punto de control y tener preparada la posibilidad de restaurar el XML original.

87.9. Procedimiento 1: Factory Reset desde la interfaz web

01. Acceder con un usuario administrativo autorizado y navegar a Diagnostics → Factory Defaults.

02. Leer la lista de cambios; confirmar específicamente LAN, WAN, DHCP, usuario y reinicio.

03. Verificar copia externa, consola y desconexión o aislamiento de la LAN corporativa.

04. Pulsar Factory Reset solo dentro de la ventana autorizada.

05. Confirmar la operación mediante OK cuando la interfaz lo solicite. Si se decide no continuar, cancelar o utilizar Keep Configuration antes de iniciar el restablecimiento.

06. No volver a pulsar el botón ni cortar la energía durante el reinicio; observar el arranque desde consola cuando sea posible.

07. Conectar el equipo de administración a la LAN inicial y realizar las comprobaciones del apartado de validación.

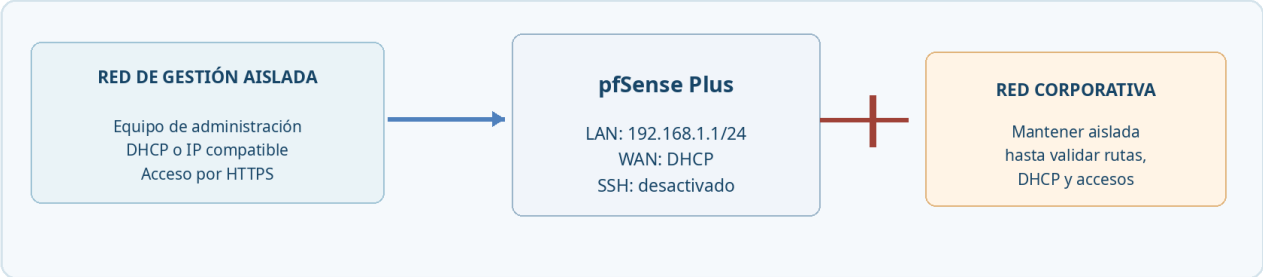


Figura 87.3. Administración inicial en segmento aislado para evitar conflictos y DHCP inesperado.

87.10. Procedimiento 2: recuperación desde consola

Netgate documenta una alternativa desde el menú de consola: acceder localmente o por un canal administrativo autorizado, elegir la opción Reset to factory defaults (habitualmente 4), pulsar Intro y confirmar escribiendo y. La numeración puede variar; debe leerse el menú efectivo del sistema. Esta ruta es útil cuando la GUI no está disponible y se conserva acceso autorizado.

El uso de SSH como acceso a consola no elimina el riesgo de desconexión cuando se aplican cambios de red. Para una recuperación crítica, la consola local/serie o el acceso fuera de banda debe ser el mecanismo de referencia.

87.11. Restablecimiento mediante botón de hardware

Solo debe intentarse cuando el manual oficial del equipo lo indique de forma expresa. El tiempo de pulsación, estado del equipo y comportamiento del botón cambian entre plataformas. Algunos botones producen únicamente un reinicio eléctrico o de hardware; usarlos como si fueran una restauración de configuración puede ocasionar una caída de servicio sin resolver el problema.

PROHIBIDO GENERALIZAR No se proporciona una secuencia universal de pulsación: primero identificar el hardware, consultar su manual oficial y mantener un plan de consola como respaldo.

87.12. Primer acceso seguro tras el reset

01. Conectar el PC a la LAN destinada a administración, sin interconectarla con una red productiva.

02. Configurar el PC como cliente DHCP o con una dirección compatible, evitando cualquier conflicto de subred.

03. Abrir https://192.168.1.1 y verificar la identidad del dispositivo por un canal confiable; no aceptar ciegamente un aviso TLS en una red no controlada.

04. Autenticarse con las credenciales de fábrica vigentes en la documentación del producto; sustituir inmediatamente la contraseña predeterminada.

05. Comprobar interfaz WAN, DHCP de LAN, DNS, reglas base y actualización/hora antes de reconectar servicios empresariales.

06. Restaurar una configuración validada o reconfigurar de forma gradual; registrar nueva copia segura después de las pruebas.

87.13. Riesgo de LAN por defecto y servidor DHCP imprevisto

Al activar DHCP en la LAN inicial, un firewall restablecido puede responder a solicitudes de clientes en una red a la que se conecte por error. En una infraestructura existente esto puede entregar puerta de enlace o DNS incorrectos y afectar a múltiples estaciones. Por ello, no unir la LAN restaurada a redes compartidas hasta validar el papel del servidor DHCP y sus enlaces.

El direccionamiento predeterminado 192.168.1.1/24 está documentado oficialmente como valor de fábrica, no como una dirección de ejemplo inventada. En los diagramas se utiliza exclusivamente para explicar ese valor universal y no se incorpora ningún direccionamiento privado de una instalación particular.

87.14. Riesgo de WAN, VPN y administración remota

Cuando la WAN vuelve a DHCP, los entornos con autenticación PPPoE, parámetros de ISP, VLAN WAN o IP estática pueden perder salida. Las rutas especiales y las políticas Multi-WAN ya no estarán disponibles, y cualquier túnel VPN utilizado para administrar remotamente el equipo se interrumpirá al reiniciarlo.

La propia transición a la interfaz predeterminada puede cambiar la IP de gestión y el nombre lógico de una interfaz. No planificar este procedimiento sin una forma fiable de acceder por consola o por la LAN física tras el reinicio.

87.15. Restauración posterior desde una copia XML

01. Localizar el archivo completo de configuración exportado antes del reset; verificar origen, integridad y compatibilidad de versión.

02. Acceder desde la LAN de recuperación y abrir Diagnostics → Backup & Restore.

03. Elegir Restore area = All para una copia completa y seleccionar el XML correcto; introducir la contraseña si el archivo está cifrado.

04. Aplicar Restore Configuration y permitir el reinicio necesario; no desconectar la energía.

05. Revisar asignación de interfaces y conectividad antes de reconectar redes productivas; reinstalar o comprobar los paquetes necesarios.

06. Validar rutas, NAT, VPN, DNS, DHCP, usuarios y accesos; guardar un nuevo respaldo cuando finalice la recuperación.

Netgate señala que una configuración completa de versión antigua puede migrarse en general a una versión nueva compatible, mientras que la restauración de una configuración más reciente a una versión anterior puede fallar. No se debe forzar un XML parcial entre versiones de configuración distintas.

87.16. Alta disponibilidad: cómo evitar un segundo incidente

Un nodo perteneciente a un clúster HA no debe restablecerse como si fuera un cortafuegos aislado. La pérdida de CARP, pfsync y XMLRPC puede introducir una segunda interrupción si el nodo vuelve a la red con interfaces predeterminadas. Documentar previamente qué nodo mantiene el servicio, reservar una ventana y mantener aislado el equipo restaurado hasta reconstruir su rol.

Después de recuperar la configuración, verificar VIP, sincronización de estados y reglas de ambos miembros. No dar por concluida la actuación solo porque la GUI responda.

87.17. Por qué Factory Reset no sirve para sanitizar un equipo

La operación no está diseñada para eliminar con garantías archivos recuperables, modificaciones del sistema, históricos, registros ni otros datos guardados fuera de la configuración. Antes de vender, ceder o retirar un equipo, seguir un proceso de borrado seguro o reinstalación sobre soporte adecuadamente tratado, acorde con la política de seguridad y el hardware específico.

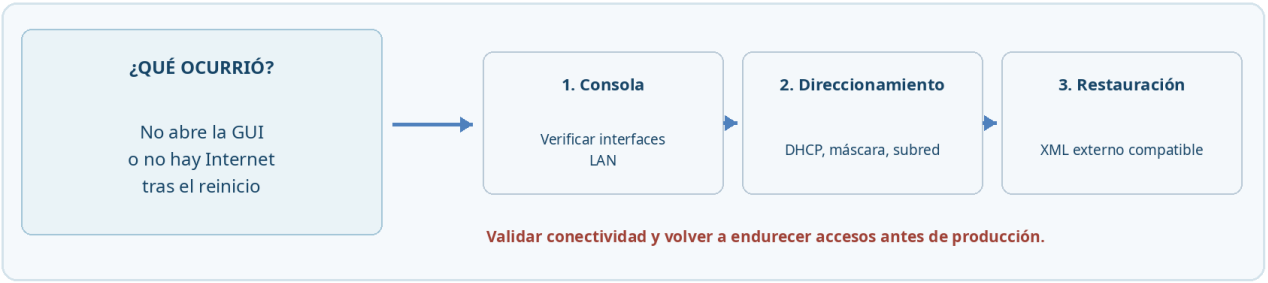


Figura 87.4. Ruta de recuperación cuando el sistema no es accesible después del reset.

87.18. Procedimiento 3: restaurar conectividad después del reinicio

01. Comprobar por consola que el sistema arranca y qué interfaces identifica como WAN y LAN.

02. Verificar conectividad física del puerto, enlace y direccionamiento de la estación de gestión.

03. Si no existe acceso, revisar si la subred por defecto se solapa con otra red y corregir las asignaciones desde consola si es necesario.

04. Acceder por HTTPS, revisar DHCP y gateway antes de restaurar configuraciones más complejas.

05. Si la configuración inicial funciona pero faltan servicios, restaurar el backup validado o reconstruir por fases.

06. Registrar la causa de la pérdida de acceso y las pruebas realizadas.

87.19. Matriz de incidencias y primera comprobación

Síntoma	Hipótesis inicial	Primera comprobación no destructiva
No responde la GUI	IP LAN distinta, VLAN/puerto equivocado o conflicto.	Consola, IP LAN y ARP del PC.
Equipo con IP pero sin Internet	WAN exige parámetros no predeterminados.	Estado WAN, gateway, DNS y proveedor.
Clientes reciben otra puerta de enlace	Servidor DHCP inicial conectado a la LAN productiva.	Aislar el puerto, comprobar oferta DHCP.
VPN desconectadas	Configuraciones y credenciales de túneles restablecidas.	Confirmar ausencia de instancias; restaurar XML.
No aparece un paquete	Retirada de paquetes durante el proceso.	Inventario previo, estado de Packages y logs.
Un fichero sigue modificado	Factory Reset no limpia todos los archivos.	Comparar con instalación limpia; no asumir borrado.
El navegador advierte del certificado	Identidad TLS inicial del firewall.	Validación controlada en LAN aislada.
Acceso remoto imposible	Cambian WAN, rutas y reglas.	Consola local; no intentar repetir reset a ciegas.

87.20. Checklist de validación posterior

Comprobación	Evidencia de aceptación
Arranque y firmware	Se identifica la versión instalada y no se observan fallos de inicio.
LAN física y administración	GUI accesible desde red de gestión aislada; contraseña cambiada.
Direccionamiento y DHCP	Servidor y rango conocidos; ausencia de ofertas a redes ajenas.
WAN y gateway	Dirección asignada y conectividad externa comprobada solo si procede.
DNS y NTP	Resolución y hora verificadas con pruebas independientes.
Firewall / NAT	Reglas esperadas confirmadas; sin exposición no prevista.
VPN, HA y servicios	Restaurados, probados y documentados antes de puesta en servicio.
Respaldo y cierre	XML exportado tras la validación y custodiado fuera del equipo.

87.21. Caso práctico: laboratorio que vuelve a configuración inicial

Situación: un equipo de pruebas ha acumulado reglas de laboratorio y túneles temporales. Se conserva un backup para auditoría y se confirma que no presta servicios críticos. Se aísla su LAN, se aplica Factory Reset, se accede por la subred inicial, se sustituye la contraseña y se reconstruye una base mínima documentada.

Criterio de éxito: los servicios configurados anteriormente ya no se presentan, la GUI es accesible de forma controlada y ningún cliente externo recibe DHCP inesperado.

87.22. Caso práctico: recuperación de una configuración defectuosa

Situación: una modificación de interfaces ha bloqueado la administración. Antes de borrar el sistema se evalúa la opción menos destructiva: consola, revisión de IP y recuperación de una revisión XML. Si se elige Factory Reset, se hace desde consola autorizada, se confirma acceso a la LAN inicial y se restaura una copia completa compatible.

Criterio de éxito: servicios y rutas vuelven a un estado conocido y las pruebas de conectividad se documentan. El reset no debe convertirse en la primera respuesta a cualquier fallo de firewall.

87.23. Caso práctico: sustitución de equipo y recuperación controlada

Situación: un firewall averiado se reemplaza por otro con pfSense Plus instalado. El trabajo no consiste solo en importar un XML: deben identificarse correspondencias de interfaces físicas, funciones del switch, plataformas de paquetes y compatibilidad de configuración. Se valida primero con un segmento aislado y posteriormente se integra en la red con cambios planificados.

Criterio de éxito: la administración, las interfaces, las rutas, el NAT, la VPN y el resto de dependencias funcionan sobre el nuevo hardware sin exponer servicios inesperados.

87.24. Seguridad, auditoría y recuperación de evidencias

La autorización de un reset debe documentar causa, fecha, responsables y plan de reversión. Conservar fuera del equipo la copia XML cifrada y los datos necesarios para reconstruir la infraestructura. Evitar que secretos, nombres internos, direcciones o rutas acaben en informes públicos, correos sin protección o medios extraíbles sin custodia.

Tras el primer inicio, cambiar credenciales, revisar usuarios y exposición de la GUI y verificar que no quedan servicios administrativos accesibles desde redes inadecuadas. Los registros pueden no sobrevivir al mismo proceso de forma recuperable; capturar evidencias imprescindibles antes de intervenir.

87.25. Preguntas frecuentes y errores de interpretación

Pregunta	Respuesta técnica
¿Es igual a reiniciar?	No: reboot conserva la configuración; Factory Reset la restablece.
¿Devuelve la versión del firmware a la original?	No es un procedimiento de downgrade ni de reinstalación.
¿Borra absolutamente toda la información?	No; no garantiza limpieza del sistema de archivos ni sanitización segura.
¿Recupera automáticamente túneles VPN?	No; requieren respaldo/restauración o reconfiguración.
¿Puedo finalizar solo con acceso remoto?	No es prudente: cambian interfaces y servicios; prever acceso de consola.
¿El botón físico de todos los modelos hace lo mismo?	No; depende del hardware y debe consultarse su manual.

87.26. Glosario técnico esencial

Término	Definición
Factory Reset	Restitución de la configuración a sus valores predeterminados.
config.xml	Archivo XML que centraliza la configuración de pfSense.
Reboot	Reinicio del sistema sin volver necesariamente a valores de fábrica.
WAN / LAN	Lado exterior e interior definidos en la configuración de interfaces.
DHCP	Servicio que asigna parámetros IP de manera automática.
Out-of-band / consola	Acceso alternativo de recuperación independiente del plano IP habitual.
HA / CARP	Mecanismos para mantener servicio mediante nodos y direcciones virtuales.
Sanitización	Eliminación controlada de datos que requiere métodos distintos al simple reset.

87.27. Acta de intervención y recuperación

Ficha recomendada para acreditar un reset autorizado y las verificaciones posteriores, sin reproducir credenciales ni topología real en documentación pública.

Hito de control	Registro mínimo exigido
Autorización	Cambio autorizado y ventana de intervención documentada.
Backup externo	Copia XML íntegra, ubicación protegida y restauración probada.
Consola alternativa	Acceso de contingencia disponible antes de la operación.
Restablecimiento	Confirmación formal y reinicio observado.
Seguridad inicial	Nueva contraseña y exposición de administración revisada.
Servicios esenciales	Conectividad LAN/WAN, DNS, DHCP, reglas y VPN validadas.
Cierre	Conformidad operativa y respaldo posterior custodio.

87.28. Referencias oficiales verificables

01. Netgate: Resetting to Factory Defaults
02. Netgate: Console Menu Basics
03. Netgate: Default Username and Password
04. Netgate: Perform the Installation — Default Configuration
05. Netgate: Backup and Recovery
06. Netgate: Making Backups in the GUI
07. Netgate: Restoring from Backups
08. Netgate: Restoring a Configuration File to a Different Version
09. Netgate: XML Configuration File
10. Netgate: Automatically Restore Configuration During Installation
11. Netgate: Hardware Factory Reset Guidance
12. Netgate: Rebooting the Firewall

CRITERIO DE ADMINISTRACIÓN Antes de restablecer: respaldo externo, autorización y consola. Después de restablecer: aislamiento, cambio de contraseña, validación de servicios y respaldo renovado.

88 Diagnostics → Halt System

Apagado ordenado · continuidad de servicio · alta disponibilidad · recuperación

Un firewall no es únicamente un equipo informático: concentra las rutas, controles y servicios de los que dependen otros sistemas. Detenerlo correctamente exige distinguir el cierre ordenado del sistema operativo, el corte de energía física y la recuperación posterior de la conectividad.

ADVERTENCIA PRIORITARIA Un apagado de un firewall único interrumpe el servicio de red. No utilizar esta función durante una sesión remota sin disponer de un método probado para recuperar el encendido y el acceso. La confirmación de la operación puede provocar la pérdida inmediata de la sesión de administración.

88.1. Finalidad técnica y ruta de acceso

Ruta exacta: Diagnostics → Halt System. La herramienta ordena detener pfSense Plus de forma controlada. Netgate documenta el botón Halt y una confirmación OK. Una vez detenido el sistema operativo, el equipo también puede apagar su alimentación si el hardware admite esa función. No se trata de un mecanismo de diagnóstico pasivo ni de una prueba de conectividad.

El objetivo es finalizar procesos y operaciones pendientes antes de una retirada de alimentación, mantenimiento físico, traslado o intervención de hardware. La pantalla específica del equipo no se ha verificado para una versión concreta: los controles descritos a continuación proceden de la documentación oficial vigente.

88.2. Controles y comportamiento de la página

Elemento verificado	Comportamiento	Precaución
Ruta Diagnostics → Halt System	Abre la función de detención del firewall.	No implica iniciar un apagado por el mero hecho de entrar.
Botón Halt	Solicita detener el sistema operativo de forma ordenada.	Operación disruptiva para la red y la administración.
Confirmación OK	Confirma y comienza el proceso de detención.	Es el punto de decisión final documentado por Netgate.
Opciones adicionales	No se documentan campos editables o modos de halt en la guía consultada.	No asumir que Halt ofrece reinicio o parada selectiva de servicios.

ALCANCE DOCUMENTAL Los nombres Halt y OK y la ruta se han contrastado con Netgate. Los elementos visuales exactos, su color y la redacción de avisos pueden diferir entre versiones y plataformas.

88.3. Secuencia técnica: qué sucede al detener el firewall

El cierre ordenado solicita al sistema operativo terminar su actividad normal: detener servicios, cerrar procesos y completar las operaciones pendientes de almacenamiento. Después, el sistema queda detenido. La secuencia concreta depende de FreeBSD, la versión de pfSense Plus, los paquetes instalados y el hardware; no se garantiza un orden idéntico para todas las instalaciones.



Figura 88.1. Secuencia conceptual desde la preparación hasta la detención final.

88.4. Halt, Reboot, Factory Defaults y corte de alimentación

Acción	Resultado	Cuándo utilizarla
Halt System	Detiene el sistema; puede apagar la alimentación según plataforma.	Mantenimiento con apagado real o retirada controlada de energía.
Reboot	Apaga servicios y vuelve a arrancar el sistema.	Aplicación de cambios que requieren reinicio o recuperación temporal.
Factory Defaults	Restablece la configuración; implica un reinicio.	Recuperación/reconfiguración planificada, no como medida rutinaria.
Corte eléctrico forzado	Interrumpe energía sin cierre ordenado.	Solo emergencia cuando no queda alternativa segura.

Netgate aconseja evitar cualquier corte de energía mientras el sistema esté ejecutándose. En unidades con almacenamiento UFS, un cierre inesperado puede exigir comprobaciones y, excepcionalmente, reparaciones del sistema de archivos; con ZFS los mecanismos de recuperación son distintos y no existe un equivalente directo de fsck.

88.5. Planificación previa a una parada en producción

Comprobación	Evidencia que debe quedar	Criterio de aceptación
Autorización y ventana	Responsable, motivo, horario y afectados.	Impacto comunicado y aprobado.
Configuración y copias	Backup XML actual, ubicación y custodia.	Restauración viable si es necesaria.
Acceso de recuperación	Consola física, serial, hipervisor o gestión OOB.	Capacidad de encendido/arranque probada.
Dependencias de red	WAN, NAT, DHCP, DNS, VPN, túneles y monitorización.	Servicios dependientes identificados.
Energía	SAI/UPS, PDU, alimentación y método de encendido.	Se conoce cómo volver a alimentar el equipo.
HA, si existe	Estado MASTER/BACKUP, pfsync, XMLRPC y pruebas.	Secundario operativo antes de tocar primario.

PREVENCIÓN Si la administración depende de la misma conexión que va a detenerse —por ejemplo, VPN remota—, no iniciar Halt sin una vía de gestión independiente. Perder la sesión web es un resultado esperable, no una confirmación de éxito.

88.6. Procedimiento 1. Apagado seguro desde la GUI

1. Revisar la autorización, comunicar la ventana y guardar una copia de configuración actual.
2. Verificar acceso local, serial, consola del hipervisor o gestión fuera de banda, y documentar el mecanismo de reencendido.
3. Entrar en Diagnostics → Halt System con una cuenta autorizada.
4. Pulsar Halt y revisar que el sistema solicita la confirmación.
5. Confirmar con OK únicamente cuando todos los servicios dependientes estén preparados.
6. Observar desde la consola el progreso hasta que finalice la detención; no interpretar la pérdida de HTTPS como señal suficiente.
7. Retirar la alimentación física únicamente cuando se haya confirmado que el apagado terminó y si el procedimiento de mantenimiento lo requiere.

88.7. Procedimiento 2. Apagado desde la consola

Netgate documenta la misma función desde el menú de consola local o accesible por SSH con una cuenta administrativa. El número de opción puede cambiar entre versiones; en los ejemplos oficiales se indica la opción 6.

1. Acceder a la consola autorizada y verificar el equipo de destino.
2. Seleccionar la opción de menú correspondiente a Halt system (habitualmente 6) y pulsar Intro.
3. Introducir y para confirmar, seguido de Intro.
4. Vigilar los mensajes finales y comprobar que el sistema ha quedado detenido.
5. Si la sesión se inició por SSH, asumir que se desconectará; preferir consola local o serial para confirmar el final del proceso.

88.7.1. Sobre comandos de shell

El menú de consola es el método recomendado para esta operación. Los comandos directos de FreeBSD pueden ser útiles en intervenciones avanzadas, pero su sintaxis, permisos y consecuencias deben verificarse antes de emplearlos; no deben sustituir la vía documentada cuando existe acceso normal a la consola.

88.8. Disponibilidad de red y dependencia de servicios

Componente	Efecto posible de Halt	Comprobación en la recuperación
Internet y NAT	Se pierde el encaminamiento por el firewall detenido.	Salida WAN, rutas, NAT y DNS.
DHCP/DHCPv6	El servidor alojado en pfSense deja de responder.	Solicitar una concesión desde un cliente de prueba.
VPN	Túneles terminan o quedan inaccesibles.	Handshake, rutas y aplicaciones de extremo a extremo.
DNS Resolver	Consultas dirigidas al firewall pueden fallar.	Resolución desde LAN y desde el propio sistema.
Multi-WAN	No aporta tolerancia si se apaga el único firewall.	Gateways y grupos, failover cuando corresponda.
Registros/telemetría	Se interrumpe la captura local y el envío de eventos.	Logs, NTP y servicios al arrancar.

88.9. Alta disponibilidad: parar un nodo no es parar la red

En un par HA validado, detener el primario puede activar la toma del rol MASTER por el secundario mediante CARP. pfsync sincroniza estados y XMLRPC sincroniza configuraciones; son mecanismos distintos. Netgate documenta pruebas de conmutación por apagado o reinicio del nodo primario, acompañadas de verificación de Internet, DHCP y VPN.



Figura 88.2. Comparación entre firewall único y par HA con respaldo verificado.

RIESGO DE FALSO RESPALDO La existencia de dos equipos no garantiza continuidad: si el secundario no dispone de interfaces, rutas, paquetes, VIP, estados o enlaces correctos, el apagado del primario puede causar una caída completa.

88.10. Procedimiento 3. Parada planificada en clúster CARP

1. Confirmar que ambos nodos muestran estados coherentes en Status → CARP y que el secundario está operativo.

2. Verificar sincronización de configuración, estados, gateways, acceso a Internet, DHCP y VPN desde el secundario.

3. Cuando el mantenimiento lo requiera, realizar previamente una conmutación controlada con CARP y observar el tráfico real.

4. Detener el nodo en mantenimiento utilizando la opción Halt y comprobar que el compañero sigue MASTER.

5. Tras el encendido, validar la recuperación de las VIP y la continuidad de las aplicaciones antes de devolver roles.

88.11. Plataformas físicas, máquinas virtuales y energía

El final de la detención del sistema operativo y el corte físico de alimentación no siempre son lo mismo. Según la plataforma, la unidad puede quedar sin alimentación, en un estado de espera o a la espera de que el operador desconecte la fuente. Netgate advierte de diferencias concretas de ACPI y hardware; no se debe concluir que un ventilador o LED encendido implica necesariamente que FreeBSD siga funcionando.

Entorno	Señal de finalización	Método de puesta en marcha
Appliance físico	Mensajes finales de consola y estado documentado de LEDs.	Alimentación o botón según manual de hardware.
VM en hipervisor	Máquina detenida en consola del hipervisor.	Iniciar máquina desde gestión del hipervisor.
Equipo con PDU/UPS	Registro de parada y salida energética controlada.	Restaurar el suministro conforme al procedimiento eléctrico.

88.12. Qué hacer cuando el equipo no se apaga físicamente

Si la consola indica que el sistema terminó, pero el dispositivo sigue consumiendo energía, diferenciar una limitación de ACPI o del diseño de la placa de una parada bloqueada. Netgate dispone de documentación para investigar problemas de apagado asociados a ACPI; determinados ajustes de sistema pueden modificar la interacción con el hardware, por lo que deben evaluarse bajo soporte técnico y en una ventana controlada.

88.13. UPS/SAI y automatización del apagado

Cuando existe un sistema de alimentación ininterrumpida, la política recomendada es detectar la pérdida prolongada de red eléctrica y ejecutar un apagado ordenado antes de agotar la batería. NUT y apcupsd están disponibles como paquetes compatibles en escenarios determinados; su instalación y compatibilidad dependen de la versión, el equipo UPS y la conexión USB, serie o de red.

La configuración de umbrales, notificaciones, orden de parada de otros equipos y recuperación de energía debe diseñarse como un procedimiento de toda la infraestructura. No asumir que instalar un paquete UPS active por sí mismo una política segura de apagado.

88.14. Recuperación y validación tras el encendido

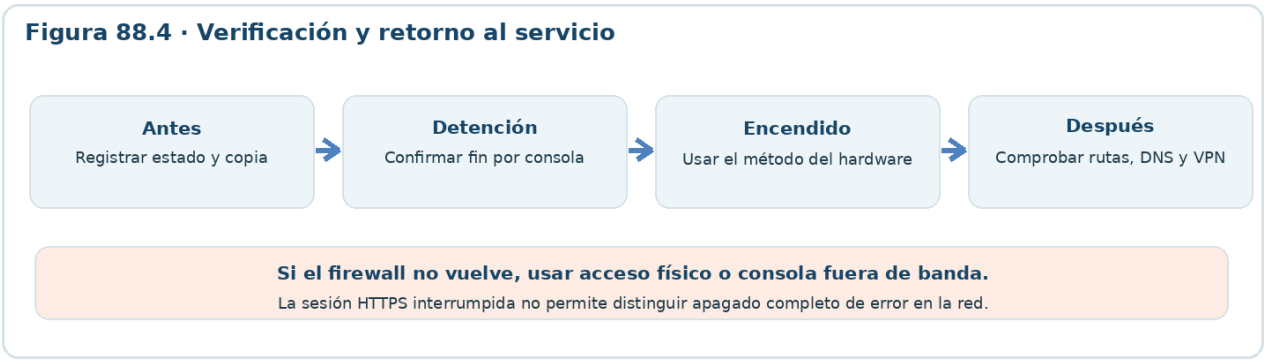


Figura 88.4. Verificación de detención, alimentación, arranque y retorno del servicio.

Fase	Comprobación objetiva	Resultado esperado
Arranque	Consola sin errores graves; interfaces asignadas.	Inicio normal de pfSense Plus.
WAN/Gateways	Gateway Online, monitor, rutas y DNS.	Salida correcta desde el firewall.
LAN/DHCP	Concesión IP, gateway, DNS y acceso administrativo.	Clientes recuperan conectividad.
VPN	Status IPsec/OpenVPN/WireGuard y pruebas.	Conexiones y rutas funcionales.
Alta disponibilidad	CARP, sincronización y roles esperados.	Sin doble MASTER ni split-brain.
Auditoría	Logs, NTP y métricas de servicio.	Evento cerrado con evidencias.

88.15. Matriz de incidencias y diagnóstico

Síntoma	Hipótesis	Actuación segura
Web dejó de responder tras confirmar	Apagado en curso o interfaz caída.	Comprobar consola y alimentación antes de intervenir.
Sistema detenido, LEDs activos	Comportamiento ACPI/hardware.	Consultar manual; verificar consola antes de retirar energía.
No vuelve tras dar corriente	Arranque requiere botón, PDU o VM Start.	Usar método documentado y consola local.
Arranca, pero sin Internet	WAN, DHCP, rutas o DNS sin restablecer.	Comprobar interfaces y gateways, luego DNS.
VPN no vuelve	Endpoint, hora, NAT, servicio o ruta.	Ver estado y logs; probar extremo a extremo.
Ambos nodos HA anuncian MASTER	CARP/segmento L2/monitores mal configurados.	No modificar a ciegas; aislar y revisar anuncios.
Error de disco al arrancar	Apagado incompleto anterior o fallo de soporte.	Seguir diagnóstico UFS/ZFS según filesystem.

88.16. Escenarios profesionales de aplicación

88.16.1. Mantenimiento físico de firewall único

Objetivo: sustituir alimentación, cableado o componente físico. La parada afecta a toda la red a través del firewall. Exigir una ventana aprobada, copia reciente, acceso local y prueba de arranque posterior.

88.16.2. Mantenimiento de un nodo en HA

Objetivo: intervenir en un nodo sin perder la salida a Internet. Antes del Halt se demuestra que el secundario mantiene la operación completa; posteriormente se valida que el nodo reintegrado no provoca oscilaciones de CARP.

88.16.3. Recuperación de fallo que exige apagado en frío

Determinados errores de firmware, controladoras o módulos requieren retirar completamente la alimentación después de un halt. En tales casos, el reinicio ordinario puede ser insuficiente; seguir las instrucciones específicas del fabricante para el ciclo de energía.

88.16.4. Apagado por autonomía insuficiente de UPS

Objetivo: preservar datos y permitir un cierre seguro antes de agotar la batería. Probar la detección de eventos y el orden de apagado de dependencias: hipervisor, switches, almacenamiento y firewall según diseño.

88.17. Comandos y fuentes de evidencia no disruptivas

Herramienta	Comprobación	Limitación
Status → Dashboard	Uptime, servicios, recursos y estado general.	Un indicador verde no sustituye pruebas reales.
Status → Gateways	RTT, pérdida y disponibilidad de salida.	Monitor Online puede no validar toda Internet.
Status → CARP	Rol MASTER/BACKUP por IP virtual.	Necesario contrastar cada VIP.
Status → System Logs	Eventos de arranque, interfaces y servicios.	La retención puede ser limitada.
Consola física/serial	Mensajes de apagado/arranque.	Requiere acceso y procedimiento probado.

88.18. Errores frecuentes y cómo evitarlos

Son prácticas peligrosas confundir Halt con Reboot; accionar el botón sin plan de reencendido; apagar remotamente por la única VPN disponible; retirar energía sin confirmar la parada; asumir que Multi-WAN sustituye una segunda unidad física; y dar por válido un failover HA solo porque CARP cambió de rol.

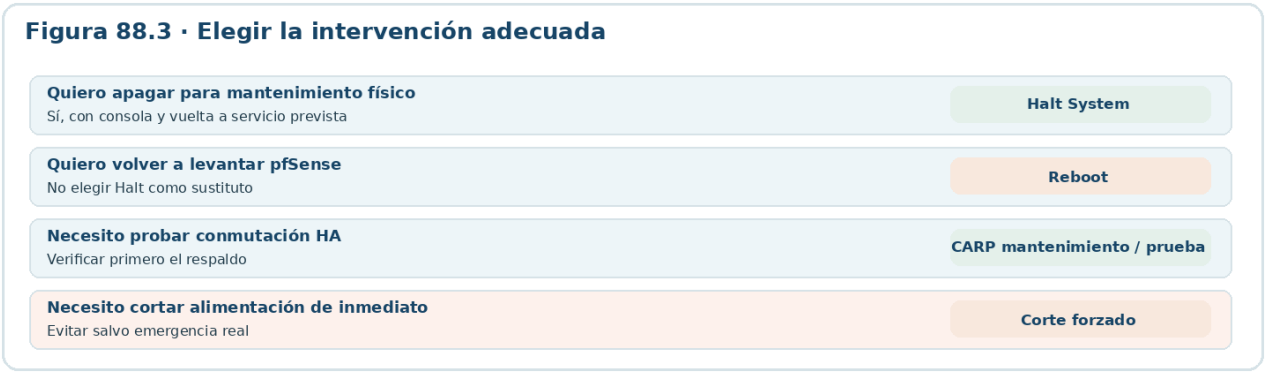


Figura 88.3. Decisión operativa: elegir Halt, Reboot, mantenimiento HA o emergencia.

88.19. Checklist de intervención y acta de cierre

Momento	Pregunta de control	Resultado
Antes	¿Tengo copia, autorización, acceso OOB y responsable de retorno?	Sí / No
Antes	¿Están identificados usuarios, VPN y servicios críticos afectados?	Sí / No
Antes	¿Está probado el respaldo HA si se promete continuidad?	Sí / No
Durante	¿He confirmado el final de halt por consola o plataforma?	Sí / No
Después	¿Vuelven WAN, DNS, DHCP, reglas, VPN y logs?	Sí / No
Cierre	¿Se registraron hora, evidencias, incidencia y resultado?	Sí / No

88.20. Glosario esencial

Término	Definición
Halt	Orden de detención del sistema operativo, sin arranque automático implícito.
Power off	Corte de alimentación física, cuando el hardware lo admite.

Término	Definición
Graceful shutdown	Finalización controlada de procesos y operaciones del sistema.
OOB	Gestión fuera de banda, independiente del tráfico de producción.
CARP	Protocolo de redundancia para direcciones IP virtuales.
pfsync	Sincronización de estados PF entre firewalls.
XMLRPC	Sincronización de configuración entre nodos de pfSense.
UPS / SAI	Alimentación ininterrumpida para gestionar interrupciones eléctricas.

88.21. Referencias oficiales verificables

[1] Netgate — Halting and Powering Off the Firewall

[2] Netgate — Console Menu Basics

[3] Netgate — Rebooting the Firewall

[4] Netgate — Troubleshooting Hardware Shutdown and Power Off

[5] Netgate — Diagnostics Menu Guide

[6] Netgate — Testing High Availability

[7] Netgate — High Availability

[8] Netgate — NUT package

[9] Netgate — Troubleshooting Disk and File System Issues

[10] Netgate — Troubleshooting Upgrades

89 Diagnostics → Limiter Info

Limitadores dummynet · supervisión de pipes y queues · QoS · diagnóstico de tráfico

Los limitadores permiten imponer topes de ancho de banda y controlar la distribución del tráfico por host, red o conjunto de conexiones. Esta pantalla muestra el estado operativo de dummynet, pero su interpretación requiere relacionar tres planos: configuración, reglas PF y tráfico realmente procesado.

SIN LIMITADORES El mensaje No limiters were found on this system indica que esta vista no encuentra limitadores. No demuestra que no exista una política ALTQ ni que la red carezca de restricciones aplicadas en otros equipos.

89.1. Finalidad técnica y ruta exacta

Ruta: Diagnostics → Limiter Info. La página presenta en texto plano la información de los limitadores activos, sus parámetros y el tráfico que atraviesa cada instancia. Cuando se utilizan máscaras, puede desglosar las entradas por IP o grupo. La administración de los limitadores se realiza en Firewall → Traffic Shaper → Limiters; esta página es un visor, no el formulario de definición.

El resultado de consulta procede del subsistema dummynet de FreeBSD integrado con PF. No debe confundirse con Status → Queues, dedicado a ALTQ. Los encabezados y métricas concretos de la salida dummynet pueden variar según versión del kernel, scheduler y presencia de tráfico; por ello no se atribuyen columnas fijas al visor.

89.2. La pantalla sin limitadores cargados

Elemento visible	Significado comprobable	Alcance / limitación
Diagnostics / Limiter Info	Identifica la ruta y la herramienta abierta.	Solo consulta de estado.
Limiter Information	Bloque donde se imprime la salida del subsistema.	Formato de texto, no tabla de edición.
Limiters:	Encabezado de la información del motor.	No implica que existan entradas.
No limiters were found on this system.	No se encontraron limitadores activos para mostrar en la consulta.	Comprobar definición, habilitación y aplicación en reglas antes de inferir causas.

Los iconos de navegación y ayuda de la cabecera pertenecen a la interfaz general. Limiter Info consulta el estado; la creación y edición de limitadores se realiza en Firewall → Traffic Shaper → Limiters.

89.3. Qué son los pipes, queues y máscaras

Un pipe representa un presupuesto de ancho de banda con una tasa máxima y, opcionalmente, retardo y pérdida artificiales. Las queues hijas reparten la capacidad del pipe mediante pesos, pero no definen una velocidad independiente. La máscara determina si se comparte un solo presupuesto global o se crean presupuestos por dirección IPv4/IPv6 o segmento.

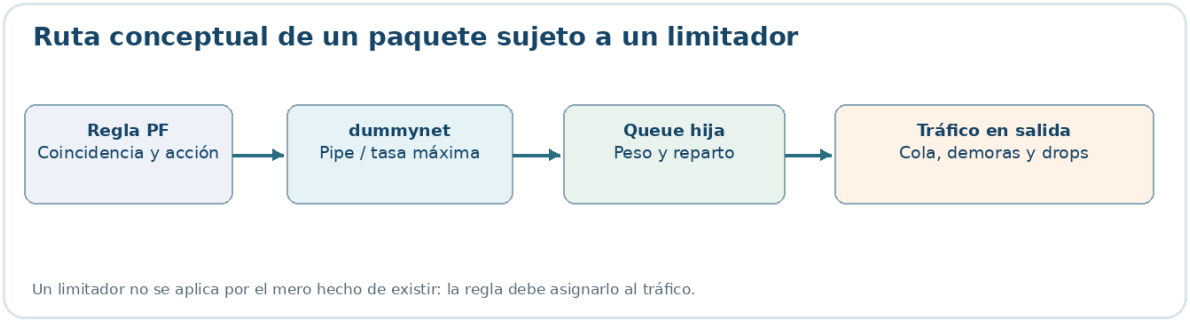


Figura 89.1. Secuencia simplificada de clasificación PF y tratamiento dummynet.

Concepto	Función técnica	Error de interpretación frecuente
Pipe (raíz)	Aplica límite máximo de tasa y, si se configura, retardo y pérdida.	Creer que reserva o garantiza un mínimo.
Queue hija	Distribuye la capacidad del pipe según scheduler y peso.	Asignarle una velocidad propia como si fuera otro pipe.
Mask	Separa instancias por host o prefijo, según bits de máscara.	Confundir un cupo individual con capacidad física ilimitada.
Scheduler / AQM	Decide el orden de salida y la gestión de colas (p. ej. FQ_CODEL).	Suponer que siempre mejora cualquier línea sin medir.
Regla PF	Relaciona tráfico coincidente con In/Out Pipe.	Crear un limitador y olvidar asociarlo a una regla.

89.4. Diferencias entre limitadores dummynet y ALTQ

Característica	Limiters (dummynet)	ALTQ
Ruta de consulta	Diagnostics → Limiter Info	Status → Queues
Control básico	Topes de ancho de banda; reparto en colas hijas.	Prioridad / reparto por colas en interfaces.
Limitación por IP/subred	Sí, mediante Mask y bits de máscara.	No ofrece el mismo modelo de cupo enmascarado por IP.
Dependencia del driver ALTQ	No exige compatibilidad ALTQ de la NIC.	Depende de los controladores admitidos.
Interfaz de administración	Firewall → Traffic Shaper → Limiters	Firewall → Traffic Shaper / Wizards
Resultado en pantalla vacía	No permite inferir el estado ALTQ.	No permite inferir el estado de dummynet.

89.5. Cómo se aplica un limitador al tráfico real

Una regla PF de paso puede seleccionar dos limitadores en Advanced Options mediante In/Out Pipe. Estos nombres se interpretan desde el punto de vista del firewall y de la interfaz donde coincide la regla. Para una regla de entrada por LAN, In suele corresponder a subida desde el cliente y Out a descarga hacia el cliente; en la WAN, los sentidos se invierten. Las reglas flotantes de salida requieren una lectura específica de dirección y gateway.

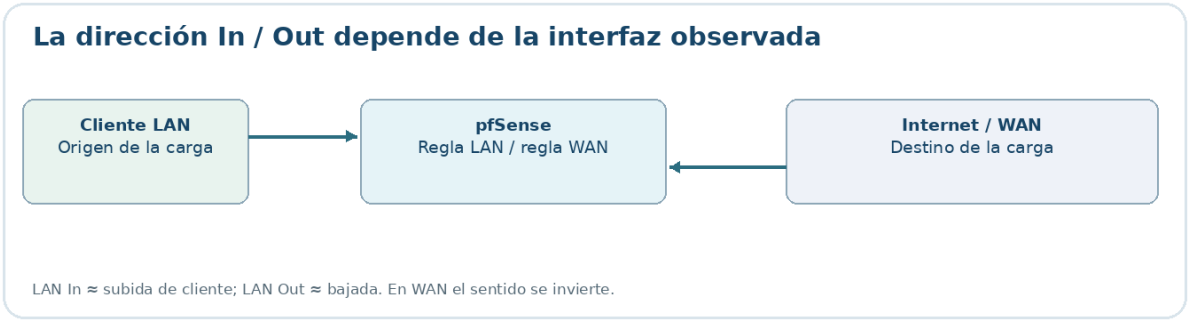


Figura 89.2. Dirección de los paquetes desde la perspectiva del firewall.

PRECAUCIÓN EN PRODUCCIÓN No cambiar pipes o reglas sobre la WAN de administración, VoIP, almacenamiento o VPN sin registrar sus valores previos y disponer de un modo de acceso alternativo. Cambiar el tratamiento de tráfico puede introducir latencia, retransmisiones o pérdida de sesiones.

89.6. Lectura de una salida dummynet con limitadores activos

La salida es texto técnico. Según el scheduler y la versión, puede mostrar identificadores de pipe o queue, ancho de banda configurado, retardos, parámetros del algoritmo, longitud o ocupación, contadores de

paquetes/bytes, descartes y flujos asociados. Los formatos internos de FreeBSD no son equivalentes a columnas normalizadas de la GUI; por eso la siguiente tabla expresa conceptos de lectura y no nombres obligatorios de campos.

Dato que puede aparecer	Cómo interpretarlo	Qué comprobar
ID de pipe / queue	Identificador del objeto cargado en dummynet.	Correspondencia con el limitador administrado.
Bandwidth / bw	Capacidad configurada, no caudal instantáneo real.	Unidades y eventual calendario.
Delay / loss	Retardo o pérdida artificial programados.	Que estén a cero salvo ensayo autorizado.
Counters / bytes / packets	Actividad acumulada observada por el objeto.	Comparar dos lecturas durante una transferencia.
Queue occupancy / drops	Presión sobre colas y descartes.	Relacionar con RTT, throughput y retransmisiones.
Buckets / flows / mask	Instancias creadas para la clave de máscara.	Saber si el límite es global o por cliente.

Los contadores pueden reiniciarse al recargar o recrear objetos y no constituyen por sí solos un histórico de facturación. Un caudal nulo en un instante no indica fallo si no hay tráfico coincidente. Los descartes ocasionales pueden formar parte de la regulación; una tasa sostenida alta debe analizarse junto a latencia, tasa efectiva y experiencia del servicio.

89.7. Máscaras IPv4 e IPv6: efecto por host o red

Mask = None aplica un único presupuesto al tráfico combinado que alcanza el pipe. Source / Destination Address permite separar presupuestos según la dirección de la regla. En un ejemplo didáctico, máscara IPv4 /32 genera cupos por dirección y /24 los agrupa por subred; para IPv6, /128 identifica una dirección individual. La aplicación real depende de las direcciones visibles tras NAT y de la dirección del paquete.



Figura 89.3. Un presupuesto compartido frente a instancias enmascaradas.

Ejemplo de laboratorio: un pipe de 8 Mbit/s sin máscara limita a 8 Mbit/s el conjunto de dispositivos que coinciden con su regla. Con máscara por host, cada dirección obtiene un tope nominal de 8 Mbit/s, pero todos continúan compartiendo la capacidad física disponible del enlace. No es una reserva de 8 Mbit/s para cada host.

89.8. Parámetros de configuración que explican la salida

Parámetro de Limiters	Uso y efecto	Implicación de diagnóstico
Enable / Name	Habilita el objeto y le asigna nombre para reglas.	Un objeto deshabilitado no está disponible para reglas.
Bandwidth / Bw Type	Fija magnitud y unidades del pipe.	Diferenciar Kbit/s, Mbit/s y velocidad real.
Schedule	Puede variar la tasa por tramo horario.	Comparar hora de la prueba y calendario activo.

Parámetro de Limiters	Uso y efecto	Implicación de diagnóstico
Mask / Mask Bits	Decide agrupación por IP o prefijo.	Revisar Source vs Destination tras NAT.
Delay / Packet loss rate	Añade degradación artificial; normalmente vacío.	Útil en laboratorio, peligroso en producción.
Weight (queue)	Reparto relativo entre queues hijas.	No equivale a prioridad estricta ni tasa fija.
Queue Size / Bucket Size	Capacidad de espera / estructura de hashes.	Excesos pueden aumentar memoria y latencia.
Scheduler / Queue Management	FQ_CODEL, CoDel, Tail Drop u otros, según versión.	Comparar jitter y latencia en carga.

89.9. Procedimiento 1. Validar un entorno sin limitadores activos

1. Abrir Diagnostics → Limiter Info y conservar evidencia del texto «No limiters were found on this system».
2. Consultar Firewall → Traffic Shaper → Limiters: verificar si existen objetos, si están habilitados y sus nombres.
3. Revisar las reglas PF del flujo estudiado; abrir las opciones avanzadas y comprobar In Pipe y Out Pipe, incluidas las reglas flotantes.
4. Comprobar que se está generando tráfico del origen, destino, protocolo y dirección que deben coincidir con la regla.
5. Si existe configuración que debería actuar, revisar avisos de aplicación y registros; no asumir que una recarga del filtro es la primera medida.
6. Registrar el resultado: «sin definir», «definido pero deshabilitado», «sin asociar a regla» o «requiere diagnóstico de carga», según evidencias.

89.10. Procedimiento 2. Ensayo de un límite de ancho de banda

1. Medir la capacidad de la conexión y establecer una línea base de RTT, pérdida y caudal en una ventana de prueba.
2. Crear un pipe de prueba en Firewall → Traffic Shaper → Limiters con nombre neutro y una tasa inferior a la capacidad disponible; guardar y aplicar.
3. Asignarlo a una regla de paso dedicada a un equipo o red de laboratorio y confirmar el sentido de In/Out Pipe.
4. Iniciar tráfico medible desde el cliente y volver a Diagnostics → Limiter Info para comparar el estado y los contadores.
5. Verificar si el caudal se aproxima al techo configurado y si aumentan la cola, la latencia o los descartes.
6. Retirar la regla temporal y el objeto de prueba, y verificar que el rendimiento retorna a la línea base.

IMPORTANTE Las reglas o limitadores aplicados a sesiones ya establecidas pueden no afectar al tráfico existente hasta que se creen nuevos estados. Reiniciar la tabla completa de estados puede interrumpir conexiones: preferir sesiones nuevas o eliminación selectiva autorizada.

89.11. Procedimiento 3. Control por cliente o grupo de red

1. Determinar si el objetivo es un techo agregado o un límite por host; no son equivalentes.
2. Seleccionar la máscara IPv4 o IPv6 adecuada y la dirección Source/Destination según interfaz y NAT.
3. Aplicar a una regla limitada en alcance y comparar al menos dos dispositivos con tráfico simultáneo.
4. Comprobar que aparecen los desgloses de flujo enmascarado y que ninguno supera su tope salvo tolerancias de medición.
5. Verificar que la suma de caudales no satura el enlace externo y documentar los resultados.

89.12. Procedimiento 4. Multi-WAN y alta disponibilidad

Netgate requiere especial cuidado con Multi-WAN: los limitadores asociados a gateways no predeterminados suelen necesitar reglas flotantes de salida con el gateway correcto. Cada WAN puede necesitar su propia pareja de objetos, con capacidad adaptada a su enlace. Las reglas excesivamente amplias pueden capturar tráfico del enlace equivocado. En HA, verificar la sincronización de configuración y realizar la prueba desde cada nodo cuando proceda.

1. Inventariar capacidades de cada WAN y definir un plan separado para cada enlace.
2. Configurar reglas por interfaz y gateway con criterios de origen acotados, evitando solapamiento entre WAN.
3. Forzar una conexión nueva de prueba para cada ruta y comprobar en Limiter Info el pipe que se utiliza.
4. Validar una conmutación de enlace controlada y medir RTT, pérdida y ancho de banda después del cambio.
5. Restaurar el estado habitual de gateways y conservar el plan de reversión.

89.13. Procedimiento 5. Diagnóstico de bufferbloat

Bufferbloat es la elevación notable de latencia durante saturación por acumulación de paquetes en colas. Netgate documenta FQ_CODEL en limitadores para mitigarlo, pero exige medir antes y después, configurar ambos sentidos y ajustar las tasas a la capacidad real. La receta oficial incluye colas hijas y reglas flotantes; no se debe copiar sin adaptar a la topología.

1. Registrar RTT en reposo y bajo carga, además de la velocidad útil.
2. Verificar si el cuello de botella se encuentra realmente en el enlace a controlar.
3. Configurar una pareja de limitadores y colas de laboratorio siguiendo la receta de Netgate y adaptando los valores.
4. Observar en Limiter Info las colas y los cambios de contadores mientras se repite el ensayo.
5. Conservar solo la configuración que mejore la latencia bajo carga sin causar pérdidas ni degradación inaceptable de caudal.

89.14. Diagnóstico sistemático y correlación de evidencias

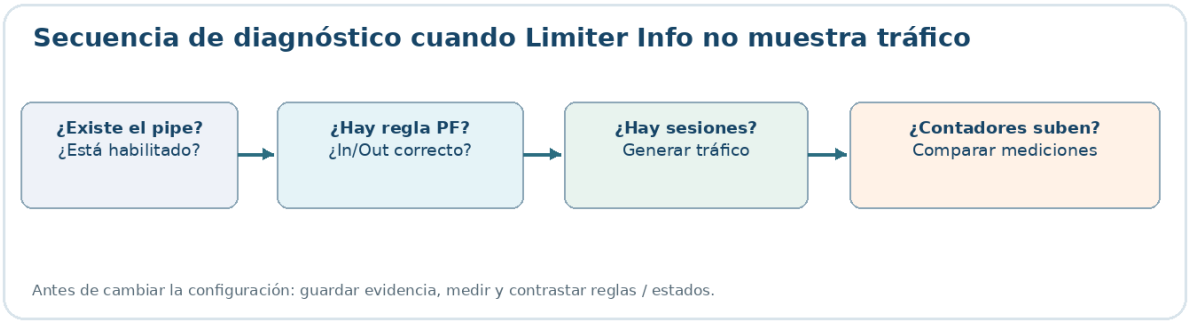


Figura 89.4. Árbol de comprobación de existencia, reglas y tráfico.

Síntoma	Causas probables	Prueba segura / corrección
No limiters were found	No hay objetos cargados, están deshabilitados o falta aplicación.	Revisar Limiters, reglas y mensajes de aplicación.
Aparece pipe sin tráfico	No coincide la regla, dirección o flujo; no hay sesiones.	Generar conexión nueva y comprobar reglas/estados.
Límite aplicado al sentido contrario	In/Out Pipe invertidos, regla en otra interfaz.	Trazar el sentido de la conexión LAN / WAN.
Un equipo consume todo el cupo	Mask None cuando se pretendía por-IP.	Probar máscara y agrupar flujos correctamente.
Latencia elevada en carga	Queue Size, tasa demasiado alta o congestión aguas arriba.	Comparar latencia/reposo, ocupación y tasa efectiva.

Síntoma	Causas probables	Prueba segura / corrección
Algunas aplicaciones no pasan	Reglas flotantes, policy routing, túneles o estados antiguos.	Comprobar NAT, reglas y tráfico por interfaz.
Problemas tras failover	Pipe aplicado a otra WAN o capacidad del respaldo distinta.	Revisar reglas por gateway y nuevas sesiones.

89.15. Comandos complementarios de solo lectura

La pantalla gráfica es el procedimiento preferente. Cuando se necesite inspección avanzada y se disponga de autorización, la utilidad FreeBSD dnctl puede listar objetos dummynet. En pfSense Plus la disponibilidad y sintaxis exactas dependen de la versión; validar la ayuda instalada antes de ejecutar comandos. Evitar opciones de eliminación, flush o modificación fuera de una intervención controlada.

Consulta conceptual	Finalidad	Cautela
dnctl pipe show	Inspeccionar pipes cargados si la utilidad está presente.	Solo lectura; formato dependiente de versión.
dnctl queue show	Consultar queues de dummynet.	No asumir nombres o contadores constantes.
pfctl -sr	Inspeccionar reglas de filtro; puede ayudar a localizar criterios.	Los detalles internos generados pueden variar.
Status → Monitoring	Comparar CPU e interfaces a lo largo del tiempo.	No sustituye la prueba de un flujo concreto.
Diagnostics → pfTop / States	Ver las conexiones y sus estados.	No confundir bytes de conexión con bytes de pipe.

89.16. Escenarios empresariales de uso

Escenario	Objetivo	Validación
Wi-Fi de invitados	Evitar que una red no crítica sature un enlace.	Caudal de invitados y continuidad de aplicaciones corporativas.
Enlace de contingencia 4G	Reducir el consumo cuando se conmuta a una WAN limitada.	Regla ligada al gateway de respaldo; tráfico acotado.
Teletrabajo con VPN	Controlar el consumo agregado de un segmento de túnel.	Verificar interfaz, NAT, cifrado y rutas del túnel.
Telefonía y videoconferencia	Mitigar latencia alta durante transferencias.	Jitter, pérdidas, audio real y RTT bajo carga.
Servicios de laboratorio	Simular retardo o pérdidas mediante dummynet.	Resultados reproducibles y retirada de degradación.

89.17. Seguridad, capacidad y recomendaciones operativas

El uso de dummynet consume recursos adicionales de procesamiento y buffers. Un Queue Size excesivo puede aumentar la latencia; uno demasiado pequeño puede causar descartes. Los pipes imponen techos y no garantizan reserva de caudal mínimo. Ajustar los valores con pruebas reales y registrar la configuración previa para evitar errores al retocar políticas de servicio.

Restringir la administración a perfiles autorizados y separar la cuenta operativa de la observación. Conservar evidencia de modificaciones, horarios, versión, interfaz, reglas afectadas y pruebas de aceptación. En entornos Multi-WAN, validar también el camino de retorno y la variación de capacidad del enlace secundario.

RIESGO DE INTERRUPCIÓN No ejecutar limpieza global de estados, cambios masivos de reglas o modificaciones de pipes en horas críticas sin plan de marcha atrás: puede afectar VPN, VoIP, ERP, acceso remoto o servicios publicados.

89.18. Ficha de verificación posterior a la intervención

Prueba	Resultado esperado	Registro de evidencia
La página Limiter Info carga	Salida visible o mensaje coherente con la configuración.	Fecha, versión y pantalla anonimizada.
Regla PF relevante	Correcta interfaz, protocolo, acción y pipes.	ID funcional de regla, sin direcciones reales.
Tráfico de prueba	Aumento de contadores durante conexiones nuevas.	Valores antes/después y duración.
Calidad de servicio	Tasa y RTT compatibles con el objetivo pactado.	Muestras medibles en reposo y bajo carga.
Multi-WAN	Política separada para cada gateway cuando aplica.	Conmutación y validación de retorno.
Reversión	Posibilidad de volver a baseline documentado.	Confirmación tras deshacer la prueba.

89.19. Glosario esencial

Término	Definición
dummynet	Mecanismo de FreeBSD para colas, limitación de tasa y emulación de red.
Pipe	Objeto raíz que impone un techo de ancho de banda.
Queue	Objeto de reparto de capacidad y peso en el pipe.
Mask	Agrupación de flujos por IP o prefijo.
FQ_CODEL	Algoritmo de planificación de flujos y control de retardo en cola.
Bufferbloat	Incremento de latencia por colas excesivas durante congestión.
ALTQ	Otra familia de tráfico conformado, diferente de dummynet.
Policy routing	Selección de gateway mediante reglas para un flujo concreto.

89.20. Referencias oficiales y documentación técnica

[1] Netgate · Diagnostics — Menú y función Limiter Info
[2] Netgate · Limiters — definición, parámetros y consulta
[3] Netgate · Traffic Shaper — ALTQ y limitadores
[4] Netgate · Configuring CoDel Limiters for Bufferbloat
[5] Netgate · Hardware Limitations — compatibilidad ALTQ
[6] Netgate · Troubleshooting Traffic Shaping
[7] Netgate · Troubleshooting Low Interface Throughput
[8] Netgate · ALTQ Traffic Shaper Queue Monitoring
[9] FreeBSD Manual · dnctl(8) — administración dummynet
[10] Netgate · pfSense Plus 25.11, corrección Multi-WAN/limiters

Nota de versión. Los conceptos se han contrastado con la documentación pública de Netgate vigente en noviembre de 2026. La disponibilidad y presentación de ciertos contadores puede variar según la versión exacta de pfSense Plus y de FreeBSD; no se presupone una edición concreta a partir de una sola pantalla.

90 Diagnostics → NDP Table

Vecinos IPv6 · ICMPv6 · caché NDP · diagnóstico de conectividad

La tabla de Neighbor Discovery permite inspeccionar las correspondencias entre direcciones IPv6 y direcciones de enlace conocidas por el firewall. Es esencial para determinar si un problema de conectividad se produce antes del enrutamiento, durante la resolución de vecinos o en capas superiores.

CRITERIO DE LECTURA Una entrada NDP no equivale a un dispositivo permanentemente conectado y una tabla vacía no prueba que no existan dispositivos IPv6. La página representa la visión local del firewall en un momento concreto.

90.1. Finalidad técnica, alcance y ubicación

Ruta exacta: Diagnostics → NDP Table. Esta vista es de diagnóstico y administración de la caché de vecinos IPv6 del sistema operativo. Permite buscar entradas conocidas, observar su tiempo de expiración y retirar entradas individuales o vaciar la tabla. No es un inventario de dispositivos, un servidor DHCPv6 ni un escáner de red.

Su valor principal es correlacionar dirección IPv6, MAC y segmento de red. El vecino debe estar en un enlace directamente conectado o ser el siguiente salto de una ruta. Una máquina de una red remota no tiene por qué figurar: normalmente aparecerá el router vecino que permite alcanzarla.

90.2. Fundamentos: Neighbor Discovery Protocol

NDP, definido en RFC 4861, sustituye en IPv6 la función de descubrimiento de vecinos que ARP realiza en IPv4. Funciona mediante mensajes ICMPv6, no mediante peticiones ARP ni puertos TCP/UDP. Además participa en descubrimiento de routers, detección de inalcanzabilidad y redirecciones de enrutamiento.

Tipo ICMPv6	Mensaje	Función
133 · RS	Router Solicitation	Un host solicita anuncios de router para conocer parámetros de red.
134 · RA	Router Advertisement	El router anuncia prefijos, routers y opciones; interviene en SLAAC.
135 · NS	Neighbor Solicitation	Busca la dirección MAC de un vecino, verifica alcance o participa en DAD.
136 · NA	Neighbor Advertisement	Aporta información del vecino y puede confirmar la correspondencia IPv6–MAC.
137 · Redirect	Redirect	Informa de un siguiente salto alternativo en las condiciones previstas por IPv6.



Figura 90.1. Intercambio básico de descubrimiento en el segmento local.

90.3. Acceso a la pantalla y zona Search

La página presenta Search y NDP Table. El icono de ayuda abre la documentación contextual. El botón con signo menos minimiza el bloque Search; no borra datos ni desactiva NDP.

Control	Comportamiento	Interpretación y precaución
Search Term	Introduce una cadena o expresión regular de estilo *nix para filtrar filas.	Permite buscar IPv6, MAC, hostname o contenido que la página admita; no debe interpretarse como consulta DNS activa.
Selector All	Restringe el ámbito del filtrado; All abarca las categorías disponibles.	No se enumeran otras opciones del desplegable porque no aparecen abiertas en la pantalla.
Search	Ejecuta el filtrado solicitado.	Una búsqueda sin resultados no vacía la caché y no prueba ausencia del host.
Clear	Limpia el criterio de búsqueda y restablece la presentación del listado.	No debe confundirse con Clear NDP Table.
Icono «−»	Oculta o pliega los controles del área Search.	Cambio visual, sin efectos sobre vecinos registrados.

90.4. Lectura de las seis columnas de NDP Table

Columna	Qué representa	Claves de interpretación
IPv6 Address	Dirección IPv6 del vecino o dirección local de interfaz.	Con fe80:: puede incluir %interfaz para identificar su ámbito.
MAC Address	Identificador de enlace registrado para el vecino.	(Incomplete) significa que aún no llegó respuesta válida de descubrimiento.
Hostname	Nombre hallado por resolución inversa, cuando está disponible.	Su ausencia no invalida la entrada; DNS puede faltar o no coincidir.
Interface	Interfaz asignada o nombre de dispositivo del sistema.	Es fundamental en VLAN, puertos físicos y direcciones link-local.
Expiration	Temporizador de vida o condición permanent.	La cuenta atrás no equivale a tiempo encendido ni a una sesión activa.
Actions	Icono de papelera por entrada.	Solicita la eliminación puntual de ese registro, con confirmación.

La información procede de la caché de vecinos y del contexto del sistema operativo; el nombre de host es auxiliar. No se debe inferir fabricante o identidad de usuario únicamente a partir de una dirección MAC, ya que las máquinas virtuales y los mecanismos de privacidad pueden modificarla.

90.5. Ámbito link-local y notación %interfaz

Las direcciones IPv6 link-local pertenecen a fe80::/10 y se utilizan en un mismo enlace. El sufijo de zona, como %vlan10 en un ejemplo ficticio, identifica la interfaz por la que se alcanza esa dirección. Dos interfaces diferentes pueden tener vecinos con texto IPv6 idéntico pero ámbitos distintos: omitir el scope produce diagnósticos ambiguos.

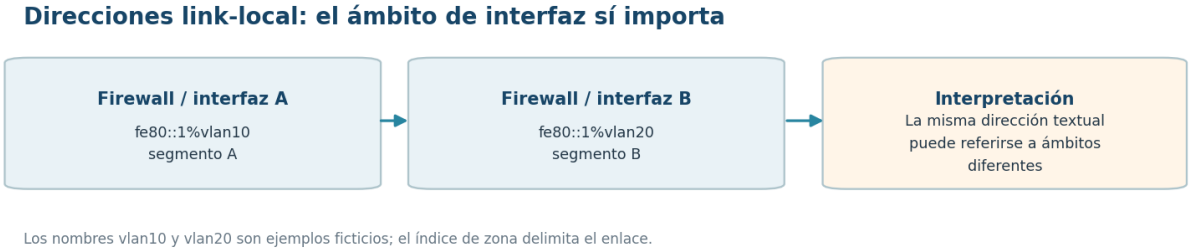


Figura 90.3. El índice de zona separa ámbitos locales distintos.

PRECAUCIÓN No copiar direcciones link-local sin su índice de zona al ejecutar pruebas desde el propio firewall. En cambio, las direcciones globales normalmente no necesitan esta especificación de interfaz.

90.6. Expiration, permanent e incomplete

Presentación	Interpretación correcta	Qué NO implica
Tiempo restante	Entrada dinámica que puede caducar si no se renueva su actividad o confirmación.	No equivale al lease DHCPv6 ni a disponibilidad garantizada.
permanent	Entrada local de interfaz/VIP o entrada NDP estática del sistema.	No significa que un host remoto sea permanentemente accesible.
(Incomplete)	El sistema inició la resolución, pero no recibió aún una respuesta válida.	No identifica por sí solo una causa única; puede ser VLAN, equipo apagado, filtrado o pérdida.

Netgate utiliza el término “Expiration” en esta página para diferenciar entradas permanentes y dinámicas. Los estados técnicos internos del algoritmo de RFC 4861 son otra cosa; no deben confundirse con la etiqueta de expiración mostrada en la GUI.

90.7. Estados técnicos de Neighbor Unreachability Detection

El algoritmo NUD mantiene estados conceptuales INCOMPLETE, REACHABLE, STALE, DELAY y PROBE. La caché puede pasar de una entrada confirmada a otra pendiente de comprobación cuando deja de existir prueba reciente de alcance, sin que ello implique pérdida definitiva de conectividad.

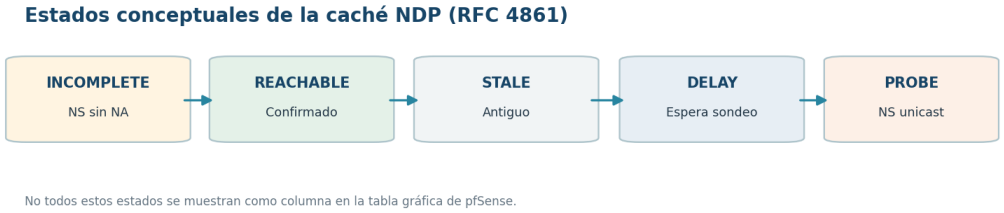


Figura 90.2. Vista simplificada de la máquina de estados NUD.

Estado	Acción esperada en términos de diagnóstico
INCOMPLETE	Esperar NA o comprobar que NS llega al segmento; verificar la pertenencia a VLAN y el enlace físico.
REACHABLE	Recientemente se confirmó el camino hacia el vecino; no garantiza disponibilidad de aplicaciones.
STALE	La entrada existe, pero no tiene confirmación reciente; puede verificarse al generar tráfico.
DELAY	Se aplaza brevemente el sondeo activo por si capas superiores confirman conectividad.
PROBE	Se envían solicitudes unicast para volver a confirmar el vecino antes de declarar fallo.

90.8. Acciones sobre entradas individuales

La papelera de la columna Actions retira una asociación concreta de la caché. Netgate documenta que se solicita confirmación antes de eliminarla. Su propósito es permitir que, cuando un host cambia de MAC, el firewall vuelva a descubrir la correspondencia durante el siguiente tráfico pertinente.

El borrado no modifica la dirección IPv6 del equipo, sus concesiones DHCPv6, sus anuncios RA ni las reglas PF. Puede ocasionar una interrupción breve si el firewall debe esperar un nuevo intercambio NS/NA. Una entrada local o estática puede ser regenerada según el estado del sistema y su configuración.

90.9. Acción global: Clear NDP Table

El botón rojo Clear NDP Table purga todas las entradas de la caché, no solo las visibles tras aplicar Search. Es una acción excepcional, apropiada únicamente cuando se sospechan múltiples asociaciones obsoletas o existe una indicación operativa clara. La recuperación depende de que el tráfico pueda volver a generar descubrimiento de vecinos.

ALTO IMPACTO Evitar el vaciado global desde una sesión remota que depende de la misma interfaz y del mismo tráfico IPv6, especialmente sobre enlaces críticos. Registrar primero las asociaciones y disponer de acceso alternativo o consola.

90.10. Relación con ARP Table y otras pantallas de pfSense

Herramienta	Objeto principal	Cuándo compararla
Diagnostics → ARP Table	Relaciones IPv4–MAC.	Si un problema afecta solo a IPv4 o a un host de doble pila.
Diagnostics → NDP Table	Vecinos IPv6–MAC.	Si falla conectividad IPv6 en un enlace directo.
Status → DHCPv6 Leases	Direcciones/prefijos otorgados por DHCPv6.	Si se investiga la concesión, identidad DUID o expiración del préstamo.
Services → Router Advertisement	Mensajes RA y parámetros de autoconfiguración.	Si un equipo carece de ruta por defecto o prefijo SLAAC esperado.
Diagnostics → Routes	Rutas y siguientes saltos.	Si la red destino está fuera del enlace local.
Diagnostics → Packet Capture	Tráfico real ICMPv6 recibido/transmitido.	Si la entrada no se resuelve o aparece una MAC inesperada.

90.11. Procedimiento 1. Lectura de la caché sin alterar el servicio

1. Abrir Diagnostics → NDP Table y registrar hora, interfaz y tipo de dirección, sin copiar datos personales a informes públicos.
2. Aplicar Search por una dirección concreta y seleccionar el alcance necesario; si no aparece, eliminar el filtro para evitar falsos negativos.
3. Comparar IPv6, MAC e interfaz con las rutas y con el estado de enlace; determinar si se trata de vecino directo o siguiente salto.
4. Consultar Expiration y, si procede, registrar si una entrada es dinámica, local o incompleta.
5. Generar una prueba puntual desde la interfaz adecuada y revisar si se crea o actualiza la entrada.

90.12. Procedimiento 2. Investigar una entrada (Incomplete)

1. Confirmar que el destino pertenece realmente al segmento o que el siguiente salto esperado es el vecino consultado.
2. En IPv6 link-local, repetir la prueba especificando el índice de zona de la interfaz correspondiente.
3. Revisar estado físico, VLAN y pertenencia del puerto al dominio de enlace correcto.
4. Capturar ICMPv6 NS/NA en Diagnostics → Packet Capture; observar si se transmite NS y si vuelve NA.
5. Si no llega NA, comprobar host, adaptador, controles de red, aislamiento Wi-Fi o reglas de seguridad de capa 2.
6. No borrar toda la caché: una entrada incompleta suele requerir corregir causa, no limpiar indiscriminadamente.

90.13. Procedimiento 3. Resolver un cambio de MAC

1. Identificar una dirección IPv6 y la MAC que muestra la caché; contrastar con el equipo esperado por un canal fiable.
2. Confirmar que hubo sustitución de equipo, movimiento de VM o cambio autorizado de adaptador.
3. Guardar evidencia mínima y seleccionar solamente la papelera de la entrada afectada.
4. Confirmar la acción, generar tráfico hacia el vecino y verificar que aparece la nueva MAC.
5. Si la asociación vuelve a ser incorrecta, revisar duplicidad, proxy NDP o anuncios de vecino no legítimos.

90.14. Procedimiento 4. Diagnosticar fallo en una VLAN IPv6

1. Correlacionar interfaz física, VLAN y interfaz asignada en Status → Interfaces.
2. Examinar Router Advertisements y dirección link-local del gateway esperada en ese enlace.
3. Buscar el host en NDP y confirmar que su interfaz coincide con la VLAN de acceso.
4. Comparar tabla de rutas y gateway IPv6; una ruta ausente no se resuelve limpiando NDP.
5. Efectuar una captura dirigida de ICMPv6 antes de modificar reglas o etiquetas de VLAN.
6. Aplicar la corrección mínima y repetir conectividad de vecino y de aplicación por separado.

90.15. Procedimiento 5. Captura de Neighbor Discovery

Seleccionar en Diagnostics → Packet Capture la interfaz de recepción esperada. En versiones que ofrecen el selector, filtrar por protocolo ICMP6; con filtros personalizados se puede emplear un filtro BPF equivalente. Limitar duración y volumen para proteger la disponibilidad del equipo.

Mensaje	Filtro/identificación	Lectura esperada
NS	ICMPv6 type 135	El firewall pregunta por la MAC correspondiente a una IPv6.
NA	ICMPv6 type 136	El dispositivo responde; examinar si hay dirección de enlace y en qué interfaz.
RA	ICMPv6 type 134	Si el fallo es de prefijo o router, comprobar anuncios.
RS	ICMPv6 type 133	El cliente intenta descubrir routers en el enlace.
DAD	NS con origen ::	Sondeo de unicidad previo a la asignación; no confundir con NS normal.

90.16. Comandos de solo lectura y eliminación puntual

En la consola del sistema subyacente, el comando FreeBSD ndp permite consultar la caché. Su sintaxis concreta puede depender del release; el siguiente conjunto es de referencia y no obliga a modificar configuración persistente.

Comando	Resultado	Impacto
ndp -an	Muestra vecinos con direcciones numéricas.	Solo lectura.
ndp -a	Muestra las asociaciones IPv6/MAC conocidas.	Solo lectura.
ndp -d <IPv6>	Elimina una entrada concreta; añadir zona si el destino lo requiere.	Modifica temporalmente la caché.
ndp -c	Vacía entradas de Neighbor Discovery.	Disruptivo: evitar en producción sin plan previo.
tcpdump -ni <if> icmp6	Muestra ICMPv6 en una interfaz indicada.	Captura: limitar duración; puede mostrar identificadores.

PRÁCTICA SEGURA Sustituir los marcadores <IPv6> y <if> por valores conocidos del propio equipo solo al ejecutar pruebas autorizadas; no pegar una línea con marcadores literalmente. Priorizar la GUI para las operaciones ordinarias.

90.17. Procedimiento 6. Borrado completo con control de cambios

1. Documentar la incidencia concreta y justificar por qué el borrado selectivo no basta.
2. Comprobar acceso alternativo (consola o canal de gestión) y ventana de mantenimiento.
3. Anotar las asociaciones pertinentes y activar una comprobación de disponibilidad en el segmento.
4. Accionar Clear NDP Table y confirmar, evitando ejecuciones repetidas sin nueva evidencia.

5. Generar tráfico de prueba para reconstruir vecinos, revisar la tabla y verificar rutas, DNS y servicios esenciales.
6. Cerrar la intervención con hora, resultado y acciones de reversión; no atribuir al vaciado la solución si no se ha diagnosticado la causa.

90.18. Escenarios empresariales habituales

Situación	Señal	Prueba prioritaria
Sustitución de una máquina virtual	IPv6 conocida con MAC antigua o fluctuante.	Comprobar MAC actual y borrar únicamente esa entrada.
Cliente Wi-Fi aislado	(Incomplete) al intentar alcanzar el host.	Verificar aislamiento de clientes, VLAN y captura NS/NA.
Nueva VLAN sin IPv6 funcional	Ausencia de vecinos y rutas esperadas.	Revisar interfaz, RA, filtrado ICMPv6 y trunk del switch.
Router de borde con fallos intermitentes	Vecino siguiente salto con confirmaciones irregulares.	Combinar NDP, pings y monitorización de enlace.
Equipo con direcciones temporales IPv6	Varias IPv6 distintas relacionadas con un mismo adaptador.	No inferir error ni duplicidad sin validar políticas de privacidad.

90.19. Riesgos de seguridad y privacidad

NDP está expuesto a suplantación de anuncios de vecino y de router si la red local no dispone de controles apropiados. La confianza en una asociación IPv6–MAC no debe sustituir mecanismos de identidad de usuario, inventario ni autenticación de red. En segmentos gestionados pueden aplicarse controles de primer salto compatibles con el switch (p. ej., RA Guard), revisando cuidadosamente su interoperabilidad.

Las direcciones IPv6 temporales, la aleatorización de MAC y la virtualización pueden producir múltiples entradas para un mismo dispositivo o identidad. Por ello se recomienda almacenar las evidencias mínimas necesarias, restringir el acceso al registro de vecinos y aplicar políticas de retención coherentes.

90.20. Matriz de resolución de incidencias

Síntoma	Hipótesis principal	Verificación antes de actuar
No se ve un dispositivo	No ha generado tráfico hacia/desde pfSense.	Probar conectividad, ruta y segmento; no declarar ausencia.
(Incomplete) persistente	NS sin NA válido.	Captura de ICMPv6; VLAN y estado del host.
MAC distinta a la esperada	Movimiento, reemplazo o posible suplantación.	Comprobar origen por switch y registros autorizados.
La tabla se repuebla tras borrarla	Actividad IPv6 normal del segmento.	Esperado; no es prueba de ataque.
Ping link-local falla	Índice de zona incorrecto.	Precisar interfaz de origen y scope.
IPv6 local funciona pero no Internet	Problema de ruta, RA, DNS o filtrado.	Mirar Routes, interfaces, gateway y Packet Capture.
Entrada permanent no cambia	Interfaz local, VIP o entrada estática.	Revisar configuración del sistema; no forzar borrados.

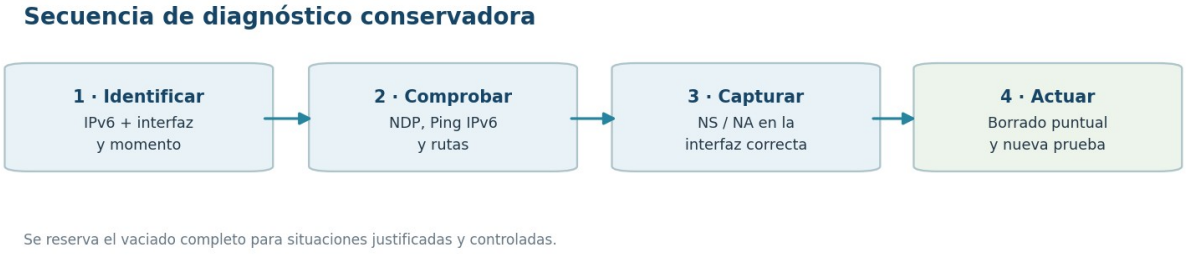


Figura 90.4. Método de mínimo impacto para trabajar con NDP.

90.21. Diferencias con DHCPv6, SLAAC y tabla de rutas

NDP descubre vecinos y participa en la detección de alcance. SLAAC utiliza RA para configurar direcciones; DHCPv6 puede asignar direcciones o delegar prefijos, pero no sustituye la necesidad de descubrimiento de vecinos de capa local. La tabla de rutas decide hacia dónde encaminar paquetes destinados a redes remotas. Un fallo en cualquiera de estas etapas produce síntomas diferentes.

90.22. Buenas prácticas de administración

1. Filtrar por IPv6 e interfaz para trabajar con un vecino específico.
2. Distinguir claramente dirección link-local, dirección global y scope de interfaz.
3. Correlacionar NDP con rutas, RA, DHCPv6, DNS y capturas sin inferir conclusiones solo a partir de una vista.
4. Evitar borrados masivos durante tareas de acceso remoto, especialmente en entornos críticos.
5. Conservar un procedimiento de reversión antes de modificar VLAN o reglas de ICMPv6.
6. Anonimizar direcciones, MAC, nombres e identificadores antes de enviar evidencias a terceros.

90.23. Ficha operativa de comprobación

Dato a registrar	Ejemplo de anotación segura
Interfaz de prueba	Segmento de laboratorio vlan10, sin identificadores de cliente.
Dirección comprobada	2001:db8:10::25 (prefijo reservado para documentación).
Estado observado	Caché dinámica con expiración; o Incomplete.
Prueba de NS/NA	Solicitud observada / respuesta observada o ausente.
Cambios realizados	Sin cambios; borrado puntual autorizado; corrección de VLAN.
Validación posterior	Ping IPv6 al vecino, ruta, DNS y servicio de negocio verificados.

90.24. Glosario técnico

Término	Definición
NDP / ND	Neighbor Discovery Protocol, componente ICMPv6 para vecinos y routers.
Neighbor Cache	Caché temporal que asocia una IPv6 del enlace con su dirección de capa 2.
NS / NA	Neighbor Solicitation / Neighbor Advertisement; tipos ICMPv6 135 y 136.
RS / RA	Router Solicitation / Advertisement; descubrimiento y anuncios de router.
NUD	Neighbor Unreachability Detection: confirmación de alcanzabilidad de vecinos.
DAD	Duplicate Address Detection, verifica la unicidad antes de utilizar una IPv6.
Scope / zone ID	Sufijo %interfaz que determina el ámbito de una dirección link-local.
SLAAC	Autoconfiguración de direcciones IPv6 a partir de anuncios RA.

90.25. Referencias oficiales y normativas

Netgate — NDP Table

Netgate — ARP Table

Netgate — IPv6 Subnets / Neighbor Discovery

Netgate — Diagnostics Menu

Netgate — Packet Capture GUI

Netgate — Using tcpdump

Netgate — IPv6 Interface Status

RFC 4861 — Neighbor Discovery for IPv6

FreeBSD — ndp(8) manual

Los estados internos y el intercambio ICMPv6 se explican conforme a RFC 4861. La disponibilidad de campos y acciones adicionales depende de la edición, versión y paquetes instalados.

91 Diagnostics → Packet Capture

Captura de paquetes · tcpdump · filtros BPF · VLAN/QinQ · Wireshark

El análisis de paquetes permite observar las comunicaciones en el punto concreto donde atraviesan una interfaz del firewall. Es una de las herramientas más eficaces para distinguir problemas de origen, enrutamiento, filtrado, NAT, encapsulación o respuesta del destino, siempre que se seleccione correctamente el punto de captura y se interprete lo observado dentro del flujo real de pfSense Plus.

PRINCIPIO FUNDAMENTAL Ver paquetes en una interfaz no demuestra que hayan sido aceptados por el firewall. La captura de entrada se realiza antes del procesamiento de reglas y NAT; la de salida refleja el tráfico tras ese procesamiento.

91.1. Finalidad, alcance y ubicación

Ruta exacta: Diagnostics → Packet Capture. La interfaz web utiliza tcpdump como motor de captura y permite generar archivos de paquetes para su consulta local o análisis externo mediante Wireshark. No constituye un sistema de monitorización permanente ni sustituye a los registros de firewall, las tablas de estados o la revisión de rutas.

Los usos principales son localizar dónde deja de circular una conexión, confirmar cabeceras de protocolos, comprobar respuestas, observar la traducción de direcciones y analizar si una VLAN transporta las tramas esperadas. La herramienta opera sobre interfaces del firewall; por sí sola no permite espiar todo el tráfico de un switch de terceros.



Figura 91.1. Entrada y salida respecto al procesamiento de PF y NAT.

91.2. Orientación y controles generales de la pantalla

La pantalla presentada contiene Packet Capture Options, Custom Filter Options y el botón Start. En el encabezado se muestra la ruta y un icono de ayuda. El primer bloque agrupa configuración de captura y visualización; el segundo define condiciones de coincidencia para tráfico sin etiquetas o con VLAN. La documentación de Netgate describe opciones y controles adicionales que aparecen al iniciar o finalizar una captura.

Control visible	Función	Implicación
Interface (primera lista)	Selecciona la interfaz en la que tcpdump observa paquetes.	La selección es decisiva: WAN, LAN, un enlace VLAN lógico o una VPN ofrecen vistas distintas.
Filter preset (segunda lista)	Selecciona Custom Filter u otros perfiles de captura.	Los perfiles predefinidos pueden ocultar Custom Filter Options.
Packet Count	Número máximo de paquetes antes de detener la captura.	Si se deja vacío se aplica el valor predeterminado documentado de 1000; 0 elimina el límite.
Packet Length	Cantidad máxima de bytes por paquete almacenado.	En blanco el predeterminado es 0, captura completa; una longitud menor puede truncar cargas.

Control visible	Función	Implicación
Promiscuous Mode	Solicita recepción de tráfico visible hacia otras MAC.	No convierte un enlace conmutado en espejo de todos los puertos.
View Detail	Grado de detalle de la presentación textual.	No altera la información conservada en el archivo de captura.
View Type	Fuerza interpretación del tipo de tráfico al visualizar.	Útil en determinados protocolos, como CARP; no cambia el paquete.
Name Lookup	Resuelve nombres de hosts, puertos y fabricantes de MAC al visualizar.	Puede introducir demoras y nombres inexactos.
Start	Inicia la captura.	Posteriormente se muestran la vista previa y las acciones Stop/View/Download.

91.3. Interface: seleccionar el punto de observación

La etiqueta de la interfaz presentada al usuario puede diferir del identificador del sistema operativo. En un diagnóstico real se debe verificar Interfaces → Assignments antes de usar tcpdump manualmente. Netgate describe que se pueden seleccionar interfaces asignadas o no asignadas, salvo ciertas interfaces especiales.

Punto de captura	Lo que normalmente permite comprobar	Precaución
LAN o VLAN de usuarios	Solicitudes originales de equipos y recepción de respuestas.	Puede no ver tráfico entre equipos del mismo dominio L2 que no cruza pfSense.
WAN	Tráfico entregado por el ISP y tráfico traducido que sale.	Una WAN detrás de NAT upstream verá direcciones privadas, no necesariamente IP públicas.
Interfaz VPN	Tráfico del túnel según el tipo de interfaz y su capa de encapsulación.	No confundir tráfico cifrado sobre WAN con paquetes interiores del túnel.
Interfaz física/trunk	Tramas sin etiquetar o con 802.1Q/QinQ.	El hardware, los offloads y la interfaz lógica pueden modificar la visibilidad de etiquetas.
Loopback	Comunicaciones locales de servicios.	Una captura vacía en WAN no descarta un intercambio local por loopback.

91.4. Packet Capture Filter: perfiles disponibles

Las opciones documentadas de filtrado incluyen Custom Filter, Everything, Only Untagged y Only Tagged. Seleccionar la que corresponda al tráfico buscado y comprobar los controles disponibles en la revisión instalada.

Perfil documentado	Significado	Uso representativo
Custom Filter	Activa condiciones específicas en las secciones Tagged y Untagged.	Captura focalizada por IP, MAC, protocolo, puerto y etiqueta.
Everything	Captura paquetes sin restringir por esos tipos de filtro.	Confirmación exploratoria breve, preferiblemente con Packet Count limitado.
Only Untagged	Incluye solo tráfico no etiquetado.	Comprobar una red de acceso nativa.
Only Tagged	Incluye solo tráfico con etiqueta VLAN.	Comprobar un trunk o etiquetado no esperado.

91.5. Packet Count y Packet Length: volumen y fidelidad

Packet Count limita cuántos paquetes se registran. La documentación oficial establece 1000 como cantidad por defecto si el formulario la deja sin especificar. Para incidencias de tráfico abundante puede ser necesario ampliar el límite, pero sin generar archivos innecesarios. El valor 0 permite una captura sin límite por número de paquetes, que debe controlarse manualmente.

Packet Length es la longitud de instantánea o snaplen. El valor 0 guarda la trama completa y ofrece mayor fidelidad para Wireshark. Un valor reducido —por ejemplo, 96 o 128 bytes, como criterio de diseño y no como valor por defecto— disminuye la exposición de datos y el uso de almacenamiento, pero puede impedir inspeccionar protocolos o cabeceras extendidas. El tamaño total depende del número de paquetes y de la longitud capturada.

SEGURIDAD DE LA EVIDENCIA Una captura completa puede contener contraseñas de protocolos sin cifrar, cookies, datos personales, información de infraestructura y otros secretos. Antes de exportarla hay que delimitar objetivo, duración, accesos y periodo de conservación.

91.6. Promiscuous Mode y límites físicos

Con Promiscuous Mode activado, tcpdump solicita a la tarjeta recibir tramas visibles aunque su MAC de destino no sea la del firewall. Desactivado, la captura se limita normalmente a tráfico destinado o originado en la interfaz y tramas de difusión y multidifusión. Netgate advierte de posibles problemas con ciertos controladores al activar este modo.

El modo promiscuo no fuerza a un switch Ethernet a reenviar tráfico ajeno hacia el puerto del firewall: se requiere mirroring/SPAN o una posición de red adecuada para verlo. Asimismo, en VLAN y máquinas virtuales, offloads y adaptadores virtuales pueden mostrar tramas de una forma distinta a la que existe físicamente en el enlace.

91.7. View Options: detalle, tipo y resolución de nombres

View Detail modifica la verbosidad de la visualización en texto y View Type permite forzar una interpretación concreta de la captura, por ejemplo en determinados diagnósticos CARP. Name Lookup intenta presentar nombres de host, puertos y fabricantes; normalmente conviene desactivarlo para conservar direcciones literales y evitar retrasos por DNS inverso o identificaciones inexactas.

Las opciones View Detail, View Type y Name Lookup son opciones de visualización: el archivo pcap descargado sigue conteniendo las tramas capturadas con el límite Packet Length establecido. Puede cambiarse la visualización después de realizar la captura y pulsar View cuando dicho botón esté disponible.

91.8. Custom Filter Options: lectura estructural

Los filtros personalizados se dividen en Untagged Filter y Tagged Filter. Cada sección puede incluirse o excluirse. Dentro de cada sección, los campos permiten introducir múltiples valores separados por espacios y establecer operadores internos. El selector OR entre tipos permite cambiar la forma de unir las condiciones entre campos distintos.

Por ejemplo, si se introducen dos direcciones IP distintas en un mismo campo Host y se selecciona «all of», el sentido del filtro puede exigir que ambas aparezcan en el mismo paquete, algo que depende de la construcción concreta y no debe confundirse con elegir uno de dos hosts de interés. Para estudiar conversaciones con cualquiera de los dos extremos, suele ser más apropiado «any of», seguido de la comprobación de la expresión efectiva que se construye. El campo solo limita los paquetes que cumplan su condición; no genera tráfico ni provoca pruebas sobre esos destinos.

La conjunción entre varios tipos también es decisiva. Filtrar simultáneamente por host y puerto suele buscar paquetes que satisfacen ambas restricciones; emplear «OR <type>» puede ampliar mucho el resultado al aceptar paquetes que satisfagan una condición u otra. En una red con tráfico abundante, esa ampliación aumenta rápidamente el tamaño del archivo y puede esconder los pocos paquetes relevantes entre numerosos falsos positivos.

La comprobación profesional consiste en diseñar una prueba con un origen de laboratorio claramente identificable, registrar qué tráfico se espera y revisar el comando tcpdump que genera la interfaz. Si el resultado difiere de la hipótesis, se ajusta un único selector por vez; cambiar varios operadores a la vez dificulta atribuir la diferencia a una causa precisa.



Figura 91.3. Diferencias entre operadores dentro y entre tipos de filtro.

Selector documentado	Efecto lógico	Error habitual
include any of	Habilita la captura de paquetes del tipo de sección si cumplen su criterio.	Creer que cualquier coincidencia global implica capturar todo.
exclude all	Excluye el tráfico de esa sección, aunque se hayan escrito valores.	Configurar una VLAN y mantenerla excluida.
all of	Todos los valores del mismo campo deben coincidir.	Pedir dos orígenes diferentes imposibles simultáneamente.
any of	Basta con que coincida uno de los valores del campo.	Pensar que exige todas las direcciones.
none of	Excluye coincidencias con cualquiera de los valores del campo.	Descartar por error respuestas necesarias.
OR <type>	Coloca OR lógico entre tipos/campos del filtro.	Confundir OR entre campos con any of dentro de un campo.

LECTURA LÓGICA Los operadores de los campos no deben interpretarse mecánicamente como una única regla AND. Para combinaciones complejas, inspeccionar la expresión tcpdump que la GUI muestra después de pulsar Start y validar el resultado con tráfico controlado.

91.9. Untagged Filter: paquetes sin etiqueta VLAN

La sección Untagged Filter se aplica a paquetes sin etiqueta. En la pantalla se observan el selector de inclusión, los operadores junto a cada campo y las cajas de entrada para Host IP Address or Subnet, Host MAC Address, Protocol, Port Number y Ethertype. Si el selector general está en «include any of», los campos activos delimitan el tráfico sin etiqueta.

Campo Untagged	Qué compara	Ejemplo exclusivamente didáctico
Host IP Address or Subnet	Dirección IP de origen/destino o red en formato CIDR.	192.0.2.10 198.51.100.0/24
Host MAC Address	Dirección MAC completa o prefijo parcial.	02:00:00:00:00:01
Protocol	Número IP o nombre de protocolo reconocido por tcpdump.	tcp udp icmp icmp6
Port Number	Puerto de origen o destino de TCP/UDP.	53 443
Ethertype	Tipo Ethernet: IPv4, IPv6, ARP, etc.	arp 0x86dd

Los números de protocolo IP y el Ethertype cumplen funciones distintas: TCP (6) o UDP (17) corresponden a la cabecera IP, mientras que ARP (0x0806), IPv4 (0x0800) e IPv6 (0x86dd) pertenecen a la cabecera Ethernet. El puerto solo resulta aplicable a protocolos con puertos, como TCP/UDP.

91.10. Tagged Filter: VLAN Tag y Level para QinQ

Tagged Filter trabaja con tramas que contienen etiquetas VLAN. Además de los campos IP, MAC, protocolo, puerto y Ethertype, incluye VLAN Tag y Level para identificar la VLAN y el nivel de etiqueta en QinQ/802.1ad. La opción exclude all excluye el tráfico etiquetado de ese grupo; ajustar las casillas según el alcance de la captura.



Figura 91.2. Tráfico sin etiqueta, con 802.1Q y con dos niveles QinQ.

No debe asumirse que el valor de VLAN Tag corresponde siempre a la misma cabecera física cuando existe doble etiquetado. Debe identificarse qué nivel está seleccionando el filtro. En enlaces trunk, comparar captura de la interfaz física y captura de la interfaz VLAN lógica puede revelar diferencias por el tratamiento del driver o del hardware.

CAMBIOS DE ENLACE No habilitar o modificar VLAN en el firewall como prueba improvisada si se administra el equipo a través de ese enlace. Primero utilizar la captura sin alterar la configuración y validar los extremos del trunk.

91.11. Interpretación de ejemplos de filtros

Objetivo	Criterio representativo	Resultado esperado / matiz
DNS de un host de prueba	Host 192.0.2.10 + UDP/TCP puerto 53	Ver preguntas y respuestas en el punto capturado; DNS sobre TLS/HTTPS usa otros puertos.
TCP a una aplicación	Host 192.0.2.20 + TCP puerto 443	SYN/SYN-ACK/ACK si el flujo atraviesa la interfaz y el filtro incluye ambos sentidos.
Descubrimiento ARP	Ethertype arp, en sección sin etiqueta	Solicitudes y respuestas ARP del segmento correspondiente.
ICMPv6/Neighbor Discovery	Protocol icmp6 y ámbito IPv6	NS/NA y otras tramas visibles en ese punto; no se utiliza ARP en IPv6.
Trunk con VLAN 100	Tagged incluye VLAN 100, Level según etiqueta	Solo tramas con la etiqueta pertinente si el driver la expone.
Verificar si el firewall recibe tráfico	Filtro amplio, ventana breve, límite definido	La ausencia puede ser un problema de interfaz, filtro, routing o upstream.

91.12. Inicio, detención y consulta de una captura

1. **Preparar.** Definir hipótesis, interfaces, tiempo de prueba, filtro y volumen máximo. Evitar capturas generalistas durante periodos largos.
2. **Iniciar.** Pulsar Start; la interfaz muestra una vista previa actualizable y la línea tcpdump aplicada, según la documentación oficial.
3. **Reproducir.** Generar un único intento de comunicación identificable desde un equipo de prueba autorizado; anotar momento y extremo de origen.
4. **Detener.** Pulsar Stop si no se ha alcanzado el límite automático de Packet Count. Guardar el contexto de la prueba.

5. **Consultar.** Utilizar View para ver Packet Capture Output; variar View Detail/Type o Name Lookup sin repetir la captura cuando solo cambie la visualización.
6. **Exportar.** Descargar el archivo pcap con Download para analizarlo, si procede, en Wireshark; conservarlo bajo control de acceso.

Stop, View y Download aparecen según el estado de la captura. Stop la detiene, View permite examinarla y Download descarga el archivo para su análisis. Comprobar el estado antes de buscar estas acciones.

91.13. Análisis en Wireshark: captura frente a filtro de visualización

Wireshark permite analizar la lista de paquetes, los encabezados por capas y los datos binarios. Sus display filters reducen lo que se muestra, pero no recuperan tramas que fueron excluidas al capturar con un filtro BPF ni datos recortados mediante Packet Length. Conviene conservar el original y trabajar sobre una copia cuando la captura se utilice como evidencia.

Filtro de visualización Wireshark	Lectura
ip.addr == 192.0.2.10	Cualquier paquete IPv4 con esa dirección en origen o destino.
tcp.port == 443	Tráfico TCP con puerto 443 de origen o destino.
dns	Paquetes reconocidos por el disector DNS.
icmpv6	Mensajes ICMP para IPv6.
vlan.id == 100	Tramas con etiqueta VLAN 100 visibles en la captura.
tcp.flags.syn == 1 && tcp.flags.ack == 0	Intentos TCP SYN iniciales.

Un display filter de Wireshark no utiliza la misma sintaxis que los capture filters de tcpdump/BPF. Por ejemplo, la expresión BPF tcp port 443 equivale funcionalmente al propósito de tcp.port == 443 como filtro de visualización, pero no es intercambiable en la misma caja.

91.14. tcpdump desde consola: alternativa profesional

La consola permite crear filtros BPF y capturas simultáneas de forma más flexible. Es imprescindible identificar previamente el nombre real de interfaz con Interfaces → Assignments o con herramientas de consulta. Los comandos siguientes son ejemplos de lectura en una instalación de laboratorio, sin modificación de reglas:

```
tcpdump -ni igb0 -c 200 "host 192.0.2.10 and (tcp port 443 or udp port 53)"
tcpdump -ni igb1 -s 0 -c 300 -w /tmp/prueba_diagnostico.pcap "tcp port 443"
tcpdump -eni igb0 -c 100 "vlan 100"
```

Parámetros orientativos: -n evita resolución de nombres, -i selecciona interfaz, -c limita paquetes, -s controla longitud, -w escribe un archivo y -e presenta encabezados Ethernet. Las herramientas se ejecutan con privilegios de administración; el archivo debe gestionarse como dato sensible. No se recomienda crear capturas indefinidas con archivos crecientes en el almacenamiento del firewall.

91.15. Cómo localizar una interrupción de NAT o firewall

El diagnóstico más fiable compara al menos dos puntos: interfaz de entrada e interfaz de salida. En entrada WAN se puede ver un SYN recibido antes de que una regla lo bloquee; en LAN se comprueba si se reenviaron los paquetes con el destino traducido por un port forward. En el sentido inverso, la respuesta debe atravesar nuevamente el firewall y salir con la traducción correspondiente.

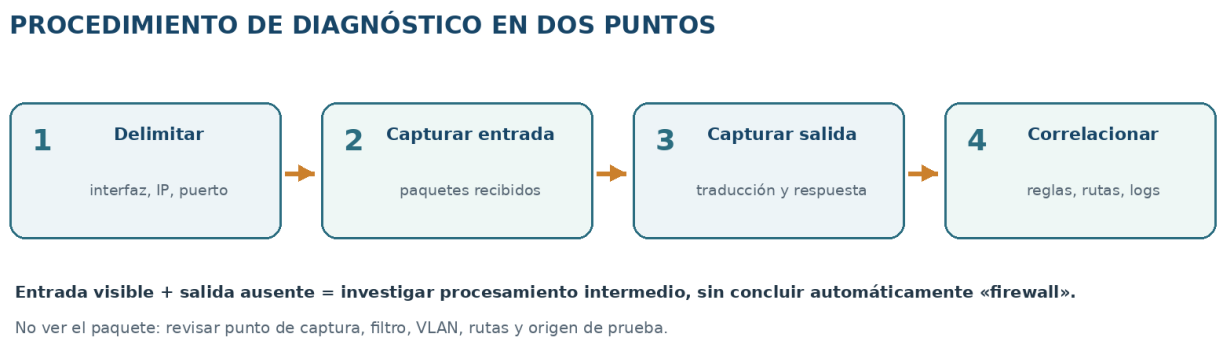


Figura 91.4. De una prueba reproducible a una conclusión contrastada.

Observación	Hipótesis razonable	Siguiente comprobación
No aparece tráfico al entrar	Origen de prueba, upstream, interfaz o filtro erróneo.	Revisar ruta, puerto, etiqueta y punto físico de captura.
Entra por WAN, no sale por LAN	Filtrado, NAT, enrutamiento o configuración intermedia.	Correlacionar System Logs → Firewall, States, NAT y Routes.
Sale por LAN sin respuesta	Host destino, gateway local, servicio o firewall del equipo.	Capturar en el host destino o su segmento.
Hay respuesta en LAN, no sale por WAN	Estado, traducción, ruta de retorno o policy routing.	Examinar estado PF, reglas y gateway de retorno.
Se observa handshake VPN pero no datos	Rutas interiores, selectors/Allowed IPs, reglas o DNS.	Capturar interfaz VPN adecuada y comparar con LAN.
Se ven paquetes con VLAN inesperada	Trunk, etiquetado de switch o QinQ.	Comparar parent, interfaz lógica y configuración del switch.

91.16. Procedimiento 1: diagnosticar una redirección de puerto

1. Desde una fuente externa autorizada, repetir el acceso a un servicio de laboratorio en 203.0.113.20:443 (dirección de documentación).
2. Capturar en WAN con TCP puerto 443 y Packet Count limitado; buscar el SYN al destino exterior.
3. Capturar en LAN con TCP puerto 443 hacia 192.0.2.20; comprobar la llegada tras NAT y el cambio de dirección de destino.
4. Contrastar los resultados con Firewall → NAT y Firewall → Rules, además de Diagnostics → States. Si no hay respuesta, verificar el propio servicio y el gateway del destino.

91.17. Procedimiento 2: diagnosticar pérdida de DNS o DHCP

Para DNS: tomar la captura en la interfaz donde aparece el cliente, limitar por UDP/TCP 53 y verificar solicitudes y respuestas. Si se usa DNS cifrado, el filtro de puerto 53 no basta para demostrar ausencia de consultas. Para DHCPv4: observar UDP 67/68 y, si corresponde, mensajes Discover, Offer, Request y Acknowledge en el segmento pertinente. Los retransmisiones sin respuesta deben correlacionarse con el estado de Kea/ISC DHCP, relay, VLAN y reglas de firewall. Para DHCPv6 revisar UDP 546/547 e ICMPv6 cuando sea necesario.

91.18. Procedimiento 3: errores de VLAN y QinQ

1. Identificar si la interfaz observada es una interfaz física trunk o una VLAN lógica asignada.
2. Utilizar Only Tagged, o Custom Filter con Tagged incluido y Untagged excluido, para aislar tráfico etiquetado.
3. Introducir VLAN Tag 100 y Level correspondiente; comparar con una captura sin filtro de VLAN y con el diseño de etiquetado esperado.

4. Si no aparecen etiquetas, comprobar si el driver presenta tramas después de retirar las etiquetas o si se está observando la interfaz lógica y no el parent.

91.19. Procedimiento 4: Multi-WAN y VPN

Cuando un flujo sale por un enlace distinto del esperado, capturar primero en la interfaz de entrada, después en cada WAN pertinente, y contrastar con Status → Gateways, Diagnostics → States y rutas de policy routing. En VPN, debe distinguirse el tráfico cifrado exterior (UDP de OpenVPN/WireGuard o IKE/IPsec) del tráfico interior tras descifrado. El punto de captura de las interfaces virtuales depende del tipo de túnel y del comportamiento de la plataforma.

91.20. Rendimiento, offloading y límites de interpretación

Los paquetes capturados pueden diferir de la estructura física transmitida si hay offloading de checksum, TSO/LRO, fragmentación o tratamiento hardware de VLAN. Un checksum aparentemente incorrecto no prueba por sí solo un paquete mal transmitido: puede calcularse después de la observación del software. Si se sospecha un problema de captura, contrastar con el punto remoto y, cuando proceda, con una captura externa/SPAN.

Capturas muy extensas pueden cargar CPU, memoria, disco y transferencia WAN en equipos compactos. Resulta preferible usar filtros específicos y un límite de paquetes, salvo en casos controlados. En investigación de errores intermitentes, fijar ventanas breves asociadas a un evento reproducible.

91.21. Seguridad, privacidad y conservación de evidencias

El archivo pcap puede incluir direcciones, topología, nombres, MAC, identificadores de sesión y cargas útiles sensibles. Debe considerarse una evidencia técnica con acceso restringido: definir responsable y finalidad, cifrar el almacenamiento/transporte, aplicar retención mínima, registrar fecha y punto de captura, y evitar compartirlo sin anonimización apropiada. Si se remite a soporte externo, revisar contenidos y minimizar la exposición antes del envío.

PROTECCIÓN DE DATOS El uso de Name Lookup puede enriquecer la visualización con nombres sensibles. Desactivarlo no anonimiza la captura ni elimina identificadores de los paquetes. No es una medida de desidentificación.

91.22. Matriz de incidencias y acciones de diagnóstico

Síntoma	Causa frecuente	Acción inicial
No se ve ningún paquete	Interfaz incorrecta, filtro demasiado restrictivo, VLAN oculta.	Cambiar a Everything por una ventana breve y comprobar la interfaz.
Captura demasiado grande	Count ilimitado o filtro amplio.	Detener; aplicar puertos/host y snaplen adecuado.
No aparecen etiquetas VLAN	Interfaz lógica o offload de etiquetas.	Capturar en interfaz física y comprobar switch/driver.
Solo se ven SYN	Servicio inaccesible o respuesta por otra ruta.	Capturar en destino y revisar rutas/estados.
Wireshark no decodifica completo	Packet Length recortado o protocolo encapsulado.	Repetir con snaplen 0 y View Type adecuado.
Retrasos al usar View	Name Lookup activado.	Desactivar resolución de nombres y repetir View.
Captura muestra IP inesperada	NAT o doble NAT en otro punto.	Comparar entrada/salida con States y NAT.
El tráfico desaparece tras failover	Rutas o cambio de interfaz/gateway.	Capturar en WAN de respaldo; revisar states y policy routing.

91.23. Glosario operativo

Término	Definición resumida
pcap	Formato de fichero para conservar paquetes capturados.
BPF	Lenguaje/filtro usado por tcpdump para decidir qué paquetes registrar.
Snaplen	Máximo de bytes de cada paquete que se conservan.
Promiscuous mode	Recepción ampliada de tramas visibles en la interfaz.
802.1Q / QinQ	Etiquetado VLAN sencillo / etiquetas VLAN apiladas.
SPAN	Copia de tráfico de puertos de switch hacia una interfaz de observación.
Capture filter	Condición aplicada al registrar paquetes, irreversible sobre la captura resultante.
Display filter	Condición de visualización sobre un archivo ya capturado.

91.24. Lista de comprobación para intervención profesional

Antes de capturar	Al capturar	Después de capturar
Acreditar autorización y finalidad.	Confirmar interfaz y filtro BPF real.	Detener proceso y conservar contexto.
Definir IP/protocolo/puertos de prueba.	Limitar duración, count y snaplen.	Guardar copia controlada del pcap.
Comprobar reloj NTP del firewall.	Anotar hora y acción que dispara tráfico.	Contrastar entrada, salida y logs.
Evitar capturas del tráfico ajeno.	No sacar conclusiones por un único lado.	Eliminar duplicados según política de retención.

91.25. Referencias técnicas oficiales y normativas

Netgate · Packet Capture GUI
Netgate · Packet Capturing
Netgate · Selecting the Proper Interface
Netgate · Limiting capture volume
Netgate · Using tcpdump on the command line
Netgate · Using Wireshark
Netgate · Ordering of NAT and Firewall Processing
Netgate · Troubleshooting NAT Port Forwards
Netgate · VLAN Configuration
Wireshark · Display Filter Reference

La denominación exacta de controles, valores y opciones adicionales puede variar según la versión de pfSense Plus y los dispositivos de red. La descripción de los controles visibles se corresponde con la pantalla de referencia; las restantes opciones se fundamentan en los documentos oficiales enlazados.

92 Diagnostics → pfInfo

Motor PF · tablas de estados · contadores · límites · rendimiento · diagnóstico

La pantalla pfInfo proporciona una visión estadística del filtro de paquetes de pfSense Plus. Su utilidad no reside en un número aislado, sino en relacionar actividad, límites de memoria, resultados de filtrado y cambios de comportamiento durante una incidencia. Este capítulo convierte el listado de indicadores en un método de diagnóstico reproducible.

CRITERIO OPERATIVO La información de pfInfo es esencialmente de lectura. Antes de modificar reglas, límites, estados o parámetros de kernel, documentar una línea base, verificar el impacto y disponer de un acceso alternativo al firewall.

92.1. Función técnica y ruta de acceso

Ruta: Diagnostics → pfInfo. El filtro de paquetes PF mantiene reglas, tablas de estados, seguimiento de orígenes y contadores que permiten explicar cómo circula el tráfico por el firewall. pfInfo presenta el estado agregado de estos mecanismos; no sustituye a los registros ni al análisis de una conexión concreta.

La página muestra un control de actualización automática y un bloque de salida textual. Los valores dependen de la versión de PF/FreeBSD, las interfaces disponibles, el perfil de tráfico y las opciones activas. El vocabulario se ha contrastado con la guía oficial; ciertos nombres internos pueden variar entre versiones.



Figura 92.1. Relación entre el recorrido del paquete, la tabla de estados y las herramientas de supervisión.

92.2. Auto Update Page, Refresh y Output

Control / área	Qué realiza	Cómo debe utilizarse
Auto Update Page	Permite activar la actualización repetida de la salida mostrada.	Detenerla si se necesita comparar o conservar una lectura concreta.
Refresh	Control asociado a refrescar periódicamente los datos; la presentación puede variar según versión.	Evitar confundir la tasa/s con un valor acumulado desde el último clic.
Output	Bloque textual con estadísticas del filtro PF, por categoría.	Copiar solo después de anonimizar interfaces, identificadores y topología.

La consulta es de observación, pero una actualización intensiva puede añadir carga marginal a una sesión administrativa y alterar la lectura visual. Los contadores acumulados deben compararse con sus intervalos de referencia y con la hora del último reinicio o reinicialización del filtro.

92.3. Cabecera de estado: Enabled, tiempo, Debug, Host ID y Checksum

Indicador	Interpretación técnica	Cautela
Status: Enabled/Disabled	Indica si el filtro PF se encuentra habilitado y durante cuánto tiempo.	No representa necesariamente el uptime completo de FreeBSD.

Indicador	Interpretación técnica	Cautela
Debug	Nivel de depuración del motor PF; define mensajes internos generados por el filtro.	Urgent es un nivel de depuración, no una alarma de gravedad actual.
Hostid	Identificador de 32 bits utilizado por PF para identificar el origen de los estados.	Puede cambiar al recargar el filtro; no divulgarlo como dato de topología.
Checksum	Resumen hexadecimal asociado al conjunto de reglas PF cargado.	No es una firma de seguridad del appliance ni prueba de reglas correctas.

Una diferencia de checksum entre dos momentos merece contrastarse con los cambios de configuración y Status → Filter Reload. La presencia de un mismo checksum no verifica que servicios externos, NAT o rutas funcionen. En HA, además, los estados sincronizados se interpretan con el Host ID apropiado.

92.4. Interface Stats: Bytes y Packets In/Out

El bloque Interface Stats contiene recuentos separados para IPv4 e IPv6. Las columnas In y Out se refieren al sentido visto desde la interfaz, mientras que Passed y Blocked distinguen el resultado del filtro. Estos totales no deben interpretarse como una lista de sesiones ni como un medidor de uso de Internet.

Campo	Significado	Lectura práctica
Bytes In / Bytes Out	Bytes contabilizados en sentido entrante o saliente.	La interpretación depende del punto de observación y del contador mostrado.
Packets In → Passed	Paquetes entrantes admitidos por PF.	Correlacionar con la interfaz y estados.
Packets In → Blocked	Paquetes entrantes descartados por PF.	Comparar con reglas y Firewall Logs; no todos son incidentes.
Packets Out → Passed	Paquetes salientes admitidos.	Puede aumentar incluso cuando no se completa una conversación remota.
Packets Out → Blocked	Paquetes salientes descartados.	Considerar reglas flotantes y rutas asimétricas.

INTERPRETACIÓN Un total elevado de bloqueos, sin tendencia ni comparación, no demuestra un ataque. La exposición de WAN produce tráfico no solicitado normal; conviene medir incrementos por minuto y localizar su causa con registros y capturas.

92.5. State Table: conexiones activas y tasas

PF es un filtro con estado. Normalmente, cuando un primer paquete coincide con una regla permisiva, se crea una entrada que permite reconocer los paquetes posteriores del mismo flujo y sus respuestas. La tabla de estados soporta también el seguimiento asociado a NAT.

Campo	Qué contabiliza	Significado operativo
Current entries	Estados presentes en ese instante.	Comparar frente al límite hard limit de states y a la memoria disponible.
Searches / rate	Consultas a la tabla y consultas por segundo.	Estima el trabajo de búsqueda; no es una medida exacta de conexiones nuevas.
Inserts / rate	Nuevos estados creados y creación por segundo.	Un pico puede corresponder a muchas conexiones nuevas, escáneres o clientes.
Removals / rate	Estados retirados y tasa de eliminación.	La evolución ayuda a entender reciclaje o expiración de conexiones.

Ejemplo exclusivamente didáctico: 12 000 estados activos frente a un límite de 120 000 representan una ocupación del 10 %. El porcentaje aporta más contexto que el número sin referencia. Deben estudiarse simultáneamente la memoria, la tasa de inserciones y los contadores de rechazo por límite.

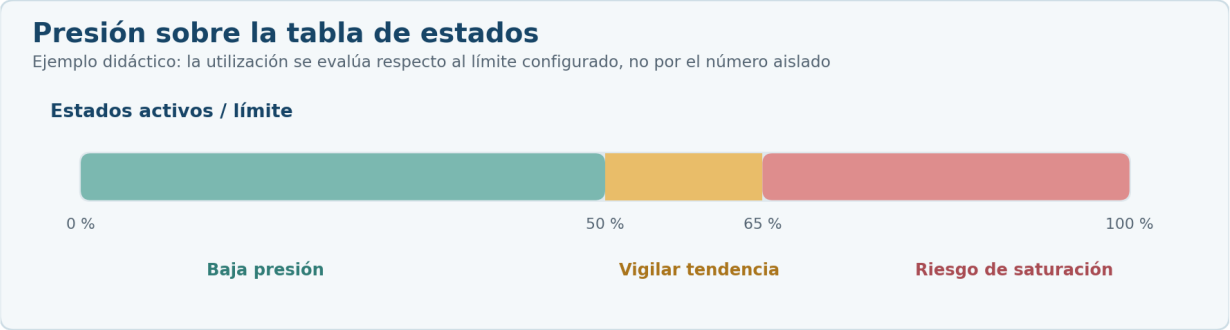


Figura 92.2. Comparación de utilización de estados con el límite configurado; franjas ilustrativas no normativas.

92.6. Source Tracking Table: seguimiento de orígenes

La tabla de seguimiento de orígenes se utiliza con funcionalidades específicas, como conexiones adhesivas (sticky connections) en grupos de gateways de balanceo. La existencia de cero entradas puede ser totalmente esperable si el mecanismo no interviene en el tráfico observado.

Métrica	Interpretación	Qué verificar
Current entries	Asociaciones origen/seguimiento existentes.	Revisar si Sticky Connections está configurado.
Searches, Inserts, Removals	Accesos, creación y retirada de entradas.	Correlacionar con grupos de gateways y failover.
Rate	Actividad reciente de la categoría.	No deducir consumo de ancho de banda.

92.7. Fragments y reconstrucción de paquetes

Fragments expone los registros relacionados con fragmentos IP y sus altas, búsquedas y retiradas. Una actividad de fragmentación elevada puede justificar revisar MTU, PMTUD, túneles y políticas de normalización. Los contadores de fragmentos no permiten, por sí solos, identificar la causa o afirmar que existe una anomalía.

El indicador Reassemble informa de la modalidad activa de reensamblado/normalización del motor PF. Su interpretación depende del contexto de las reglas y las versiones; no es un permiso para modificar la opción de scrub sin una prueba controlada.

92.8. Counters: visión general de eventos y descartes

El bloque Counters combina coincidencias, paquetes malformados, comprobaciones de estado, límites de memoria y circunstancias relacionadas con NAT. Sus nombres son los de PF y deben leerse como instrumentación diagnóstica. Un valor distinto de cero puede ser histórico o normal.

Contador	Qué señala de forma general	Validación recomendada
match	Actividad de coincidencia con reglas/criterios del filtro.	Correlacionar con reglas activas y tráfico real.
bad-offset	Desplazamientos o formato de paquete no válido.	Capturar muestras y revisar cabeceras.
fragment	Paquete/fragmento rechazado en el tratamiento de fragmentación.	Comprobar MTU y capturas IP.
short	Tramas o datagramas demasiado cortos para ser válidos.	Distinguir errores de captura de tráfico malformado.
normalize	Fallos al normalizar/reensamblar según políticas PF.	Verificar scrub, MTU y paquetes.
memory	Falta de recursos o memoria para el procesamiento PF.	Comprobar límites, memoria y tendencia del contador.

Contador	Qué señala de forma general	Validación recomendada
bad-timestamp	Incoherencias de timestamp TCP detectadas.	Revisar flujos TCP y asimetrías.
congestion	Descartes asociados a congestión o presión interna.	Examinar carga, colas y hardware.

92.9. Counters: opciones IP, checksums, estados y NAT

Contador	Interpretación operativa	Contexto de diagnóstico
ip-option	Problemas o tratamiento de opciones IP no aceptadas.	Verificar tipo de opciones y reglas.
proto-cksum	Comprobación de checksum de protocolo fallida.	Cotejar con offloading y captura en interfaces.
state-mismatch	Paquetes que no encajan en el estado PF esperado.	Examinar rutas asimétricas, retransmisiones y estados antiguos.
state-insert	Fallo en el intento de insertar un nuevo estado.	Buscar límites, recursos o inconsistencias.
state-limit	Tope de estados alcanzado para el ámbito aplicable.	Revisar capacidades y reglas que limitan estados.
src-limit	Límite aplicable a orígenes superado.	Revisar límites por IP y rate-limit.
synproxy	Eventos relacionados con el proxy SYN de PF.	Validar políticas SYN proxy y establecimiento TCP.
map-failed	Error en asignación o traducción asociada a mapeos.	Correlacionar con NAT y disponibilidad de puertos.
translate	Eventos/error al traducir direcciones o puertos.	Correlacionar con NAT, reglas y estados.



Figura 92.3. Lectura correcta de un contador: tendencia, correlación y acción proporcional.

92.10. Limit Counters: reglas con restricciones de conexión

Los Limit Counters permiten identificar rechazos por restricciones configuradas y la actividad de las defensas específicas de PF. No representan necesariamente una amenaza: pueden aparecer durante pruebas o como consecuencia de una regla demasiado restrictiva.

Nombre en pfInfo	Concepto asociado	Precaución
max states per rule	Máximo de estados permitidos por una regla.	La denegación afecta a nuevas conexiones.
max-src-states	Máximo de estados por dirección de origen.	Revisar si hay NAT compartido por muchos usuarios.
max-src-nodes	Máximo de nodos de origen seguidos.	Examinar reglas y diversidad de clientes.

Nombre en pfInfo	Concepto asociado	Precaución
max-src-conn	Límite de conexiones TCP establecidas por origen.	Puede afectar servicios con muchas conexiones.
max-src-conn-rate	Límite de nuevas conexiones en una ventana temporal.	Verificar ráfagas legítimas y escaneos.
overload table insertion	Inclusión de origen en tabla por superar límites.	Revisar entrada generada y política de expiración.
overload flush states	Eliminación de estados relacionada con sobrecarga.	Puede producir cortes activos.
synfloods detected	Detección de patrones compatibles con inundación SYN.	Confirmar con registros y capturas.
syncookies sent / validated	Cookies SYN emitidas y comprobadas.	Interpretarlas junto con el modo activo y la presión de estados.

92.11. Syncookies: protección del establecimiento TCP

Las SYN cookies ayudan a mitigar determinadas situaciones de carga asociadas al establecimiento TCP y a la gestión de estados semiabiertos. pfInfo muestra parámetros como mode, active, highwater, lowwater y halfopen states. Los porcentajes son umbrales de operación propios del mecanismo; no deben copiarse como recomendaciones universales.

Indicador	Significado
mode	Política configurada para el uso del mecanismo; los valores posibles dependen del PF incluido en la versión.
active	Indica si el mecanismo está actuando en el instante consultado.
highwater / lowwater	Umbrales superior e inferior asociados a su activación/desactivación según el modo.
halfopen states	Número de conexiones TCP en estados de negociación incompleta contabilizadas.

SEGURIDAD No activar ni desactivar SYN cookies, SYN proxy o límites globales guiándose solo por un contador de la pantalla. Primero comprobar el tipo de servicio expuesto, la versión de PF y el comportamiento de tráfico legítimo.

92.12. Límites duros: estados, nodos, fragmentos, tablas y anchors

Límite en la salida	Qué limita	Riesgo si se agota
states hard limit	Cantidad máxima de estados PF.	Rechazo de nuevos estados; degradación general.
src-nodes hard limit	Entradas para seguimiento de fuentes.	Fallo de políticas que requieren nodos de origen.
frags hard limit	Entradas para manejo de fragmentos.	Problemas con tráfico fragmentado.
table-entries hard limit	Entradas en las tablas PF (aliases y otras).	Fallo de carga o actualización de tablas.
anchors hard limit	Cantidad máxima de anchors.	Limitación en la composición del ruleset.
eth-anchors hard limit	Anchors Ethernet en escenarios compatibles.	Revisar solo si se utilizan reglas Ethernet.

La configuración de tamaño de tabla de estados y sus límites está relacionada con RAM, políticas activas y reglas. Aumentar el máximo sin analizar la memoria disponible puede cambiar una saturación de estados por un problema de recursos más grave. Ver también System → Advanced → Firewall & NAT.

92.13. State Timers: estructura y unidades

El bloque de tiempos de espera muestra valores en segundos para distintas fases de las conexiones. Son tiempos de retención de estados que pueden verse modificados por el modo de optimización y, cuando procede, por reglas con excepciones. No son pruebas de la duración real de cada sesión ni deben alterarse como primera medida de diagnóstico.

Familia	Parámetros que pueden verse	Función resumida
TCP	first, opening, established, closing, finwait, closed, tsdiff	Gestión desde el primer paquete hasta el cierre y comprobaciones temporales.
SCTP	first, opening, established, closing, closed	Control del ciclo de las asociaciones SCTP; su disponibilidad depende del PF.
UDP	first, single, multiple	Persistencia al inicio, tráfico unilateral y bilateral.
ICMP	first, error	Conservación de estados para peticiones y errores ICMP.
Other	first, single, multiple	Otros protocolos sin el estado TCP específico.
General	frag, interval, src.track	Fragmentos, revisión periódica y seguimiento de origen.

92.14. Adaptive Start y Adaptive End: expiración bajo presión

Los timeouts adaptativos reducen la retención de estados conforme su ocupación supera Adaptive Start y se aproxima a Adaptive End. Netgate documenta que, por defecto, estos umbrales derivan del máximo de estados (habitualmente 60 % y 120 %, respectivamente, cuando se aplica el cálculo automático). La intención es recuperar espacio antes de agotar recursos.

Ejemplo didáctico: límite de 100 000 estados, inicio adaptativo en 60 000 y final en 120 000. Si hay 90 000 estados, el factor teórico de retención sería (120 000 − 90 000)/(120 000 − 60 000) = 0,5. Se trata de un cálculo para comprender el mecanismo, no de una pauta de configuración.

OPERACIÓN Al acelerar expiraciones es posible que aplicaciones de larga duración experimenten cierres inesperados. Un temporizador alto no corrige saturación permanente; puede incluso agravarse si hay numerosas sesiones ociosas.

92.15. Estadísticas detalladas por interfaz y familia IP

La segunda parte de la salida de pfInfo suele mostrar bloques por interfaz y por pila IPv4/IPv6. En cada uno aparecen References, Cleared y contadores In4/Out4/In6/Out6, separados en Pass y Block, con paquetes y bytes. Esos datos complementan los contadores globales.

Campo	Significado	Interpretación segura
Interface	Identificador de la interfaz según el sistema operativo.	No confundir con el nombre descriptivo de la GUI.
Cleared	Momento en que se inicializó o puso a cero ese bloque.	Dos interfaces pueden tener ventanas distintas.
References	Referencias internas del subsistema PF a esa interfaz.	No equivale al número de equipos conectados.
In4 / Out4	Tráfico IPv4 entrante/saliente y Passed/Blocked.	Comparar direcciones coherentemente.
In6 / Out6	Igual para IPv6.	Los mensajes de control IPv6 tienen patrones distintos.
Packets / Bytes	Volumen y tamaño acumulado por categoría.	El delta entre lecturas describe mejor una incidencia.

En la documentación de ejemplo se utilizarán únicamente interfaces genéricas como em0 y em1, sin vinculación con una instalación real. Los bloques del tipo enc0, lo0, interfaces de túneles o pfsync pueden tener semánticas distintas; las cifras cero no implican necesariamente que el servicio correspondiente esté averiado.

92.16. Cómo obtener tasas correctamente

Los campos Total y Rate ofrecen lecturas diferentes. Cuando existe Rate, debe respetarse la unidad indicada (normalmente eventos por segundo). Para un contador acumulado, calcular la diferencia entre dos lecturas separadas por tiempo conocido: tasa estimada = (contador final − contador inicial) / segundos transcurridos.

Ejemplo didáctico: si In4/Block pasa de 800 a 920 eventos en 60 segundos, el incremento medio es de 2 descartes por segundo. No se debe calcular esa diferencia a través de una recarga o reinicio que haya puesto contadores a cero.

92.17. Correlación con otras pantallas de pfSense Plus

Síntoma en pfInfo	Pantalla complementaria	Pregunta que resuelve
Aumentan Inserts	Diagnostics → States / States Summary	¿Quién crea las conexiones?
Aumenta state-mismatch	Diagnostics → Packet Capture; Status → Gateways	¿Existe retorno asimétrico o cambio de ruta?
Crecen In4/Block	Status → System Logs → Firewall	¿Qué regla y origen coinciden con los descartes?
Se acerca hard limit states	Status → Dashboard; Diagnostics → System Activity	¿Existe presión de RAM o CPU?
Aumentan errores de NAT	Firewall → NAT y Diagnostics → States	¿Qué traducción o estado falla?
Diferencias WAN / VPN	Status → OpenVPN/IPsec; Diagnostics → Routes	¿El túnel está conectado y con rutas válidas?

92.18. Procedimiento 1: registrar una línea base fiable

1. Abrir Diagnostics → pfInfo durante un periodo conocido de operación estable y desactivar la actualización automática para guardar una primera lectura.

2. Anotar hora, versión de pfSense, ocupación de estados, tasas Searches/Inserts/Removals, contadores anómalos y momento de Cleared, sin publicar identificadores.

3. Guardar de forma segura información complementaria de Dashboard y de las interfaces; anotar si hay cambios recientes en reglas, NAT, VPN o gateways.

4. Repetir la lectura en otra franja representativa, calculando incrementos sobre los contadores comparables. Diferenciar picos aislados de tendencias persistentes.

92.19. Procedimiento 2: investigar pérdidas de conexión y state-mismatch

1. Reproducir un fallo controlado desde un host autorizado, registrando origen, destino y hora en una ficha interna protegida.

2. Revisar evolución de state-mismatch y de descartes por interfaz. Un pequeño acumulado sin cambios recientes no es causa suficiente.

3. Verificar el estado concreto en Diagnostics → States y la ruta de ida y vuelta, especialmente en instalaciones Multi-WAN o tras un failover.

4. Consultar System Logs y realizar una captura acotada en las dos interfaces relevantes. Comprobar si el tráfico de retorno utiliza una salida distinta.

5. Proponer la corrección mínima comprobada; no eliminar toda la tabla de estados como primer paso. La eliminación masiva interrumpe conexiones establecidas.

92.20. Procedimiento 3: detectar agotamiento de estados

1. Comparar Current Entries con hard limit de states; estudiar memoria y tasa de inserciones. Una tabla casi llena exige actuar sobre la causa, no solo sobre el límite.

2. Consultar States Summary para identificar fuentes o destinos con muchos estados, recordando que en firewalls con tablas enormes el informe puede ser costoso.

3. Revisar reglas con máximos de conexiones, nuevos estados por segundo y controles de sobrecarga. Considerar servicios legítimos detrás de NAT.

4. Evaluar si existe actividad maliciosa, conexiones no cerradas o configuración incorrecta. Solo tras dimensionamiento se justifica cambiar límites o optimización.

92.21. Procedimiento 4: descartar problemas IPv6, fragmentación o VPN

1. Separar contadores In4/Out4 de In6/Out6 y verificar que las reglas y rutas IPv6 existen cuando se esperan comunicaciones de esa familia.

2. Si aumenta Fragments o errores de normalización, comprobar MTU, PMTUD y la encapsulación VPN sin desactivar características de seguridad indiscriminadamente.

3. Revisar el estado del túnel y sus rutas reales. Una interfaz virtual con contadores a cero puede estar sin tráfico mientras un túnel de control permanece activo.

4. Correlacionar un cambio de ruta o de NAT con los estados mantenidos. Conservar evidencias antes de cualquier reinicio o limpieza de tablas.

92.22. Procedimiento 5: inspección desde consola con pfctl

Comando orientativo de consulta	Utilidad	Precaución
pfctl -si	Estadísticas y contadores generales del motor PF.	Ejecutar en consola autorizada, solo lectura.
pfctl -vvsI	Estadísticas por interfaces (si la sintaxis está admitida).	Confirmar sintaxis exacta en el PF de la versión.
pfctl -ss	Listado de estados activos.	La salida puede ser muy voluminosa.
pfctl -s rules	Inspección de reglas cargadas.	Puede contener información sensible del entorno.
pfctl -s memory	Límites de memoria del filtro en versiones compatibles.	No modificar parámetros durante el diagnóstico inicial.

CUIDADO Nunca utilizar comandos de limpieza o desactivación del filtro, como operaciones globales sobre estados o reglas, en una sesión de diagnóstico no autorizada. Su efecto puede cortar el acceso remoto al firewall.

92.23. Escenarios empresariales de interpretación

Escenario	Señal orientativa	Secuencia de comprobación
Oficina con navegación lenta	Sube Searches y crece el tiempo de respuesta de aplicaciones.	Contrastar CPU, RTT gateway, DNS y capturas; no atribuirlo directamente a PF.
Sede conectada por VPN	Aumentan errores de estado tras reconexión del túnel.	Verificar rutas de ida/vuelta, política de estados y MTU.
Servidor publicado	Picos de Inserts con límites por origen.	Correlacionar source IP, logs, regla NAT y picos legítimos.
Red con IPv6	Bloqueos In6 sin fallos visibles en IPv4.	Examinar RA, ND, políticas ICMPv6 y rutas.
Failover Multi-WAN	Cambios de gateway y flujos que no se reanudan.	Revisar states vinculados, grupos y NAT de salida.

92.24. Matriz de incidencias y decisiones seguras

Hallazgo	Posibles causas	Primera acción no disruptiva
No crecen los contadores	Tráfico no atraviesa la interfaz o contadores recientemente reiniciados.	Verificar punto de captura y timestamp Cleared.
Inserts muy superior a Removals	Numerosas conexiones nuevas o estados retenidos.	Examinar States Summary y tendencias.
sube memory / state-insert	Falta de recursos o restricción del filtro.	Comprobar límites, RAM y reglas afectadas.
crece state-mismatch	Asimetría, sesiones caducadas, retransmisiones o NAT.	Correlacionar estados, rutas y capturas.
blocked elevado	Tráfico no solicitado, reglas restrictivas o política errónea.	Revisar logs y regla exacta.
cambios bruscos tras recarga	Reset de contadores o modificación del ruleset.	Registrar ventana temporal y cambio aplicado.



Figura 92.4. Secuencia de comprobación no disruptiva y validación posterior al cambio.

92.25. Seguridad, conservación de evidencias y privacidad

pfInfo puede revelar identificadores del host, nombres de interfaces, actividad de VPN, patrones de filtrado, límites y detalles del ruleset. Tratar su salida como información operativa sensible. Antes de facilitarla a terceros, retirar identificadores, nombres de dispositivos, referencias de red, valores de infraestructura, direcciones y contexto que permita reconstruir la topología.

La evidencia debe incorporar fecha y zona horaria, versión de software, hipótesis, captura de referencia, cambios autorizados y resultado de la comprobación, evitando incluir credenciales o paquetes completos si no son indispensables. El tiempo de conservación se define por la política de la organización.

92.26. Lista de comprobación técnica antes de intervenir

Comprobación	Criterio de aceptación
Línea base	Contadores y tasas registrados con hora y cambios recientes.
Alcance	Interfaz, familia IP, ruta y servicio afectados identificados.
Saturación	States, src-nodes, RAM y límites contrastados.
Correlación	States, logs y captura sustentan la hipótesis.
Riesgo	Impacto sobre VPN, NAT, HA y acceso remoto evaluado.
Reversión	Copia y plan de vuelta atrás disponibles.
Cierre	Resultados, acciones y efectos posteriores documentados.

92.27. Glosario

Término	Definición
PF	Motor de filtrado de paquetes con estado utilizado por pfSense.
State	Registro que mantiene el contexto de una conexión o intercambio.
Ruleset	Conjunto de reglas PF aplicado al tráfico.
Anchor	Subconjunto jerárquico de reglas incluido en la estructura de PF.
Source Tracking	Registro de vínculos por origen usado por ciertas políticas.
Timeout adaptativo	Reducción dinámica de la retención de estados al crecer la presión de tabla.
Synproxy / SYN cookies	Mecanismos de defensa y gestión del establecimiento TCP.
Counter / Rate	Medida acumulada frente a actividad relativa al tiempo.

92.28. Referencias técnicas verificables

Netgate — pfInfo: descripción oficial y contadores
Netgate — Firewall & NAT: optimización, límites y timeouts
Netgate — Firewall Fundamentals: funcionamiento stateful
Netgate — Configuring Firewall Rules: límites por regla
Netgate — Viewing Firewall States in the GUI
Netgate — Firewall States Summary
Netgate — Source Tracking States
Netgate — Reset State Table / Source Tracking Table
Netgate — Troubleshooting Firewall Rules
Netgate — State Synchronization (pfsync)
Netgate — Diagnostics menu

93 Diagnostics → pfTop

Tabla de estados · filtros · vistas · NAT · sesiones · análisis operativo

pfTop es una herramienta de lectura dinámica del motor PF que permite localizar conexiones activas, examinar su evolución, ordenar estados por distintos criterios y estudiar su relación con reglas, rutas y traducciones de direcciones. El diagnóstico fiable exige correlacionar sus datos con otras herramientas del cortafuegos.

PRECAUCIÓN La salida puede contener direcciones internas, destinos externos y detalles de actividad. Su consulta no altera estados, pero una exportación o captura de pantalla debe tratarse como información operativa sensible. Evite confundir las filas In/Out con conexiones distintas sin comprobar la traducción NAT.

93.1. Finalidad técnica y ubicación en pfSense Plus

Ruta exacta: Diagnostics → pfTop. A diferencia de Status → Traffic Graph, que presenta caudales inmediatos por interfaz, pfTop se centra en las entradas de la tabla de estados PF y ofrece vistas orientadas a sesiones, reglas, volumen, tasa o antigüedad.

PF evalúa las reglas cuando se inicia un flujo y mantiene información para reconocer paquetes posteriores de la misma comunicación. Esa persistencia explica que la existencia de un estado no demuestre que el servicio de aplicación haya respondido correctamente y que una regla modificada pueda no aplicarse a conexiones ya establecidas.

Figura 93.1 · pfTop como observador de estados

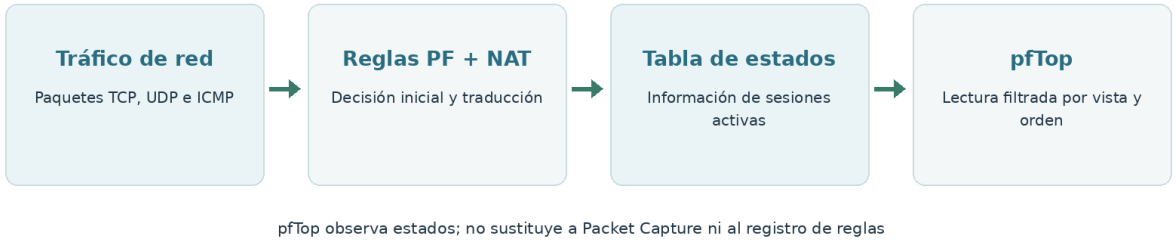


Figura 93.1. Cadena conceptual desde tráfico y reglas PF hasta la inspección de estados con pfTop.

93.2. Estructura de la pantalla y controles visibles

Campo o control	Función	Precaución / uso adecuado
View	Selecciona la perspectiva de presentación de los estados o reglas.	No todas las vistas admiten filtros y ordenación equivalentes.
Filter expression	Restringe los estados que aparecen mediante la sintaxis propia de pfTop.	No confundir con el filtro de texto de Diagnostics → States.
click for filter help	Abre la ayuda de expresiones de filtrado de la propia interfaz.	Consultar si varía la sintaxis de la versión instalada.
Sort by	Ordena por edad, volumen, puertos, direcciones o caducidad según la vista.	Algunos criterios dependen de la información disponible.
Maximum # of States	Limita filas mostradas: 50, 100, 200, 500, 1000 o all.	all puede consumir recursos y dificultar el análisis.
Output	Presenta la salida calculada del estado actual del firewall.	Una lectura puntual no es un histórico ni una captura de paquetes.

93.3. View: las nueve vistas de pfTop

Vista	Qué prioriza	Cuándo resulta útil
default	Tabla equilibrada: protocolo, dirección, origen, destino, estado y contadores.	Primer triaje de una incidencia.
label	Etiquetas y descripciones asociadas a las reglas.	Relacionar tráfico y política de firewall.
long	Filas extendidas y gateway tras destino; requiere anchura.	Correlación de dirección, política y encaminamiento.
queue	Información sobre colas ALTQ y su utilización.	Comprobaciones de Traffic Shaping ALTQ; sin colas puede carecer de datos relevantes.
rules	Reglas de firewall y sus contadores o utilización.	Identificar reglas con actividad destacada.
size	Sesiones que han transferido mayor volumen acumulado.	Descubrir flujos pesados, no necesariamente los más rápidos ahora.
speed	Conexiones con actividad de tasa alta.	Localizar tráfico intenso en la ventana de observación.
state	Vista orientada a los estados de conexión.	Investigar fases TCP y flujos sin respuesta.
time	Estados que llevan más tiempo existiendo.	Detectar sesiones longevas o persistentes.

DIFERENCIA DE VISTAS Los modos de presentación y los criterios peak, rate o size dependen de la versión y de la vista seleccionada. Consultar la ayuda del sistema instalado para confirmar los criterios disponibles.

93.4. Filter expression: sintaxis y alcance

La expresión usa selectores de protocolo, dirección y ámbito de origen o destino. Los ejemplos siguientes utilizan exclusivamente direcciones reservadas para documentación y se basan en las formas descritas en la guía oficial.

Expresión de ejemplo	Qué busca
proto tcp	Estados relacionados con TCP.
proto udp	Estados relacionados con UDP.
src host 192.0.2.25	Estados cuyo origen coincide con ese host.
dst host 203.0.113.80	Estados cuyo destino coincide con ese host.
dst port 443	Estados cuyo puerto de destino es 443.
src net 192.0.2.0/24	Estados cuyo origen pertenece a la red indicada.
in	Estados clasificados como entrantes.
out	Estados clasificados como salientes.

La documentación admite patrones de protocolo (proto), direcciones (src/dst/gw y host/net/port) y sentido (in/out). En expresiones complejas conviene comprobar los ejemplos del enlace «click for filter help» de la versión utilizada antes de asumir precedencias, negaciones o combinaciones no confirmadas.

93.5. Sort by: nueve criterios mostrados

Criterio	Interpretación y decisión
None	Orden natural de la vista, sin imponer un criterio adicional.
Age	Antigüedad acumulada del estado; permite localizar sesiones longevas.

Criterio	Interpretación y decisión
Bytes	Volumen de datos que ha coincidido con el estado; no es bps.
Destination Address	Ordenación por dirección IP de destino.
Destination Port	Ordenación por puerto de destino; útil para agrupar servicios.
Expiry	Tiempo restante de un estado si no se renueva con nuevo tráfico.
Packet	Número acumulado de paquetes observados para ese estado.
Source Port	Puerto de origen asociado al flujo.
Source Address	Ordenación por IP de origen; útil para localizar emisores.

Netgate indica orden descendente en los criterios aplicables. La guía oficial también describe en ciertos contextos Peak, Rate y Size; si no están en el menú de esta versión, no deben tratarse como controles visibles.

93.6. Maximum # of States: 50, 100, 200, 500, 1000 y all

El límite restringe filas presentadas, no la tabla PF real. Mostrar «all» no borra, crea ni amplía estados, pero puede generar una salida grande, tardar en renderizar y exponer más datos. Una búsqueda bien filtrada suele ser más útil que seleccionar indiscriminadamente todas las entradas.

93.7. Cómo leer la cabecera Output

Una salida ilustrativa puede indicar «pfTop: Up State 1-5/5, View: default, Order: bytes». La cabecera identifica el estado general de PF, el tramo de resultados visibles respecto del total considerado, la vista y el orden aplicado. «Up» no verifica por sí solo la salud de la WAN ni la accesibilidad de un servicio.

Figura 93.2 · Una sesión atravesando NAT

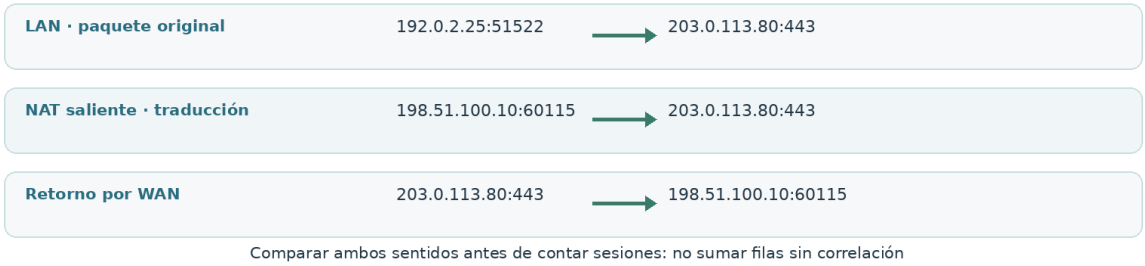


Figura 93.2. Transformación didáctica de una conexión saliente y su retorno cuando existe NAT.

93.8. Columnas PR, DIR, SRC y DEST

Columna	Significado	Precaución de lectura
PR	Protocolo (tcp, udp, icmp, ipv6-icmp, etc.).	El formato de puerto/tipo difiere en ICMP.
DIR	Sentido In u Out mostrado por el motor PF.	El sentido corresponde al punto de vista de la entrada de estado.
SRC	Dirección de origen y, según protocolo, puerto o identificador.	Tras NAT puede aparecer origen original o traducido según la entrada.
DEST	Dirección de destino con puerto o indicador.	Comparar contra reglas, rutas y captura real.

93.9. STATE: evolución TCP, UDP e ICMP

Dos estados separados por dos puntos representan información de los extremos según el seguimiento de PF. No describen un test activo realizado por pfTop y tampoco garantizan el funcionamiento de una aplicación.

Estado representativo	Lectura práctica
ESTABLISHED:ESTABLISHED	Se observa una sesión TCP establecida a ambos lados; validar intercambio y aplicación.
SYN_SENT:...	Se ha intentado iniciar una conexión TCP; si persiste, revisar respuesta SYN/ACK, rutas y filtros.
FIN_WAIT_2 / TIME_WAIT	Estados de cierre TCP; son normales según secuencia y temporizadores.
MULTIPLE:MULTIPLE	Se han visto paquetes UDP en ambos sentidos; no implica sesión de aplicación persistente.
SINGLE:MULTIPLE	El seguimiento UDP tiene distinta actividad en las dos direcciones.
NO_TRAFFIC:SINGLE	Se han observado paquetes únicamente en uno de los sentidos considerados.
NO_TRAFFIC:NO_TRAFFIC	Estado interno asociado a tráfico cuyo seguimiento no equivale a handshake TCP.

INTERPRETACIÓN ICMP e ICMPv6 pueden mostrarse con tipos/códigos entre corchetes o con valores con apariencia de puerto. No son puertos TCP/UDP y no deben analizarse como tales.

93.10. AGE, EXP, PKTS y BYTES

Campo	Qué representa	Error frecuente
AGE	Tiempo transcurrido desde que se creó el estado.	Confundir antigüedad con actividad continua.
EXP	Tiempo restante hasta caducidad si no se recibe más tráfico.	Considerarlo una fecha absoluta de cierre.
PKTS	Paquetes acumulados vinculados al estado.	Usarlo como tasa por segundo.
BYTES	Bytes acumulados asociados al estado.	Afirmar que es consumo en tiempo real o facturación.

Figura 93.3 · Edad, expiración, volumen y tasa

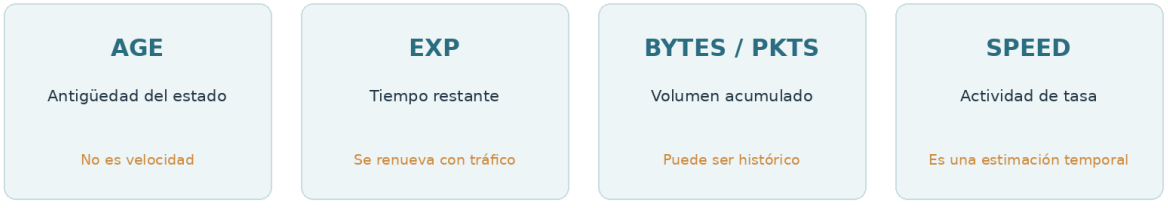


Figura 93.3. Comparación de las métricas que aparecen o se derivan de la lectura de estados.

93.11. Relación entre NAT y aparente duplicación de entradas

Una misma sesión puede aparecer con direcciones y puertos distintos en las rutas de entrada y salida, por la traducción NAT y el seguimiento de PF. Antes de sumar dos filas, compare protocolo, tiempos, tráfico, pares origen/destino y transformación de la dirección. No existe una regla universal de “dos filas por conexión”: depende de la vista, política de estados y disposición de la topología.

93.12. Diagnóstico de conexiones TCP que parecen activas

1. Filtrar por origen, destino o puerto de documentación equivalente al servicio afectado.

2. Seleccionar default o state y comprobar el estado real: SYN_SENT, ESTABLISHED, FIN_WAIT o TIME_WAIT.

3. Contrastar el volumen y los paquetes con el comportamiento esperado del servicio.

4. Revisar Diagnostics → States y Firewall Log para conocer la política y la traducción.

5. Si hay dudas de ida/retorno, capturar paquetes en ambos puntos y verificar el resultado con un cliente real.

93.13. Diagnóstico UDP: actividad sin establecimiento de sesión

UDP carece de handshake de establecimiento como TCP. En pfTop los estados SINGLE o MULTIPLE reflejan lo observado en cada sentido. Para DNS, NTP, telemetría o túneles UDP, una respuesta de aplicación debe comprobarse con el protocolo correspondiente; una entrada MULTIPLE no certifica que el contenido sea válido.

93.14. Tráfico ICMP e ICMPv6 y pruebas de conectividad

El tráfico ICMP puede mantener estados de PF para solicitudes y respuestas. La existencia de estados de ping no implica que haya un problema; un elevado recuento puede reflejar monitorización frecuente. En IPv6, ICMPv6 también interviene en descubrimiento de vecinos, por lo que conviene distinguir mensajes de control local de pruebas de conectividad extremo a extremo.

93.15. Identificación de grandes consumidores frente a grandes tasas

Use size o Bytes para identificar volumen total y speed para localizar tráfico de tasa elevada. Una sesión con muchos bytes y varias horas de antigüedad puede estar inactiva; una transferencia reciente puede ser rápida aunque acumule menos datos. Para conocer promedios históricos, recurra a Status → Monitoring y soluciones de registro de tráfico de mayor duración.

93.16. Integración con reglas, labels y queues

La vista label facilita relacionar actividad con descripciones de reglas; rules ayuda a localizar políticas activas; queue depende de colas ALTQ. No deben confundirse estos datos con limitadores dummynet, que tienen su propia inspección en Diagnostics → Limiter Info. La utilidad de estas vistas depende de la configuración y de los contadores disponibles.

93.17. Multi-WAN, policy routing y salidas inesperadas

En entornos con varios gateways, examine el origen, el destino, el gateway si aparece en long y las reglas aplicadas. Un estado creado antes de una caída WAN puede continuar atado a su interfaz original o afectar a la reconexión; no se debe borrar la tabla completa como primera medida. Contraste con Status → Gateways y la ruta efectiva.

93.18. VPN, NAT y tráfico entre redes remotas

OpenVPN, IPsec y WireGuard pueden encapsular paquetes; pfTop puede mostrar tanto el tráfico exterior del túnel como conexiones internas que cruzan interfaces lógicas, según modo y reglas. Evite sumar el tráfico cifrado y el descifrado para medir ancho de banda facturable. Utilice la vista de estado propia de cada VPN y capturas para establecer el punto exacto de pérdida.

93.19. Detección de uso inesperado y seguridad

Los cambios de volumen, antigüedad o abundancia de estados son indicios, no pruebas de actividad maliciosa. Una comunicación con puerto de administración, mensajes multicast o conexiones a destinos externos puede ser legítima. Verifique el servicio, propietario del equipo, registros y reglas antes de bloquear tráfico o atribuir una causa. Restrinja el acceso a pfTop por los datos operativos que expone.

93.20. Uso desde consola y sesión SSH

El menú de consola ofrece pfTop (opción 9). Desde una shell autorizada puede ejecutarse pftop. La documentación de Netgate indica las teclas h (ayuda), 0–8 (vistas), espacio (actualizar) y q (salir). La salida se adapta al ancho de terminal; en una ventana grande puede mostrar columnas adicionales. El modo consola es interactivo y no debe confundirse con la representación HTML de la GUI.

93.21. Procedimiento empresarial A: aplicación remota sin respuesta

1. Describir el servicio afectado, IP y puerto con direcciones de documentación en las evidencias compartidas.

2. Filtrar el estado TCP o UDP y verificar si aparece sesión con origen correcto.

3. Examinar STATE, sentido y expiración en comparación con los registros de firewall.

4. Comprobar NAT de ida y ruta de retorno del destino.

5. Validar con Packet Capture y prueba del puerto o servicio; documentar la causa y la corrección.

93.22. Procedimiento empresarial B: consumo elevado en la WAN

1. Registrar la velocidad del enlace y la franja temporal observada en Traffic Graph.

2. En pfTop usar speed para una lectura de alta actividad y size/Bytes para volumen.

3. Filtrar las direcciones de origen y distinguir usuarios, servicios y VPN.

4. Correlacionar con ancho de banda en ambas interfaces, sin sumar representaciones NAT de la misma sesión.

5. Guardar la evidencia y planificar una actuación proporcional si existe un uso no autorizado.

93.23. Procedimiento empresarial C: incidencias tras modificar reglas

1. Anotar el cambio y su hora, mantener una vía de acceso de recuperación.

2. Inspeccionar estados anteriores a la modificación y comparar con la nueva política.

3. Revisar si la conexión debería negociarse de nuevo para aplicar una regla o NAT nuevos.

4. Eliminar únicamente los estados afectados, si es posible, desde Diagnostics → States; reservar el reseteo completo para una intervención autorizada.

5. Volver a probar acceso, VPN y servicios críticos, registrando el resultado.

93.24. Procedimiento empresarial D: VPN con tráfico unilateral

1. Comprobar que el túnel VPN informa conexión en su página de estado.

2. Filtrar el flujo interior del túnel entre redes de prueba.

3. Identificar si hay bytes/paquetes en ambos sentidos o actividad aparente solo en uno.

4. Correlacionar con rutas, reglas, NAT VPN y capturas en ambas interfaces.

5. Validar ida y retorno desde los dos extremos antes de cambiar rutas o reiniciar el servicio.

93.25. Matriz de incidencias y siguiente comprobación

Síntoma	Interpretación inicial	Prueba complementaria
No aparece el flujo	No hay estado visible para ese filtro o el flujo no alcanzó PF.	Revisar filtro, interface, reglas y Packet Capture.
SYN_SENT persistente	Falta completar negociación TCP o hay asimetría.	Capturar SYN/SYN-ACK y comprobar ruta de retorno.
ESTABLISHED sin respuesta	TCP está establecido, no necesariamente la aplicación.	Probar el servicio y observar payload permitido.
Muchos bytes, baja tasa	Uso acumulado alto sin actividad proporcional actual.	Comparar speed y datos históricos.

Síntoma	Interpretación inicial	Prueba complementaria
Sesiones muy antiguas	Aplicaciones persistentes o estados que permanecen.	Verificar keepalive, timeout y tráfico real.
Dos filas parecen iguales	Pueden ser direcciones y sentidos correlacionados por NAT.	Comparar puertos traducidos, edades y PF States.
VPN en línea, acceso falla	El túnel no garantiza ruta o permiso a la subred.	Revisar rutas internas, ACL y capturas.
GUI tarda con all	Demasiados estados para representación simultánea.	Reducir máximo y aplicar filtro más estrecho.

Figura 93.4 · Ruta de diagnóstico escalonada

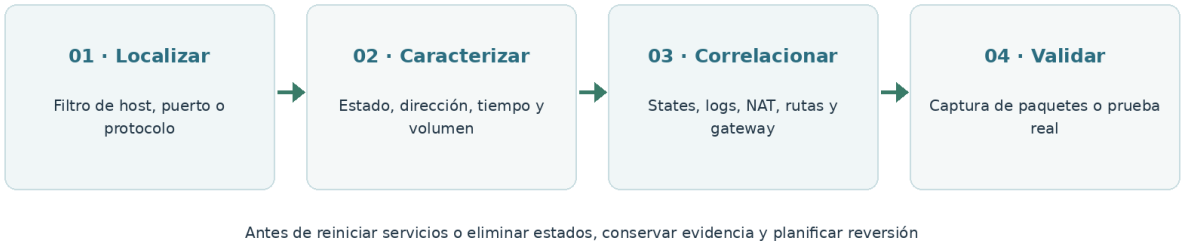


Figura 93.4. Secuencia de diagnóstico sin alterar prematuramente estados o servicios.

93.26. Seguridad y buenas prácticas de operación

pfTop es una herramienta de observación; las operaciones disruptivas, como Reset States, corresponden a otras páginas. Si fuera necesario intervenir, registre configuración previa, alcance, ventana de mantenimiento y mecanismo de reversión. Los datos extraídos de pfTop se consideran sensibles: ocultar IP, puertos de administración, nombres de sedes y detalles VPN antes de compartirlos.

93.27. Lista de comprobación y registro de evidencias

Comprobación	Resultado / evidencia esperada
Objetivo de la consulta	Servicio, usuario autorizado, franja temporal y síntoma definidos.
Vista y orden seleccionados	Indicar si se usó default, speed, size, time u otra vista.
Filtro aplicado	Expresión completa, sin información identificativa en la copia pública.
Correlación	States, Firewall Logs, Gateway, VPN Status o Packet Capture.
Validez de la interpretación	Distinguir tasa, acumulado, antigüedad y temporizador.
Actuación y reversión	Cambios autorizados; seguimiento posterior al cambio.

93.28. Glosario técnico

Término	Definición
PF	Motor de filtrado de paquetes y mantenimiento de estados.
State	Entrada que representa una comunicación conocida por el cortafuegos.
NAT	Traducción de direcciones o puertos observada en el recorrido.
Age	Tiempo transcurrido desde la creación del estado.
Expiry	Contador restante hasta caducidad en ausencia de actividad.

Término	Definición
ALTQ	Mecanismo de priorización mediante colas de tráfico.
Peak/Rate	Medidas de actividad de tasa disponibles según vista o versión.
SYN_SENT	Fase de intento de establecimiento de conexión TCP.

93.29. Análisis guiado de una salida recreada y anónima

Las siguientes filas son sintéticas; están diseñadas para enseñar el método de lectura sin exponer dispositivos reales. Se usan direcciones TEST-NET y prefijos IPv6 de documentación. No representan datos medidos ni recomiendan valores de tráfico concretos.

PR / DIR	Origen → destino (ficticio)	STATE · AGE · EXP	Conclusión limitada
tcp / In	192.0.2.25:51522 → 203.0.113.80:443	ESTABLISHED:ESTABLISHED · 00:05:10 · 23:59:55	TCP establecido; verificar solicitud y respuesta HTTPS.
tcp / Out	198.51.100.10:60115 → 203.0.113.80:443	ESTABLISHED:ESTABLISHED · 00:05:10 · 23:59:55	Posible representación traducida del flujo anterior; correlacionar NAT.
tcp / In	192.0.2.35:50001 → 203.0.113.20:3389	SYN_SENT:CLOSED · 00:00:05 · 00:00:20	No hay establecimiento completo; revisar bloqueo, destino y retorno.
udp / In	192.0.2.40:54000 → 203.0.113.53:53	SINGLE:MULTIPLE · 00:00:02 · 00:00:30	La respuesta DNS debe verificarse en los datos del protocolo.
icmp / In	192.0.2.45 → 192.0.2.1	0:0 · 00:00:12 · 00:00:10	El valor de la columna de estado no es un puerto TCP.
ipv6-icmp / In	2001:db8:1::10 → 2001:db8:1::1	NO_TRAFFIC:SINGLE · 00:00:02 · 00:00:20	Comprobar tipo ICMPv6 antes de atribuirlo a conectividad.

Un par de filas con origen LAN y origen traducido WAN, una edad similar y el mismo destino no basta para afirmar identidad; confirme puertos, interfaz, política de NAT y captura. La interfaz de pfTop no ofrece por sí sola una prueba forense de correlación.

93.30. Plan de lectura progresiva para administradores

Pregunta operativa	Vista y orden sugeridos	Dónde confirmar
¿Qué tráfico es más intenso ahora?	speed; comparar con tráfico de interfaz.	Traffic Graph, Monitoring y tasa medida del enlace.
¿Qué estado transfirió más bytes?	size o default ordenado por Bytes.	Contadores de interfaz y monitorización histórica.
¿Qué conexión lleva mucho tiempo?	time o default ordenado por Age.	States, keepalives de aplicación y temporizadores PF.
¿Por qué TCP no llega a establecerse?	state; filtro proto tcp / destino.	Packet Capture de ida/vuelta y Firewall Log.
¿Qué regla permite un flujo?	label y rules cuando sean útiles.	Firewall Rules, States y descripción de regla.
¿Existe un problema de colas?	queue si se usa ALTQ.	Status → Queues; Diagnostics → Limiter Info para dummynet.
¿Se desvió la salida WAN?	long si muestra gateway y vista de estados.	Status → Gateways, rutas y reglas de policy routing.

CRITERIO DE DECISIÓN Una anomalía de pfTop puede ser consecuencia de una causa externa: ruta asimétrica, aplicación remota sin servicio, MTU, DNS, equipos con firewall local o pérdida del gateway. Confirmar siempre en una segunda fuente antes de cambiar la configuración.

93.31. Selección de la herramienta de observación correcta

pfTop resulta idóneo para explorar flujos activos, pero no responde todas las preguntas de red. Una investigación fiable combina herramientas con diferentes puntos de observación. La siguiente tabla aporta una estrategia reproducible.

Herramienta	Pregunta que resuelve mejor	Límite de interpretación
Diagnostics → pfTop	¿Qué estados están activos, cuánto volumen acumulan y qué patrón muestran?	No certifica rendimiento histórico, accesibilidad de una aplicación ni la causa exacta de un bloqueo.
Diagnostics → States	¿Existe el estado y cómo se relaciona con NAT, interfaces y reglas?	No equivale a una captura de los paquetes intercambiados.
Diagnostics → States Summary	¿Qué IP o pares acumulan más conexiones?	El resumen puede ser costoso en tablas grandes y no mide necesariamente bps.
Status → Traffic Graph	¿Qué ancho de banda se usa ahora en una interfaz?	Muestra actividad inmediata y no un histórico exhaustivo de consumo.
Status → Monitoring	¿Se repite el problema a lo largo de horas o días?	La consolidación histórica pierde resolución temporal.
Status → System Logs, Firewall	¿Qué regla registró un bloqueo o permiso?	Solo incluye coincidencias con registros activados y reglas internas registradas.
Diagnostics → Packet Capture	¿Llegaron paquetes, salieron por la interfaz y hubo retorno?	Debe analizarse con el punto de captura, NAT y sentido correctos.
Diagnostics → pfInfo	¿Hay presión de tabla de estados, errores o límites?	Presenta contadores globales y no identifica una única sesión.
Status → Gateways	¿Está saludable la ruta de salida y su monitor de latencia?	Gateway Online no implica respuesta de todos los servicios remotos.

Si un túnel muestra Connected, pfTop registra estados y el servicio sigue fallando, priorice comprobar rutas de retorno y filtrado específico de la red remota. Solo después de recopilar evidencia se deben considerar modificaciones de firewall, NAT, gateway o la eliminación selectiva de estados.

93.32. Referencias técnicas oficiales

Netgate · pfTop (opciones, vistas, orden y consola)

Netgate · Firewall States

Netgate · Viewing Firewall States in the GUI

Netgate · Firewall States Summary

Netgate · pfInfo

Netgate · Monitoring Bandwidth Usage

Netgate · Troubleshooting NAT Port Forwards

Netgate · Troubleshooting Firewall Rules

Netgate · Reset State Table

Netgate · Firewall & NAT Advanced Options

Netgate · Packet Capture

94 Diagnostics → Ping

ICMP · origen de pruebas · IPv4/IPv6 · VPN · Multi-WAN · diagnóstico reproducible

El diagnóstico de conectividad no consiste únicamente en comprobar si un equipo responde. La utilidad Ping de pfSense Plus permite construir pruebas controladas desde distintas direcciones de origen, distinguir pérdidas de respuesta de fallos de resolución de nombres y aportar evidencias para aislar incidencias de encaminamiento, NAT y redes privadas virtuales.

PRECAUCIÓN Una respuesta satisfactoria demuestra conectividad ICMP desde el origen elegido, no acceso universal a los servicios. Una ausencia de respuesta tampoco prueba por sí sola que el destino esté apagado: puede rechazar ICMP o fallar la ruta de retorno.

94.1. Finalidad técnica y ruta en pfSense Plus

Ruta exacta: Diagnostics → Ping. La herramienta envía solicitudes ICMP Echo desde el propio firewall y muestra respuestas, errores y tiempos de ida y vuelta. Es una prueba activa del plano de datos desde la perspectiva del firewall, no un monitor permanente ni un test iniciado desde un equipo de la LAN.

Netgate documenta también una prueba de ping desde el menú de consola, pero la interfaz web permite escoger familia IP, dirección de origen, número de solicitudes e intervalo. Al usar una dirección de origen explícita, la selección de ruta y los selectores de túnel se deben considerar conjuntamente.



Figura 94.1. Flujo de Echo Request y Echo Reply entre pfSense, la red y un destino ficticio.

94.2. Inventario completo de controles visibles

Control	Valor observado o tipo	Función y consecuencia
Hostname	Campo de texto	Dirección IP o nombre del destino. Es el único campo imprescindible según Netgate.
IP Protocol	Lista; IPv4 seleccionado	Fuerza familia IPv4 o IPv6 cuando el nombre resuelve a ambas.
Source address	Automatically selected (default)	El sistema elige una IP origen basándose en las rutas; seleccionar otra cambia la prueba.
Maximum number of pings	Lista; 3 seleccionado	Número de Echo Requests por ejecución. Predeterminado documentado: 3.
Seconds between pings	Lista; 1 seleccionado	Segundos entre solicitudes. Predeterminado documentado: 1.
Ping	Botón de ejecución	Inicia la prueba y muestra el resultado cuando termina.

Las listas desplegables están cerradas en la imagen de referencia. Por ello no se atribuyen opciones numéricas adicionales ni rangos concretos que no estén visibles o publicados. Los valores por defecto de 3 y 1 segundo están confirmados en la guía oficial.

94.3. Fundamento de ICMP Echo en IPv4 e IPv6

En IPv4, Ping utiliza ICMP Echo Request (tipo 8) y Echo Reply (tipo 0). En IPv6 utiliza ICMPv6 Echo Request (tipo 128) y Echo Reply (tipo 129). Se trata de mensajes de control de red, no conexiones TCP ni pruebas de puerto: una solicitud ICMP no usa 80, 443 ni un puerto UDP como identificador de servicio.

El proceso habitual es: resolver el destino si se indicó un hostname, seleccionar un origen local, decidir ruta y túnel, enviar la solicitud, recibir una respuesta o un error, y resumir tiempos y pérdidas. En cada sentido, ACL, PF, NAT, equipos intermedios y la política ICMP del destino pueden modificar el resultado.

94.4. Hostname: formato y resolución de nombres

Acepta un nombre DNS o una dirección IPv4/IPv6. Para aislar DNS, comenzar por una IP numérica ficticia de prueba o por un destino de diagnóstico expresamente autorizado; después repetir con un nombre. Si la IP funciona y el nombre falla, estudiar DNS Lookup, los servidores configurados, las zonas internas y los registros A/AAAA.

Entrada de ejemplo	Significado	Qué evita concluir precipitadamente
198.51.100.10	IPv4 de documentación	No requiere resolver un nombre; el destino debe existir en el entorno de ensayo.
2001:db8:1::10	IPv6 de documentación	Prueba independiente de IPv4; necesita encaminamiento IPv6.
host.example.com	FQDN reservado	Permite comprobar resolución de nombres y conectividad conjunta.

94.5. IP Protocol: forzar IPv4 o IPv6

Si un hostname dispone de registros A y AAAA, esta opción determina la familia de dirección con la que se ejecuta la prueba. Elegir IPv4 no valida IPv6, y viceversa. Para comparar los dos protocolos se requieren ejecuciones separadas con la misma política de destino y un origen pertinente para cada familia.

NOTA IPv6 Las direcciones link-local fe80::/10 solo tienen alcance de enlace. Es posible que una prueba requiera identificar su interfaz o zona (por ejemplo, fe80::1%em0). La sintaxis y disponibilidad exactas del origen dependen de la interfaz y versión instaladas.

94.6. Source address: la selección crítica

Con Automatically selected (default), FreeBSD elige la dirección de origen que considera adecuada según sus rutas. La selección manual permite imitar el origen de una LAN, interfaz VPN o dirección virtual disponible en el firewall, y diagnosticar por qué una conectividad funciona desde un punto de vista y falla desde otro.

Una dirección origen seleccionada no fuerza por sí sola una interfaz física ni equivale a una regla de policy routing. El encaminamiento continúa dependiendo de las rutas, selectores IPsec, reglas PF y configuración de gateways; para comprobar el recorrido se correlaciona la prueba con Diagnostics → Routes y Packet Capture.

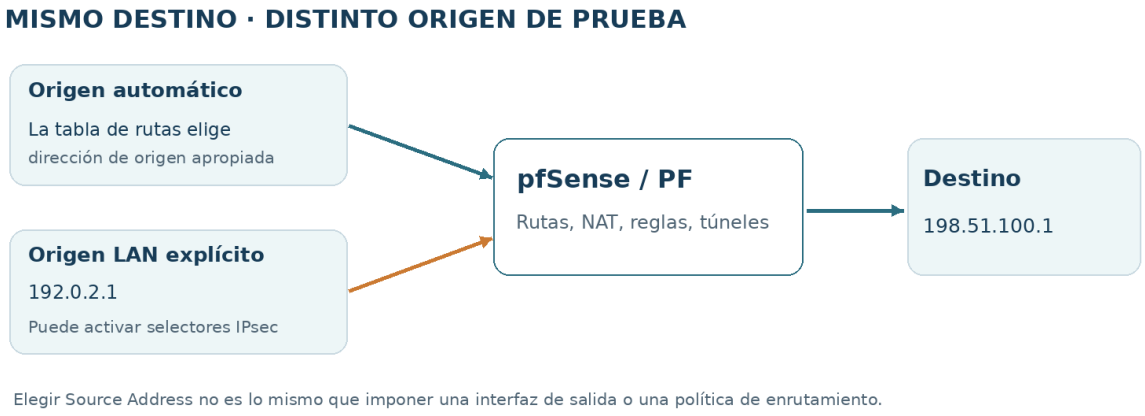


Figura 94.2. Comparación entre origen automático y origen LAN explícito ante el mismo destino.

94.7. Maximum number of pings: cantidad y valor predeterminado

El valor predeterminado es 3 solicitudes. Una prueba tan corta ayuda en el primer diagnóstico, pero no permite medir con precisión pérdidas intermitentes. Aumentar el número de intentos proporciona más observaciones, a costa de prolongar la ejecución y generar más tráfico. Ante destinos que no responden, Netgate recuerda que una prueba con más paquetes tarda más en terminar.

En IPsec es habitual que el primer ping se pierda mientras se negocia o se establece la asociación, especialmente si el túnel era inactivo. Netgate aconseja al menos tres solicitudes y repetir si es preciso antes de concluir que el enlace falla.

94.8. Seconds between pings: cadencia de las sondas

La pantalla muestra 1 segundo como valor seleccionado y Netgate lo documenta como predeterminado. Espaciar las solicitudes permite estudiar variaciones de latencia y evitarlas demasiado concentradas. La interfaz no sustituye a un monitor continuo de calidad; para observación prolongada deben utilizarse Status → Gateways y Monitoring.

94.9. Botón Ping y secuencia de ejecución

1. Introducir el destino autorizado en Hostname, preferiblemente primero como dirección numérica.
2. Elegir IPv4 o IPv6 de forma explícita y, si hace falta, una Source address que corresponda al escenario de prueba.
3. Mantener inicialmente tres solicitudes espaciadas un segundo; ampliar la muestra solo si el problema es intermitente.
4. Pulsar Ping y permanecer en la página hasta que aparezca el resultado, tal como indica Netgate.
5. Guardar la evidencia sin divulgar IP reales, nombres de equipos, tokens ni datos internos.

La herramienta no modifica la configuración del firewall ni crea una regla de autorización. Puede generar tráfico ICMP y eventos en logs dependiendo de las políticas de registro, por lo que la ejecución desde orígenes sensibles debe formar parte de un diagnóstico autorizado.

94.10. Salida del comando: respuestas, errores y resumen

Elemento habitual	Qué informa	Lectura adecuada
Reply / bytes / seq	Respuesta individual y secuencia	La respuesta demuestra que la solicitud concreta regresó.
time / RTT	Duración de ida y vuelta	No es el tiempo en un solo sentido ni el tiempo de respuesta HTTP.
TTL o Hop Limit	Límite de saltos restante del paquete recibido	No debe confundirse con un recuento exacto de routers.
packets transmitted/received	Solicitudes enviadas y respuestas recibidas	Permite calcular pérdida en la muestra.
min/avg/max (y desviación si se muestra)	Resumen temporal	Picos, dispersión y tendencia; dependen de los paquetes respondidos.
Timeout / unreachable	Ausencia de respuesta o rechazo de red	Requiere correlación con ruta, firewall y captura.

94.11. Pérdida de paquetes, latencia y variación

Pérdida (%) = (solicitudes enviadas − respuestas recibidas) / solicitudes enviadas × 100. El RTT incluye salida, viaje, procesado remoto y regreso. La variación entre muestras ayuda a sospechar colas, congestión, Wi-Fi inestable o problemas de proveedor, pero no prueba por sí sola la causa.

En una muestra ilustrativa de 7 solicitudes con 6 respuestas, la pérdida es 14,3 %. Con solo tres paquetes, una única pérdida equivale ya a 33,3 %; por eso no se debe tratar una muestra pequeña como diagnóstico estadístico definitivo.

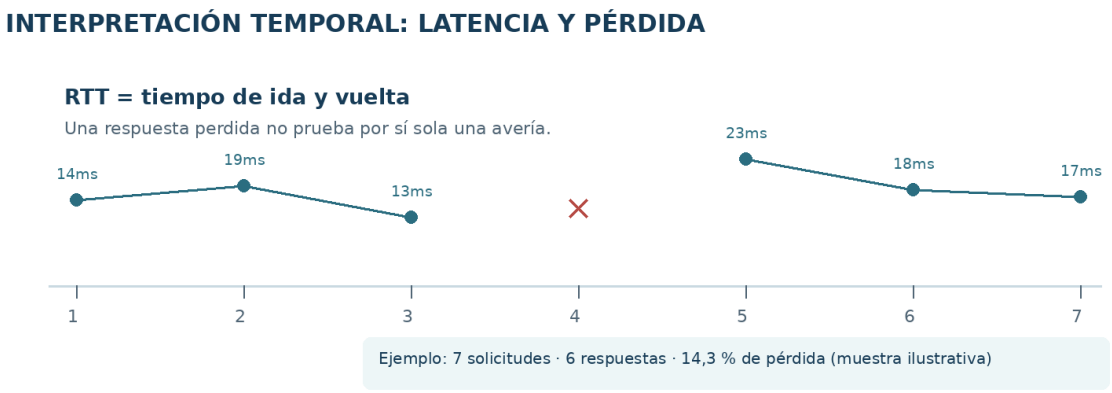


Figura 94.3. Ejemplo ilustrativo de RTT por solicitud y una respuesta ausente.

94.12. Mensajes comunes y su interpretación técnica

Resultado	Hipótesis iniciales	Siguiente evidencia
Destination Host Unreachable	Ruta, ARP/NDP o rechazo por un router	Routes, ARP Table/NDP Table, Packet Capture.
No route to host / Network unreachable	Falta ruta o interfaz adecuada	Diagnostics → Routes; estado y puerta de enlace.
Request timeout / 100% loss	Filtrado, host silencioso, retorno ausente o destino caído	Captura en entrada/salida y prueba TCP autorizada.
Temporary failure in name resolution	DNS no disponible o nombre sin resolución	DNS Lookup y registros del resolver.
Respuesta con RTT elevado	Saturación, ruta larga o destino sobrecargado	Comparar gateways, observación temporal y otros destinos.
No buffer space available	Ruta/estado obsoleto o falta de buffers entre otras causas	Netgate: rutas, NIC, estados PF y memoria; no reiniciar a ciegas.

94.13. Ping no prueba puertos, aplicaciones ni permisos

ICMP Echo no valida TLS, HTTP, autenticación, acceso a SQL Server o la negociación de una VPN. Un equipo puede responder a Ping y mantener cerrado TCP/443; otro puede responder en TCP/443 y bloquear ICMP. Para una prueba de servicio utilizar Diagnostics → Test Port, registros de aplicación y, si procede, Packet Capture.

94.14. Prueba IPv4 frente a prueba IPv6

Cuando una aplicación falla solo con IPv6, comprobar que pfSense tiene ruta IPv6, la interfaz cuenta con dirección válida y que ICMPv6 esencial no se ha bloqueado indiscriminadamente. NDP y Path MTU Discovery dependen de mensajes ICMPv6 distintos de Echo; bloquear todo ICMPv6 puede romper funciones básicas de red.

Cuando aparece una dirección link-local, el ámbito forma parte del significado de la dirección: un mismo valor fe80:: puede existir en varios enlaces y sin referencia de interfaz resulta ambiguo.

94.15. Multi-WAN: diferencia entre origen y salida real

Netgate documenta que el tráfico originado por servicios del propio firewall suele seguir el gateway predeterminado salvo rutas específicas. El balanceo por reglas para clientes LAN no implica que un ping creado por pfSense use un grupo de gateways. Por ello la elección manual de Source address no demuestra que el paquete haya salido por la WAN prevista.

1. Comprobar Status → Gateways y que el monitor de cada enlace esté Online.
2. Examinar Diagnostics → Routes y el gateway predeterminado actual.
3. Ejecutar Ping primero con origen automático y después con una dirección origen pertinente para el enlace bajo prueba.

4. Verificar con Packet Capture en la WAN correspondiente si realmente se transmitió Echo Request y regresó Echo Reply.
5. Correlacionar la prueba con reglas, NAT y el funcionamiento de dpinger sin alterar conexiones activas.

94.16. VPN IPsec: validación de tráfico entre sedes

Para túneles IPsec de modo tradicional, Netgate recomienda elegir una IP de origen que pertenezca a la red local Phase 2 y un destino de la red remota Phase 2. Si el ping usa la WAN del firewall como origen, puede quedar fuera de los selectores IPsec y no atravesar el túnel.

Ejemplo enteramente ficticio: Phase 2 local 192.0.2.0/24, Phase 2 remota 198.51.100.0/24. Ping desde 192.0.2.1 hacia 198.51.100.1. Después consultar Status → IPsec, IKE/CHILD SA y capturas para confirmar si el tráfico coincide con la política del túnel.

PRECAUCIÓN El método anterior se refiere al IPsec basado en políticas. En IPsec VTI, la comprobación depende también de interfaces asignadas, rutas y gateways; no se debe aplicar mecánicamente el mismo razonamiento a todas las topologías.

94.17. OpenVPN y WireGuard: pruebas desde el firewall

En OpenVPN, Netgate aconseja comprobar primero con origen interno (por ejemplo, LAN) y repetir con origen automático si es necesario. Si la prueba desde la interfaz del túnel funciona pero no desde la LAN, revisar rutas, redes autorizadas y reglas de retorno en el extremo remoto. En WireGuard, Allowed IPs identifica prefijos asociados a peers, pero las rutas del firewall y las reglas continúan siendo necesarias.

Una VPN puede mostrar «Connected» y aun así no proporcionar acceso a determinados hosts: la conexión del plano de control no demuestra alcance de todas las subredes ni funcionamiento de las aplicaciones.

94.18. Firewall y NAT: lo que demuestra la prueba

Los pings iniciados por pfSense tienen una perspectiva diferente de los iniciados por un cliente LAN. Una prueba desde la IP LAN puede ayudar a diagnosticar NAT de salida, pero no reproduce exactamente una sesión real de un equipo con una dirección privada distinta. Los resultados deben contrastarse con Firewall → NAT, la tabla de estados y los registros.

Para diferenciar pérdida en origen, filtrado PF o pérdida aguas arriba, capturar en las interfaces pertinentes y buscar Echo Request y Echo Reply con sus direcciones antes y después de NAT.

94.19. Método diagnóstico por capas y evidencias

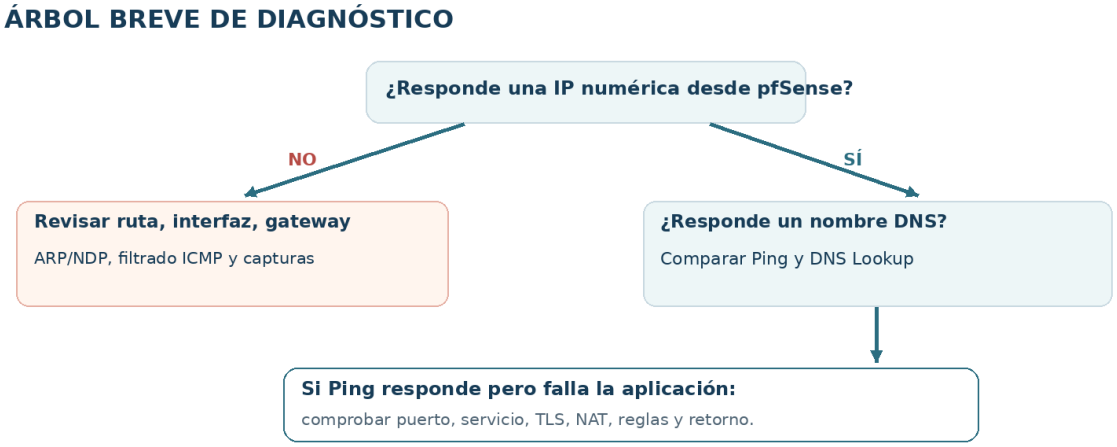


Figura 94.4. Árbol de decisión para distinguir fallos de IP, DNS y aplicaciones.

Prueba ordenada	Si funciona	Si falla
Ping al propio gateway conectado	La capa 3 inmediata probablemente responde	Revisar interfaz, ARP/NDP, enlace, VLAN y gateway.
Ping a IP remota autorizada	Hay respuesta ICMP hacia el destino	Comprobar ruta, salida WAN, políticas ICMP o retorno.

Prueba ordenada	Si funciona	Si falla
Ping a nombre del mismo destino	DNS y Echo funcionan juntos	Separar búsqueda DNS de transporte ICMP.
Test Port al servicio requerido	Existe respuesta TCP en el puerto probado	Comprobar servicio, NAT, políticas y filtrado.
Packet Capture en dos puntos	Permite ubicar ida y respuesta	Identificar dónde desaparecen los paquetes.

94.20. Procedimiento: pérdida completa de conectividad desde LAN

1. Desde el cliente, validar IP, máscara, puerta de enlace y DNS asignados.
2. Probar cliente → IP LAN de pfSense y después cliente → IP remota, separando ambos resultados.
3. Desde pfSense, ejecutar Ping hacia gateway WAN, IP remota y el propio cliente con el origen apropiado.
4. Consultar ARP/NDP, Routes, Status → Interfaces y Gateways.
5. Usar Packet Capture si no está claro en qué enlace desaparece Echo Request o su respuesta.
6. Corregir la causa identificada y repetir las mismas pruebas; documentar antes y después.

94.21. Procedimiento: una sede remota no responde por IPsec

1. Confirmar que Phase 1 e Phase 2 están configuradas y que las SA pertinentes existen, sin confundir IKE SA con flujo útil.
2. Comprobar selectores local/remoto de Phase 2 y el direccionamiento del destino.
3. Elegir en Ping la dirección LAN local contemplada por esos selectores.
4. Realizar tres solicitudes; repetir si la primera negociación ocasiona pérdida inicial.
5. Comprobar reglas IPsec, rutas remotas, filtros ICMP y retorno; confirmar en captura.

94.22. Procedimiento: latencia alta o pérdida intermitente

1. Registrar destino, familia IP, origen y hora de la prueba.
2. Repetir muestras comparables variando solo un factor: origen, destino o horario.
3. Contrastar con RTT/Loss de Status → Gateways y gráficas de Monitoring, sin atribuir automáticamente la causa al firewall.
4. Consultar utilización de interfaz, errores NIC y colas/limitadores si están configurados.
5. Comprobar si la latencia afecta solo a ICMP o también a conexiones de aplicación.

94.23. Procedimiento: un nombre falla pero la IP responde

1. Anotar la IP que corresponde al destino y probarla con Ping.
2. Ejecutar Diagnostics → DNS Lookup para el FQDN y revisar registros A/AAAA.
3. Revisar DNS Resolver, DNS Forwarder y DNS entregado por DHCP/DHCPv6.
4. Repetir la prueba por IPv4 y por IPv6 para descubrir comportamientos distintos.
5. Validar la aplicación real: un DNS correcto no demuestra que su puerto esté accesible.

94.24. Consola y alternativas de ejecución

La prueba también está disponible en el menú de consola. En FreeBSD, desde una consola autorizada se puede utilizar un comando de lectura como «ping -c 3 198.51.100.1» o fijar origen con «ping -S 192.0.2.1 198.51.100.1». Los valores mostrados son de documentación y solo producirán respuestas si se configura un laboratorio con esos destinos.

La sintaxis de IPv6 y la disponibilidad de ping6 pueden depender de la versión del sistema; la interfaz gráfica evita asumir opciones de consola no verificadas para la versión concreta. Evitar comandos indefinidos en Diagnostics → Command Prompt.

94.25. Integración con otras pantallas de diagnóstico

Herramienta	Qué añade a Ping	Uso complementario
DNS Lookup	Separación entre resolución y transporte	Nombres que fallan aunque la IP responde.
Routes	Selección de gateway y prefijo	Confirmar ruta efectiva y errores de default gateway.
ARP Table / NDP Table	Resolución de vecinos	Pérdidas en el segmento local y vecinos incompletos.
Traceroute	Saltos y recorrido aproximado	Comparar caminos y último salto visible.
Packet Capture	Paquetes antes/después de filtrado y NAT	Verificación de ida, respuesta y traducción.
Test Port	Respuesta TCP del servicio	Cuando la app falla pese a Ping positivo.
Status → Gateways	Latencia/pérdida monitorizada	Correlación temporal y operación Multi-WAN.
Status → IPsec/OpenVPN	Plano de control de VPN	Túnel declarado activo sin acceso real.

94.26. Escenarios empresariales y criterios de aceptación

Escenario	Prueba esencial	Criterio de aceptación
Sede principal / filial	Origen LAN por IPsec + destino LAN remoto	Echo Reply y conectividad del servicio requerido.
Internet con doble WAN	Ping/captura por cada circuito	Salida y retorno por el enlace previsto.
Wi-Fi de invitados	Cliente invitado + DNS + recurso permitido	Acceso permitido sin romper segmentación.
Monitorización de proveedor	IP autorizada cercana y externa	Comparar pérdida/RTT y verificar falsa alarma.
IPv6 en LAN	Destino IPv6 + dirección origen adecuada	NDP, rutas IPv6 y respuesta consistentes.
Saturación de red	Muestras equivalentes en horas de carga	Evidencia temporal reproducible, no una única prueba.

94.27. Seguridad, rendimiento y límites metodológicos

Aunque una ejecución normal genera poco tráfico, un número excesivo de paquetes o una repetición agresiva puede alterar sistemas con restricciones de ICMP. Las mediciones deben dirigirse a destinos propios o autorizados y respetar políticas de operación. No realizar cambios en reglas de firewall, gateways o VPN solo para obtener una respuesta ICMP sin evaluar sus efectos.

Registrar resultados mínimos necesarios. Ocultar identificadores operativos en documentos públicos; una captura de Ping puede revelar direccionamiento, rutas internas, DNS, nombres de sedes y presencia de servicios. Para investigación formal, conservar evidencias en un sistema de acceso restringido.

94.28. Ficha de recogida de evidencias

Dato	Anotación de ejemplo no real
Fecha/hora y ventana	Fecha, zona horaria, inicio y fin de prueba.
Destino	198.51.100.10 / host.example.com
IP Protocol / Source	IPv4 / 192.0.2.1
Número / intervalo	3 solicitudes / 1 segundo
Resultado	Respuestas, pérdida, min/avg/max RTT.

Dato	Anotación de ejemplo no real
Ruta/túnel esperado	WAN principal, WAN secundaria o selectores IPsec.
Confirmación adicional	Routes + Packet Capture + Test Port.
Acción y reversión	Cambio autorizado; prueba posterior equivalente.

94.29. Glosario técnico

Término	Definición esencial
ICMP / ICMPv6	Protocolos de control para errores, diagnóstico y funciones de red.
Echo Request / Reply	Par de mensajes de solicitud y respuesta usados por Ping.
RTT	Tiempo total de ida y vuelta de la sonda.
Packet loss	Porcentaje de respuestas no recibidas durante la muestra.
Source Address	Dirección IP local utilizada como origen del paquete.
Gateway	Siguiente salto utilizado para destinos fuera del enlace.
Selector IPsec	Prefijo local/remoto que determina tráfico sujeto a política IPsec.
NAT	Traducción de direcciones y, según regla, puertos.
Hop Limit / TTL	Límite de saltos de un paquete IP.
FQDN	Nombre DNS completo que identifica un recurso.

94.30. Referencias oficiales y normativas

Netgate · Ping Host

Netgate · Troubleshooting Network Connectivity

Netgate · Testing IPsec Connectivity

Netgate · Troubleshooting OpenVPN

Netgate · Troubleshooting Multi-WAN

Netgate · Multi-WAN Terminology and Concepts

Netgate · Gateway Settings

Netgate · Troubleshooting No Buffer Space Errors

Netgate · IPsec Client Routing and Gateway Considerations

Netgate · Verifying Multi-WAN Functionality

RFC 792 · Internet Control Message Protocol

RFC 4443 · Internet Control Message Protocol (ICMPv6)

95 Diagnostics → Reboot

Reinicio normal · reroot · ZFS Boot Environments · continuidad y recuperación

Reiniciar un firewall afecta simultáneamente al encaminamiento, la inspección de estados, la traducción NAT y los servicios de red que dependen de él. La pantalla Diagnostics → Reboot ofrece métodos diferentes y, en sistemas compatibles, la selección temporal de un entorno de arranque ZFS. Este capítulo aborda la decisión técnica, la ejecución segura y la validación completa del servicio.

PRECAUCIÓN CRÍTICA El botón Submit ejecuta el reinicio inmediatamente. Antes de utilizarlo en producción, disponer de un respaldo actualizado, autorización, acceso alternativo y un procedimiento de recuperación. Un reinicio remoto sin consola puede dejar el sistema inaccesible.

95.1. Finalidad, alcance y ubicación de la pantalla

Ruta visible en la interfaz: Diagnostics → Reboot. La documentación de Netgate utiliza también el nombre Diagnostics → Reboot System para la misma funcionalidad. Se trata de una acción administrativa de impacto alto, no de una consulta de estado.

El reinicio termina las sesiones de administración y vuelve a iniciar los servicios. Durante la interrupción pueden dejar de responder NAT, VPN, DHCP, DNS, monitorización, rutas dinámicas y los flujos en la tabla de estados. El tiempo hasta recuperar el servicio depende del hardware, los discos, la versión, los paquetes y el diseño de la red.



Figura 95.1. Contraste operativo entre reinicio normal y Reroot sin recarga de kernel.

95.2. Inventario exacto de los controles visibles

Elemento observado	Valor mostrado	Función y comportamiento
Boot Environment	default (Current, Next)	Selecciona un entorno ZFS para el siguiente arranque, cuando existe soporte. La entrada visible es el entorno actual y previsto.
Reboot Method	Normal Reboot	Selecciona el procedimiento de reinicio. La ayuda de la pantalla cita también Reroot.
Submit	Botón azul	Inicia la operación seleccionada. No es un botón para guardar ajustes diferidos.
Icono de ayuda	? en la cabecera	Acceso a ayuda contextual, según la versión y la interfaz.
Textos de ayuda	Bajo ambas listas	Indican selección temporal del entorno y comportamiento de las modalidades.

Las dos listas desplegables están cerradas en la referencia: no se atribuyen opciones o nombres adicionales como si se hubieran visto. Las modalidades adicionales descritas en documentación oficial se identifican expresamente como condicionales según versión, arquitectura y sistema de archivos.

95.3. Boot Environment: qué se selecciona realmente

Un ZFS Boot Environment (BE) es un entorno de arranque que contiene un conjunto consistente de datos del sistema derivados de instantáneas y clones ZFS. Permite ensayar una actualización o revertir un estado del sistema sin reinstalar. Esta función es exclusiva de pfSense Plus a partir de 22.05 en instalaciones compatibles con ZFS; no debe presumirse disponible en CE o en todos los equipos.

La opción presentada en Diagnostics → Reboot activa el entorno elegido solamente para el próximo arranque. Al reiniciar otra vez, el sistema vuelve al entorno marcado como predeterminado, salvo que se haya cambiado la selección persistente por otro medio. La selección permanente se gestiona desde System → Boot Environments.

ALCANCE Seleccionar un BE no equivale a restaurar exclusivamente config.xml, ni garantiza que todos los datos que residen en otros datasets o dispositivos queden revertidos. Antes de un cambio importante, conservar una copia de configuración externa.



Figura 95.2. Secuencia de activación temporal y regreso al entorno predeterminado.

95.4. Lectura de “default (Current, Next)”

La anotación Current identifica el entorno desde el que está ejecutándose el sistema; Next señala el entorno programado para el siguiente arranque. Cuando ambas etiquetas aparecen junto a default, el sistema utiliza actualmente ese entorno y prevé volver a él. No significa que exista una copia adicional lista para restaurar.

Si hay varios entornos, consultar System → Boot Environments para revisar nombre, versión base, fecha, espacio y cuál está activo o seleccionado. La lista puede variar según soporte y cantidad de clones presentes. Evitar seleccionar un entorno antiguo sin comprobar cambios de configuración y compatibilidad de paquetes.

95.5. Normal Reboot: reinicio completo

Normal Reboot termina ordenadamente la actividad del sistema, reinicia el sistema operativo y comienza de nuevo el arranque con inicialización del hardware y carga del kernel. Es el método siempre disponible según Netgate y el adecuado cuando debe cargarse un kernel distinto, activarse un entorno ZFS mediante un arranque real o reinicializar componentes del hardware.

Recomendaciones: programarlo en una ventana con mantenimiento comunicado; validar el acceso por consola; asegurar que los cambios de red y firewall han sido aplicados; y comprobar después la negociación de enlaces y todos los servicios críticos. No debe asumirse que elimina de forma permanente un error de configuración o un defecto de hardware.

95.6. Reroot: reinicio de procesos sin recargar kernel

Reroot finaliza los procesos, remonta los sistemas de archivos y ejecuta la secuencia de inicio. Es más rápido que un reinicio completo porque evita reinicializar hardware, recargar el kernel y repetir el descubrimiento de dispositivos. Aun así, interrumpe la webGUI, las VPN, el procesamiento por procesos de usuario y otros servicios; debe tratarse como una parada operacional.

Puede resultar útil para reiniciar en conjunto servicios y configuración de arranque sin necesitar un ciclo completo de hardware. No es el método correcto para activar un nuevo kernel ni debería utilizarse como sustituto fiable de un arranque real al escoger otro BE. Si el problema implica controladores, detección de interfaces, kernel o hardware, preferir Normal Reboot.

NO CONFUNDIR Reroot no es simplemente reiniciar la webGUI, ni conserva transparentemente todas las conexiones activas. La interrupción puede ser menor, pero debe planificarse y validarse.

95.7. Comparación técnica y selección del método

Criterio	Normal Reboot	Reroot
Kernel	Se recarga.	Permanece cargado.
Hardware / controladoras	Se reinicializan durante el arranque.	No se reinicializan por el procedimiento.
Procesos y servicios	Se detienen y vuelven a iniciar.	Se terminan y vuelven a iniciar.
Montaje de sistemas de archivos	Arranque completo.	Desmontaje/remontaje y secuencia de inicio.
Cambio de entorno ZFS	Método apropiado para arrancar un BE diferente.	No activa un kernel diferente.
Impacto en red y VPN	Interrupción esperada.	Interrupción esperada, potencialmente más corta.
Uso preferente	Actualización, diagnóstico de kernel, arranque completo.	Reinicio global del entorno de usuario sin cambio de kernel.

95.8. Otras modalidades documentadas, no visibles en la lista cerrada

Modalidad condicional	Objetivo	Restricción y riesgo
Reboot into Single User Mode	Arranque mínimo para intervención avanzada.	Requiere consola presencial/serial; no ofrece servicios de red. No compatible con ARM. En ZFS puede requerir limpieza manual de nextboot.
Reboot with File System Check	Ejecutar comprobación intensiva con fsck.	No compatible con ARM ni ZFS según Netgate. No ejecutar como alternativa genérica de mantenimiento.
Otras variantes por plataforma	Puede cambiar la lista disponible.	Confirmar la selección real en el desplegable de la versión instalada.

La documentación de Netgate advierte que Single User Mode puede exigir intervención manual y conocimientos avanzados de FreeBSD. No debe seleccionarse si el único acceso es remoto o si no se dispone de una consola operativa. Las opciones que no sean compatibles con la plataforma pueden no aparecer en la GUI.

95.9. Submit: efecto inmediato, sesiones y confirmación

Tras escoger Boot Environment y Reboot Method, pulsar Submit inicia el reinicio inmediatamente, según la guía oficial. La sesión web se desconectará. Si el navegador continúa mostrando una pantalla anterior, no debe concluirse que el firewall se ha quedado congelado: contrastar el progreso con la consola y el estado de interfaces, no pulsar repetidamente el botón.

Guardar antes las evidencias y la configuración. Si se accede por SSH desde una VPN que atraviesa el firewall, esa vía se perderá durante el proceso; la sesión de SSH no es una consola fuera de banda. Un equipo con administración crítica debe contar preferiblemente con consola serial o acceso OOB independiente.

95.10. Plan previo de mantenimiento: comprobaciones

Comprobación	Por qué importa	Evidencia mínima
Copia de configuración externa	Permite recuperar cambios o reinstalar.	XML protegido, fecha y lugar seguro.
Acceso alternativo	Evita bloqueo tras perder GUI o VPN.	Consola probada y credenciales autorizadas.

Comprobación	Por qué importa	Evidencia mínima
Estado de enlaces y rutas	Detecta problemas anteriores al reinicio.	Gateways, interfaces y rutas.
VPN y servicios críticos	Define el servicio que debe volver a funcionar.	Sesiones, DNS, DHCP, autenticación.
HA y dependencias	Evita apagar el único nodo operativo.	CARP MASTER/BACKUP y pfsync.
Ventana y autorización	Coordina impacto de usuarios y sedes.	Incidencia aprobada y plan de reversión.

95.11. Procedimiento 1: reinicio normal desde la GUI

1. Registrar el estado del sistema en Status → Dashboard: versión, uptime, Boot Environment, gateways, interfaces y VPN.

2. Descargar una copia actual desde Diagnostics → Backup & Restore y confirmar acceso a consola o administración fuera de banda.

3. Verificar que no existe una actualización en curso ni una restauración parcial pendiente de aplicar.

4. Abrir Diagnostics → Reboot; elegir default (Current, Next) si no se desea probar un BE diferente y Normal Reboot.

5. Pulsar Submit una sola vez. Supervisar el arranque por consola y no interrumpir la alimentación.

6. Tras recuperar la GUI, ejecutar la matriz de validación de este capítulo y documentar cualquier diferencia.

95.12. Procedimiento 2: Reroot controlado

1. Confirmar que no hay un cambio de kernel, una actualización que exige reinicio completo ni problemas que requieran reinicializar dispositivos.

2. Preparar acceso alternativo y medir una línea base de interfaces, servicios, estado de VPN y conectividad.

3. Seleccionar Reroot únicamente si está ofrecido por la plataforma y el objetivo es reiniciar la secuencia de procesos.

4. Pulsar Submit y monitorizar los registros o la consola. Validar los mismos servicios que con un reinicio completo.

5. Si la avería persiste, no repetir sin análisis: contrastar logs, rutas, estado de hardware y necesidad de Normal Reboot.

95.13. Procedimiento 3: prueba temporal de otro Boot Environment

Preparar una copia externa y verificar que el equipo tiene soporte ZFS BE y que la entrada elegida tiene versión adecuada. Desde System → Boot Environments revisar el entorno previsto y la política de arranque. Desde Diagnostics → Reboot escoger el BE de prueba y Normal Reboot, y luego verificar el valor Current en Dashboard y Boot Environments.

En el siguiente reinicio, salvo modificación persistente en System → Boot Environments, el sistema volverá al entorno predeterminado. Documentar el resultado de la prueba y evitar editar o eliminar BE en uso sin la comprobación correspondiente. El cambio de versión puede alterar paquetes y configuraciones; probar tanto la conectividad como las funciones de administración.

95.14. Reinicio desde el menú de consola

Netgate documenta la opción de menú Reboot system (habitualmente 5). Acceder por consola local, serial o una sesión autorizada con privilegios; elegir la opción y después la modalidad ofrecida por el equipo. La numeración puede variar por versión. Los métodos avanzados Single User y filesystem check requieren una confirmación diferenciada en mayúsculas.

La consola no convierte la operación en inocua: si se accede por SSH a través de una ruta dependiente del firewall, la comunicación puede perderse. El medio más seguro para recuperar un fallo grave de boot es una consola independiente del servicio que se está reiniciando.

95.15. Alta disponibilidad: CARP, pfsync y sincronización XMLRPC

En un clúster pfSense, CARP anuncia las IP virtuales y decide quién atiende el tráfico, pfsync comparte los estados de conexiones y XMLRPC replica partes de la configuración. Estas funciones son complementarias. Antes de reiniciar el nodo principal, verificar que el secundario puede asumir el servicio y que el intercambio de estados es saludable.

Netgate documenta que CARP maintenance mode permite ceder el rol y persiste a través de reinicios. En cambio, el apagado temporal de CARP no persiste. No poner simultáneamente ambos nodos en mantenimiento; después de reiniciar, revisar VIP, demotion, estados y recuperación de rutas.



Figura 95.3. Secuencia conceptual de cesión, reinicio y comprobación de HA.

95.16. Efectos sobre VPN, NAT y estados de conexión

Componente	Qué puede suceder	Comprobación posterior
OpenVPN / WireGuard / IPsec	Se corta la sesión y debe renegociarse o restablecerse.	Status de la VPN, logs y pruebas de acceso a redes concretas.
PF y tabla de estados	Se reconstruyen reglas; se pierden estados locales durante reinicio normal.	pfInfo, States, Filter Reload y aplicaciones.
NAT y redirecciones	Las reglas vuelven desde la configuración.	Comprobar servicio expuesto desde un origen externo autorizado.
Multi-WAN	Puede cambiar gateway elegido según salud y prioridades.	Status → Gateways, rutas, monitorización y política de salida.
Rutas dinámicas	Las vecindades pueden necesitar renegociación.	Tabla Routes y estados del protocolo instalado.

Un estado de la VPN “Connected” no prueba acceso a todas las subredes. Tras reiniciar, verificar negociación, encaminamiento de ida y retorno, reglas en interfaces de VPN y resoluciones DNS internas; repetir pruebas desde un cliente real, no solo desde el firewall.

95.17. Servicios y dependencias: DHCP, DNS, NTP y logs

Un reboot puede regenerar ficheros operativos, reabrir sockets, recargar interfaces y volver a iniciar servicios como Kea DHCPv4/DHCPv6, Unbound y ntpd. El inicio del demonio no implica que atienda correctamente sus consultas. Probar una consulta DNS y una asignación DHCP desde un cliente autorizado; verificar NTP cuando el arranque depende de hora y certificados.

Los registros pueden mostrar avisos normales de parada, arranque y reconexión. Antes de atribuir un error a la actualización reciente, comparar el evento con tiempos de enlace y resoluciones DNS. En entornos con syslog remoto comprobar que los eventos vuelven a enviarse después del reinicio.

95.18. Interfaces, hardware, ZFS y virtualización

Una NIC que muestra “Up” puede no tener gateway accesible; una interfaz virtual puede depender de VLAN, switch físico, hipervisor y orden de arranque. Comprobar portadoras, velocidad/dúplex, direcciones y rutas. En sistemas ZFS evaluar el estado del pool y el BE elegido, sin confundir la selección temporal con una copia externa.

En appliances físicos la modalidad Normal Reboot también ejecuta secuencia de hardware; en máquinas virtuales participa el hipervisor. Una consola de hipervisor facilita observar el arranque, pero el reinicio en la GUI de pfSense no debe confundirse con un reset forzado de la máquina virtual, que puede ser más perjudicial.

95.19. Matriz de validación posterior al reinicio

Orden	Prueba mínima	Criterio de aceptación
1	Consola, GUI y reloj	Arranque completo, login correcto, hora razonable.
2	Interfaces y gateways	Enlaces previstos y salud de rutas verificada.
3	DNS, DHCP y servicios	Consultas y asignación desde cliente, no solo proceso activo.
4	Firewall y NAT	Reglas y flujos de prueba permitidos/bloqueados como se esperaba.
5	VPN y acceso remoto	Túneles negociados y comunicación de ida/vuelta entre subredes.
6	HA y monitorización	Roles CARP, pfsync y notificaciones revisados.



Figura 95.4. Cadena de pruebas de recuperación desde enlace hasta aplicación.

95.20. Diagnóstico: la interfaz no vuelve después de Submit

Síntoma	Hipótesis orientativa	Siguiente acción segura
GUI inaccesible, consola activa	GUI, firewall, IP de gestión o ruta alterada.	Comprobar consola, direcciones y servicio web; no restaurar a ciegas.
Sin portadora WAN	Switch, VLAN, interfaz física o negociación.	Interfaces y enlace aguas arriba, revisar puertos.
DNS no responde	Unbound, interfaces de escucha, upstream o conflicto de puerto.	Status → Services, DNS Lookup y logs.
VPN no reconecta	Endpoint remoto, ruta WAN, certificados u hora.	Status de VPN, gateways, logs y capturas limitadas.
Reinicia al BE equivocado	Activación temporal/persistente distinta de lo previsto.	Dashboard, System → Boot Environments, consola.
Arranque incompleto	Filesystem, kernel, disco o actualización fallida.	Registrar salida de consola y usar recuperación soportada.

95.21. Errores frecuentes que deben evitarse

No emplear Reroot para “probar” la activación de un nuevo kernel; no escoger Single User desde una sesión de administración que dependa de la propia red; no reiniciar de forma repetitiva cuando hay errores de almacenamiento; no activar un BE antiguo sin copia de configuración; y no interpretar un ping de la GUI como validación suficiente de VPN, DHCP o servicios externos.

DECISIÓN IRREVERSIBLE DURANTE LA OPERACIÓN Ni Normal Reboot ni Reroot proporcionan un botón “Deshacer” mientras se ejecutan. Si falta un plan de acceso alternativo, aplazar la intervención y documentar primero el estado del equipo.

95.22. Casos prácticos de administración empresarial

Caso A · Reinicio tras aplicar mantenimiento planificado

El equipo tiene un cambio aprobado y un backup externo. Se elige Normal Reboot para completar la carga de sistema y kernel, se verifica que arranca en el BE esperado y se ejecuta la lista de validación con una prueba externa de acceso y una prueba interna de resolución DNS.

Caso B · Verificación controlada de un Boot Environment anterior

Después de una actualización con anomalías, se identifica un BE anterior comprobado. Se programa un arranque temporal de prueba desde Diagnostics → Reboot, se valida configuración y compatibilidad, se recoge evidencia y se decide de forma separada si cambiar el predeterminado persistentemente.

Caso C · Reinicio del nodo secundario de un clúster

Antes de intervenir, se comprueba que un nodo MASTER estable presta servicio, que CARP y pfsync funcionan, y que el nodo a reiniciar no deja ningún servicio exclusivo sin respaldo. Tras arrancar, se verifica su papel BACKUP y la sincronización sin forzar una conmutación innecesaria.

Caso D · Servicios fallan aunque la GUI vuelve

La GUI es accesible después del reinicio, pero una VPN no establece datos. Se comprueban gateway, DNS, tiempo del sistema, estados de túnel, políticas y rutas. No se repite el reboot hasta localizar evidencia que justifique esa decisión.

95.23. Registro de intervención y criterios de aceptación

Campo de acta	Dato que debe consignarse
Motivo y autorización	Ticket, alcance y responsable sin secretos.
Entorno seleccionado	Nombre del BE y razón de elegirlo; evitar valores sensibles si se distribuye el acta.
Método ejecutado	Normal Reboot o Reroot; si procede, modalidad especial y por qué.
Evidencia antes/después	Reloj, gateway, servicios, VPN, rutas y comparativa de conectividad.
Resultado y reversión	Servicio confirmado o plan de recuperación aplicado.

95.24. Glosario

Término	Definición
Boot Environment (BE)	Entorno de arranque ZFS seleccionable y, en instalaciones compatibles, recuperable.
Reroot	Reinicio de procesos y secuencia de arranque sin recarga de kernel ni reinicialización hardware.
Next boot	Siguiente arranque, que puede ser distinto del entorno predeterminado persistente.
CARP	Protocolo de redundancia que permite atender direcciones virtuales en alta disponibilidad.
pfsync	Mecanismo de sincronización de estados del firewall entre nodos.
OOB	Acceso de administración fuera de banda, independiente de la red a mantener.

95.25. Referencias oficiales y verificables

Netgate — Rebooting the Firewall
Netgate — Managing Boot Environments in the GUI
Netgate — How Boot Environments Work
Netgate — ZFS Boot Environments (Plus Only)
Netgate — Boot Environment Status
Netgate — Selecting Boot Environments in Loader
Netgate — Console Menu Basics
Netgate — Troubleshooting Single User Mode
Netgate — Troubleshooting File System Issues
Netgate — CARP Status
Netgate — Restoring from Backups
Netgate — Unexpected Reboots

96 Diagnostics → Routes

Tabla de encaminamiento · IPv4/IPv6 · gateways · VPN · Multi-WAN · análisis de rutas

La tabla de rutas muestra qué destinos conoce el sistema, por qué puerta de enlace puede alcanzarlos y qué interfaz corresponde al recorrido seleccionado. Su lectura es esencial para distinguir fallos de conectividad, errores de retorno y políticas de encaminamiento que actúan fuera de la ruta predeterminada.

ADVERTENCIA OPERATIVA La consulta de Diagnostics → Routes es informativa. Los cambios de gateways, rutas estáticas o reglas con gateway deben realizarse en las secciones de configuración pertinentes y pueden provocar la pérdida de acceso administrativo, sesiones VPN o salida a Internet.

96.1. Finalidad y ruta de acceso

Ruta: Diagnostics → Routes. La pantalla consta de Routing Table Display Options y dos tablas de salida independientes: IPv4 Routes e IPv6 Routes. Sus filas presentan el estado actual de la tabla de encaminamiento del sistema operativo (FIB); no constituyen un historial de movimientos de paquetes ni una lista completa de conexiones activas. [R1]

Permite verificar rutas conectadas, gateway por defecto, destinos de host, rutas hacia redes remotas y enlaces VPN. La consulta no modifica rutas; la administración de gateways y rutas estáticas corresponde a System → Routing, y las decisiones por política pueden depender de Firewall → Rules. [R2–R4]

Figura 96.1 · Selección de ruta por prefijo más específico

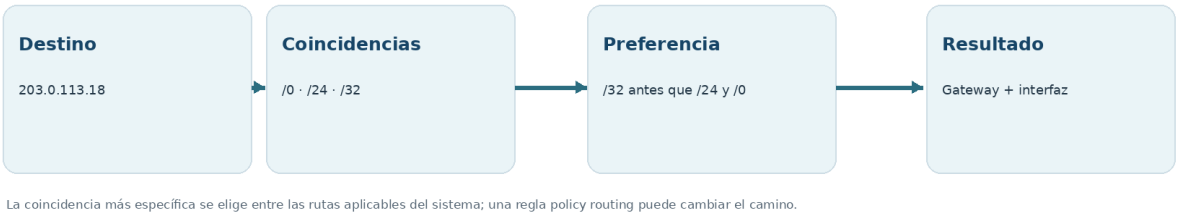


Figura 96.1. La coincidencia de prefijo más específica prevalece en la selección convencional de rutas.

96.2. Routing Table Display Options: todos los controles

Control	Valores / estado visible	Funcionamiento y precaución
Resolve names	Enable (casilla)	Desmarcado de forma predeterminada. Activa consultas DNS inversas para representar nombres cuando sea posible. Puede demorar la carga y, con tablas extensas, afectar a la respuesta de la GUI. [R1]
Rows to display	10, 50, 100, 200, 500, 1000, all	Número de filas mostradas por tabla. Netgate documenta 100 como valor predeterminado. “all” puede resultar pesado si existen numerosas rutas dinámicas. [R1]
Filter	Cadena o expresión regular	Busca coincidencias en las tablas; los patrones inválidos o considerados peligrosos se ignoran según el aviso visible. No modifica la tabla real.
Actualizar visualización	Acción de actualización	Vuelve a mostrar las rutas con la configuración de visualización vigente. La función está documentada aunque su icono no figure en el contenido copiado. [R1]

Un filtro vacío permite inspeccionar todas las rutas dentro del límite de filas. Para una investigación de conectividad, conviene desactivar Resolve names y comenzar por 100 filas; después filtrar por la red o gateway esperado. Esto es una pauta administrativa, no un valor obligatorio del sistema.

96.3. Columnas de IPv4 Routes e IPv6 Routes

Columna	Interpretación técnica	Comprobación útil
Destination	Red o host de destino; “default” es la ruta de último recurso de la familia correspondiente.	Comprobar máscara y prefijo, y si existe ruta más específica.
Gateway	Siguiente salto. “link#N” representa un destino alcanzable directamente por un enlace, no un router externo.	Comparar gateway con red conectada o túnel.
Flags	Indicadores de propiedades: U, G, H, S, entre otros.	Combinar letras; una sola marca no describe toda la ruta.
Use	Cantidad acumulada de paquetes enviados utilizando esa ruta, según Netgate.	Tomar dos observaciones si se necesita verificar incremento.
MTU	Tamaño máximo de unidad de transmisión asociado a la ruta.	No asumir rendimiento ni PMTU efectivo a partir de un único valor.
Netif	Nombre de la interfaz por la que se entregará el paquete.	Contrastar con Status → Interfaces o la interfaz VPN.
Expire	Caducidad de rutas temporales, como las derivadas de redirecciones ICMP.	Celda vacía: no hay temporizador mostrado para esa ruta.

96.4. Decodificación de flags: U, G, H, S y otras marcas

Marca	Nombre	Significado práctico
U	Up	Ruta utilizable por el núcleo.
G	Gateway	Entrega del tráfico a un salto intermedio.
H	Host	Ruta a un único host, no a una red.
S	Static	Marca RTF_STATIC; también aparece en rutas locales generadas automáticamente. No demuestra que el administrador la introdujera a mano.
D	Dynamic	Ruta generada de forma dinámica, por ejemplo a partir de una redirección.
M	Modified	Ruta modificada dinámicamente.
R	Reject	Destino rechazado / inalcanzable.
B	Blackhole	Descarta paquetes en determinadas circunstancias.
L	LLINFO	Información asociada a traducción de direcciones a enlace.
b	Broadcast	Entrada de dirección de difusión.
1, 2, 3	RTF_PROTO*	Indicadores reservados para uso específico de protocolos.

Lectura combinada: “U” identifica una red alcanzable directamente; “UGS” combina ruta utilizable, gateway intermedio y marca estática; “UHS” puede representar una dirección propia con salida lógica lo0. El valor que aparece en Flags es dependiente del núcleo FreeBSD y no equivale a un semáforo de disponibilidad de Internet. [R1]

Figura 96.2 · Tipos de ruta y destino del siguiente salto



Figura 96.2. Diferencias entre ruta conectada, ruta por gateway y dirección local del firewall.

96.5. Interpretación de destinos especiales

Ruta predeterminada y coincidencia por prefijo

La ruta IPv4 “default” equivale a 0.0.0.0/0 y se consulta cuando no existe otra ruta IPv4 más específica. La ruta IPv6 equivalente utiliza ::/0. Una ruta a un host /32 o /128 puede prevalecer sobre una ruta de red y sobre la predeterminada. El encaminamiento del sistema también depende de interfaces operativas y políticas especiales aplicables. [R1–R2]

Redes conectadas y entradas link#N

Una red directamente conectada suele aparecer con Gateway “link#N” y una Netif física o virtual. El número de enlace referencia la interfaz a nivel de sistema; no debe interpretarse como número de VLAN, identificador de gateway o puerto de switch. Una ruta local de host puede apuntar a lo0 aun cuando su dirección pertenezca a otra interfaz.

Loopback, rutas locales y valor MTU 16384

127.0.0.1 y ::1 son direcciones de loopback. Los hosts que pertenecen al propio firewall pueden representarse mediante rutas de host entregadas a lo0. Por ello, observar una MTU distinta en lo0 no significa que el puerto WAN o LAN haya negociado esa misma MTU.

96.6. Ejemplo profesional ficticio de tabla IPv4

Ejemplo didáctico, recreado íntegramente con redes reservadas:

Destino	Gateway	Flags	Netif	Interpretación
default	192.0.2.1	UGS	vtnet0	Salida de último recurso IPv4.
192.0.2.0/24	link#1	U	vtnet0	WAN directamente conectada.
192.0.2.2	link#4	UHS	lo0	Dirección local del firewall.
198.51.100.0/24	link#2	U	vtnet1	LAN directamente conectada.
203.0.113.0/24	198.51.100.1	UGS	vtnet1	Red detrás de un router interno.
203.0.113.128/25	link#9	U	ovpnc99	Red remota de ejemplo publicada por VPN.

Si un destino pertenece a 203.0.113.128/25 se prefiere esa ruta específica frente a 203.0.113.0/24. Deben existir las reglas pertinentes y una ruta de retorno válida; observar el gateway correcto en la tabla no confirma la conectividad de extremo a extremo.

96.7. IPv6 Routes: particularidades y ámbito de interfaz

IPv6 mantiene su tabla separada. La ausencia de ::/0 implica que no hay ruta IPv6 predeterminada mostrada, aunque existan entradas link-local fe80::/64 y direcciones de loopback. Una ruta link-local suele incorporar el identificador de zona, por ejemplo fe80::%vtnet1/64 o un host fe80::1%vtnet1, porque la misma dirección de ámbito local puede repetirse en interfaces distintas. [R1, R5]

Ejemplo IPv6 ficticio	Gateway	Netif	Lectura
::1	link#4	lo0	Loopback del sistema.
fe80::%vtnet1/64	link#2	vtnet1	Red link-local de la interfaz.
2001:db8:10::/64	link#2	vtnet1	Prefijo IPv6 de documentación conectado.
2001:db8:20::/64	2001:db8:10::1	vtnet1	Prefijo IPv6 tras otro router.
default	fe80::1%vtnet0	vtnet0	Ruta por defecto cuando está configurada, en este ejemplo.

INTERPRETACIÓN Una tabla IPv6 formada exclusivamente por link-local no demuestra por sí sola que IPv6 esté deshabilitado; revela que esas rutas están presentes. Contrastar la dirección global, Router Advertisements, el gateway IPv6 y las reglas del firewall antes de diagnosticar una avería.

96.8. Redes VPN: ruta del sistema frente a política IPsec

Tecnología / modo	¿Ruta de red remota en el sistema?	Dónde comprobar la decisión
OpenVPN TUN	Normalmente sí, según rutas instaladas por la configuración.	Netif de OpenVPN, rutas y configuración del túnel.
WireGuard	Necesita ruta del sistema; Allowed IPs por sí solo no crea todas las rutas necesarias.	Tabla de rutas + peer Allowed IPs + gateway asignado.
IPsec VTI	Sí; se utiliza encaminamiento convencional.	Interfaz VTI, ruta/gateway, reglas IPsec.
IPsec túnel tradicional	No se espera una ruta específica de túnel para la red remota.	Policies SPD, SAs y Phase 2 / selectores.

La ausencia de una red remota en Diagnostics → Routes no implica que esté mal configurada una VPN IPsec en modo túnel tradicional: se encamina mediante políticas IPsec. En cambio, OpenVPN, WireGuard e IPsec VTI dependen de la tabla de rutas para llegar a las redes pertinentes. [R2, R6–R7]

Figura 96.3 · Cómo se enruta el tráfico por VPN



Nota: el resultado también depende de reglas de firewall, NAT, estado de túnel y rutas de retorno.

Figura 96.3. Diferencias entre rutas de sistema, rutas internas de peers y políticas IPsec.

96.9. Gateway Groups, Multi-WAN y rutas por políticas

Los grupos de gateways no tienen por qué aparecer como una única entrada de la tabla de rutas. Las reglas de firewall pueden utilizar policy routing para enviar tráfico específico por una WAN o un grupo distinto del gateway predeterminado; estas decisiones se implementan con mecanismos PF como route-to y reply-to. La tabla de rutas es imprescindible, pero no siempre suficiente para entender una conexión atravesando el firewall. [R3, R8]

Un gateway con estado Online en Status → Gateways describe la respuesta del monitor configurado, no demuestra que todas las rutas y protocolos funcionen. Ante un fallo Multi-WAN, correlacionar: estado de gateway, regla aplicada y su gateway, tabla de estados, Outbound NAT y rutas de retorno. El tráfico originado en el propio firewall puede diferir del tráfico reenviado por reglas. [R8–R10]

RIESGO DE CAMBIO Modificar el gateway predeterminado o una ruta estática desde una sesión remota puede interrumpir la administración. Programar acceso alternativo y copia de configuración. No corregir una salida por políticas añadiendo rutas estáticas a ciegas.

96.10. Rutas estáticas, dinámicas y interfaces

Una ruta estática se administra en System → Routing → Routes y requiere definir previamente un gateway apropiado cuando el destino no es directamente conectado. El sistema puede mostrar también rutas conectadas, rutas recibidas de servicios dinámicos o rutas aprendidas mediante paquetes de routing como FRR (por ejemplo OSPF/BGP). El resultado y la persistencia dependen de quién controla cada entrada. [R4, R11]

Una modificación de rutas mediante comandos del sistema puede ser temporal o entrar en conflicto con la regeneración de configuración del firewall. Para cambios permanentes emplear las secciones soportadas; no confundir una modificación directa de la FIB con una definición persistente en pfSense.

96.11. MTU, rutas de retorno y rutas asimétricas

La columna MTU describe el máximo asociado a la ruta. No determina por sí sola el MSS TCP, la encapsulación de un túnel ni la PMTU real de extremo a extremo. Si el ping funciona pero una aplicación grande falla, investigar PMTUD, filtrado ICMP de errores, MSS de VPN y capturas a ambos lados. [R12]

En routing asimétrico, una ida puede atravesar pfSense y la respuesta regresar por otro router. Esto impide que el filtro con estado vea ambos sentidos y puede producir sesiones TCP intermitentes. No activar opciones de bypass o “sloppy states” como solución universal: revisar el diseño y los gateways. [R13]

96.12. Procedimiento 1 — Lectura de la tabla sin intervenir

1. Acceder a Diagnostics → Routes y dejar Resolve names desactivado para evitar demoras innecesarias.
2. Mantener inicialmente Rows to display en 100; ampliar a 500 o all únicamente si la investigación lo requiere.
3. Comprobar la ruta default IPv4 y, cuando corresponda, default IPv6; identificar Gateway y Netif.
4. Buscar la red de destino mediante Filter y observar si aparece otra ruta más específica.
5. Anotar Flags, Use, MTU y Expire sin convertir los contadores acumulados en tasas de ancho de banda.
6. Contrastar las interfaces con Status → Interfaces y la puerta de enlace con Status → Gateways.

96.13. Procedimiento 2 — Consultar la ruta efectiva desde consola

Los comandos de lectura siguientes son adecuados para una comprobación puntual; sustituir los destinos ilustrativos por direcciones autorizadas en un entorno real. [R1–R2]

Comando de consulta	Utilidad
netstat -rWn	Mostrar tablas IPv4/IPv6 de encaminamiento sin resolver nombres.
netstat -rWn -f inet	Limitar la salida a la familia IPv4.
netstat -rWn -f inet6	Limitar la salida a la familia IPv6.
route -n get 203.0.113.18	Consultar interfaz y siguiente salto para un destino IPv4 ficticio.
route -n get -inet6 2001:db8:20::18	Consultar un destino IPv6 de documentación, si la sintaxis está soportada en la versión.

El resultado de route -n get es una consulta del encaminamiento del sistema. Una regla con gateway puede seleccionar una WAN diferente para un flujo concreto; en ese caso revisar simultáneamente reglas PF, Estados y NAT. [R2–R3]

96.14. Procedimiento 3 — Red remota por VPN sin conectividad

1. Comprobar si el túnel figura activo en Status → OpenVPN, WireGuard o IPsec, según corresponda.
2. Para OpenVPN, verificar la ruta de red remota, el gateway del túnel y las rutas que la configuración proporciona.
3. Para WireGuard, verificar separadamente la ruta de sistema y la selección del peer mediante Allowed IPs; revisar la red de retorno.
4. Para IPsec túnel tradicional, inspeccionar SPD y CHILD_SA en Status → IPsec; no crear automáticamente una ruta estática esperando que sustituya las políticas IPsec.
5. Comprobar reglas de entrada/salida, origen seleccionado en Ping y tráfico real en Packet Capture.
6. Si una aplicación falla con ICMP funcional, comprobar puertos, MTU/MSS, NAT y asimetría de retorno.

96.15. Procedimiento 4 — Multi-WAN y gateway de salida inesperado

1. Registrar destino, origen, momento y comportamiento esperado del flujo.
2. Consultar Diagnostics → Routes para conocer el gateway default y cualquier ruta específica.
3. Revisar en Firewall → Rules la primera regla que coincide y su campo Gateway o Gateway Group.
4. Comparar los estados del gateway en Status → Gateways y los estados actuales de conexión en Diagnostics → States.
5. Comprobar si existe Outbound NAT adecuado para la WAN elegida y si reply-to/route-to condiciona la respuesta.
6. Verificar la ruta de retorno y efectuar una captura en la interfaz de salida prevista antes de modificar la configuración.

Figura 96.4 · Diagnóstico ordenado de una ruta incorrecta

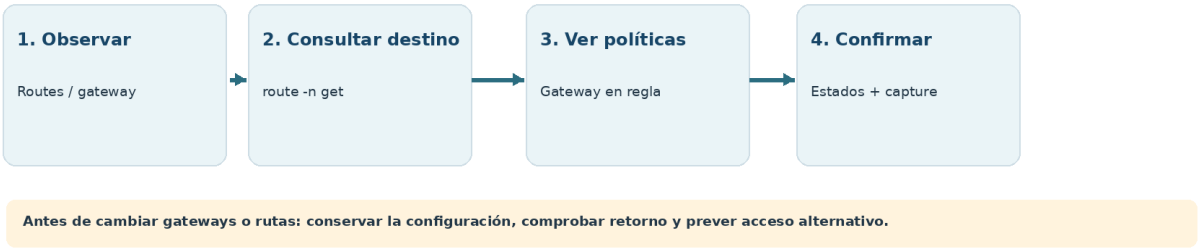


Figura 96.4. Secuencia de comprobación de rutas, políticas y tráfico real.

96.16. Errores habituales y matriz de diagnóstico

Síntoma	Posible explicación	Verificación recomendada
No aparece default IPv4	Gateway no configurado, interfaz sin enlace o cambios dinámicos.	Status → Interfaces/Gateways y configuración System → Routing.
Ruta presente, tráfico falla	Regla de firewall, NAT, destino apagado o retorno ausente.	States, System Logs y Packet Capture.
Se sale por otra WAN	Policy routing en una regla PF o ruta más específica.	Revisar Gateway de la regla y el estado PF.
VPN IPsec tradicional sin ruta	Comportamiento previsto para modo túnel basado en SPD.	Comprobar selectores IPsec y SAs.
WireGuard con Allowed IPs correctas	Falta una ruta estática/dinámica del sistema o gateway.	Revisar FIB y gateway del peer.
IPv6 solo muestra fe80	Sin ruta global o sin gateway IPv6 detectado.	Router Advertisements, WAN IPv6 y routing.
Resolución de nombres lenta	Resolve names habilitado con muchos destinos y DNS lento.	Desactivarlo y recargar la vista.
TCP intermitente entre redes	Asimetría de ida/vuelta o gateway interno incorrecto.	Captura en ambas interfaces y tabla de estados.
Rutas IPv4 correctas, IPv6 falla	Tablas de rutas separadas; IPv6 puede carecer de default.	Comprobar ::/0 y ruta IPv6 por destino.

96.17. Escenarios empresariales: interpretación contextual

Sede con router interior adicional

Un segmento remoto alcanzable mediante un router conectado a LAN requiere una ruta estática adecuada, además de las rutas de retorno en el router interior. Si los equipos usan gateways diferentes, vigilar el estado de conexión PF y no presumir que agregar la ruta arreglará una asimetría de ambos sentidos. [R4, R13]

Conmutación de enlace de Internet principal a respaldo

La caída del gateway predeterminado puede modificar la ruta general, pero una regla por políticas puede seleccionar el grupo failover independientemente. Verificar el estado del gateway, la regla aplicada, NAT y la persistencia de estados creados antes del fallo. [R3, R8]

Acceso a red de servidores publicada por OpenVPN

Una ruta a la red de servidores debe usar el siguiente salto o interfaz OpenVPN correspondiente. No basta con un túnel “Connected”; asegurar la red remota, los selectores internos de OpenVPN cuando proceda, las reglas y el camino de vuelta. [R2, R6]

Oficina con IPv6 parcial

La presencia de rutas fe80::/64 indica ámbito link-local, pero no representa una ruta IPv6 de Internet. Examinar dirección global, prefijo, rutas recibidas por RA y posible default ::/0; el diagnóstico de IPv4 debe realizarse por separado. [R1, R5]

96.18. Buenas prácticas para administración y cambios

Registrar ruta esperada y resultado real antes de editar gateways o reglas; guardar configuración y forma de acceso alternativo.

Evitar Resolve names y all en tablas muy extensas si la GUI responde lentamente; el filtro es una herramienta de visualización.

Comparar rutas por destino con route -n get y validar la decisión final con estado PF y capturas de tráfico.

No interpretar una ruta U o un gateway Online como prueba de que la aplicación de destino responde.

Distinguir VLAN, interfaz física, túnel VPN e interfaz lo0; cada uno puede tener rutas locales independientes.

Separar siempre IPv4 e IPv6 y documentar retorno, NAT y excepciones de policy routing.

96.19. Glosario técnico

Término	Significado
FIB	Forwarding Information Base: tabla utilizada por el sistema para decidir salidas convencionales.
Gateway / next hop	Router al que se entrega el paquete hacia un destino.
Prefijo CIDR	Red más máscara, como /24 en IPv4 o /64 en IPv6.
Netif	Interfaz por la que se transmite el paquete según la ruta.
Link-local	Dirección IPv6 local al enlace que necesita ámbito de interfaz.
Policy routing	Selección de salida condicionada por reglas de firewall, no solo por destino.
SPD	Security Policy Database de IPsec para aplicar políticas de túnel.
PMTUD	Descubrimiento de MTU máxima del camino.
Asimetría	Tráfico de ida y vuelta que sigue recorridos distintos.

96.20. Validación posterior a un cambio de rutas

Una vez aplicada una modificación en System → Routing o en una regla que seleccione gateway, conviene efectuar una secuencia de aceptación con resultados medibles. La prueba tiene que ejecutarse desde el firewall y desde al menos un cliente representativo: un Ping efectuado en pfSense no reproduce necesariamente las reglas y estados que afectan al tráfico reenviado. [R2–R3]

Evidencia	Resultado esperado	Si no coincide
Tabla IPv4/IPv6	La ruta prevista aparece con destino y siguiente salto correctos.	Verificar gateway, origen de la ruta y prioridad de prefijos.
Consulta de un destino	route -n get identifica interfaz/gateway previstos.	Buscar ruta más específica o default distinto.
Regla de salida	El flujo coincide con la regla y gateway configurados.	Revisar orden de reglas, grupos y bypass de políticas.
Tabla PF de estados	La conexión nueva usa el recorrido esperado.	Examinar estados anteriores y asimetría antes de borrarlos.
Capturas en dos interfaces	Se observa la solicitud y la respuesta en la dirección correcta.	Examinar filtrado, NAT, retorno o servicio remoto.
Prueba del servicio	TCP/UDP de aplicación opera además de ICMP.	Comprobar puerto, ACL del servicio y MTU/MSS.

96.21. Reversión planificada y conservación de evidencias

Antes de modificar una ruta por defecto o una regla que afecte a la sesión de administración, guardar el XML de configuración en un repositorio seguro, registrar el gateway anterior y disponer de consola o canal de gestión alternativo. En un clúster, evaluar si el cambio se sincronizará y su efecto en los estados del nodo secundario.

1. Anotar el cambio exacto, hora, responsable, destino de prueba y conectividad de referencia.
2. Aplicar una única modificación aprobada y verificar conectividad desde el punto de gestión.
3. Comparar de nuevo Diagnostics → Routes, Gateway Status y las pruebas de aplicación.
4. Si falla, revertir mediante el mecanismo soportado en la configuración; no introducir rutas de consola adicionales que compliquen el estado.
5. Comprobar estabilidad de VPN, DNS, salida WAN y rutas de retorno después de la reversión.

CRITERIO DE CIERRE Una intervención se considera validada cuando coinciden tabla de rutas, política aplicada, estados PF y tráfico observado, y la aplicación de destino responde. Conservar evidencia de la prueba y del camino de retorno.

96.22. Referencias oficiales y normativas

Referencias 1–7	Referencias 8–13
[1] Netgate — Route Table Contents	**[8]** Netgate — Troubleshooting Multi-WAN
[2] Netgate — Troubleshooting Routes	**[9]** Netgate — Troubleshooting Network Connectivity
[3] Netgate — Policy Routing Configuration	**[10]** Netgate — Multi-WAN and NAT
[4] Netgate — Static Routes	**[11]** Netgate — Routing Logs
[5] Netgate — IPv6 and pfSense Software	**[12]** Netgate — Troubleshooting Lost Traffic
[6] Netgate — Choosing a VPN Solution	**[13]** Netgate — Troubleshooting Asymmetric Routing
[7] Netgate — WireGuard Routing	

97 Diagnostics → S.M.A.R.T. Status

Estado del almacenamiento · atributos SMART · registros · autopruebas · eMMC · continuidad

Una unidad puede seguir leyendo datos aunque no pueda escribirlos. Vigilar la salud del almacenamiento y anticipar el reemplazo permite evitar pérdidas de configuración, errores en registros y paradas inesperadas.

ADVERTENCIA OPERATIVA Las pruebas de unidades pueden afectar al rendimiento. «PASSED» no elimina el riesgo de fallo y las copias de seguridad deben existir antes de iniciar una investigación de disco.

97.1. Finalidad, alcance y ruta

Ruta: Diagnostics → S.M.A.R.T. Status. El panel Information & Tests permite consultar información del soporte, obtener registros internos, lanzar autopruebas y detener una prueba activa. Todas estas operaciones se aplican al dispositivo seleccionado, no a una interfaz de red ni a un volumen lógico.

No se debe equiparar la presencia del dispositivo en el selector con una compatibilidad completa con SMART. La funcionalidad disponible depende del firmware de la unidad, su controlador, el bus y la versión de software.

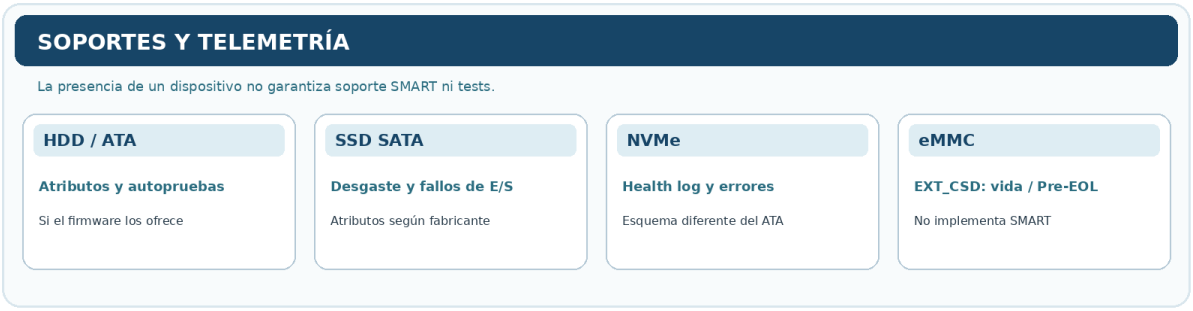


Figura 97.1. HDD, SSD SATA, NVMe y eMMC ofrecen telemetría distinta, y no todas las pruebas son intercambiables.

97.2. Fundamentos de SMART y su valor diagnóstico

S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) permite consultar métricas internas y, en determinadas unidades, iniciar autotests en el propio firmware. No es un sistema de predicción perfecto: un disco puede fallar con estado general correcto. Los errores que aparecen en logs, sus tendencias y los síntomas de E/S tienen más valor que un resultado «PASSED» aislado.

En ATA/SATA los atributos pueden mostrar VALUE, WORST, THRESH y RAW_VALUE; los tres primeros suelen ser valores normalizados, mientras que RAW_VALUE depende del fabricante. En NVMe la información procede de registros de salud y eventos; eMMC usa mecanismos distintos, basados en EXT_CSD, y no implementa SMART ATA.

97.3. Panel Information: controles y comportamiento

Control visible	Valores / acción	Interpretación y precaución
Select a drive and type	Selector Device: unidad disponible	Selecciona el disco objetivo; no presupone que todas las funciones sean compatibles.
Information Type	All SMART and Non-SMART Information, entre otros	Selecciona la extensión de la consulta. Las alternativas concretas dependen del menú de la versión.
View	Botón de consulta	Solicita datos al dispositivo y muestra el resultado; puede no devolver datos SMART si el soporte carece de esta función.
Device /dev/	Prefijo del identificador de dispositivo	Ruta del sistema operativo. Confirmar siempre la unidad elegida antes de iniciar pruebas.

97.4. Tipos de información documentados oficialmente

Tipo	Qué devuelve	Utilidad
Device Information	Modelo, versión, capacidad, interfaz, capacidades y números de serie.	Identificar el soporte; ocultar seriales al compartir informes.
Device Health	Evaluación resumida de salud o estado general.	Orientación; no descarta fallos.
SMART Capabilities	Soporte de autopruebas, duración estimada y funciones de firmware.	Decidir qué test admite el dispositivo.
SMART Attributes	Atributos de error, uso, temperatura y desgaste.	Análisis de tendencias y umbrales.
All SMART Information	Datos anteriores y registros/autopruebas.	Inspección ampliada.
All SMART and Non-SMART Information	Salud, eventos y otras estadísticas adicionales que ofrece la unidad.	Vista general extensa; puede producir salida muy larga.

La etiqueta exacta de opciones adicionales puede cambiar entre versiones. Estos nombres corresponden a los tipos documentados por Netgate, no a desplegables adicionales observados en la captura.

97.5. Lectura profesional de atributos ATA/SSD

Atributo / dato	Qué vigilar	Decisión orientativa
Reallocated_Sector_Ct	Aumento sostenido de sectores reasignados.	Investigar; preparar reemplazo según evolución.
Current_Pending_Sector	Sectores pendientes de verificación o reasignación.	Alta prioridad si aumenta o coincide con errores de lectura.
Offline_Uncorrectable	Sectores imposibles de corregir en pruebas internas.	Riesgo alto, proteger datos y planificar sustitución.
UDMA_CRC_Error_Count	Problemas de enlace SATA/cable/controladora; no siempre daño del medio.	Examinar cableado/controladora y tendencia.
Power_On_Hours	Horas de servicio.	Contexto de antigüedad; no fallo por sí solo.
Temperature	Temperatura reportada por la unidad.	Comparar con el rango del fabricante.
Media_Wearout / Spare	Vida consumida o reserva disponible del SSD.	Interpretar según documentación del modelo.

97.6. Panel View Logs: campos y botón View

En «Select a device and log» se eligen la unidad y el Log correspondiente. «View» devuelve las entradas registradas por el firmware. En la captura se observa «Summary Error Log»; la disponibilidad de otros tipos no puede deducirse solo de esa selección visible.

Registro oficial	Qué muestra	Limitación
Summary Error Log	Resumen de errores de lectura/escritura, CRC y otros eventos.	Puede no existir en algunos soportes.
Extended Error Log	Errores con más detalle.	Depende del firmware.
SMART / Extended Self-Test Log	Resultados, abortos, porcentaje restante y LBA del primer fallo.	Puede reflejar pruebas de días anteriores.
Selective Self-Test Log	Bloques LBA seleccionados y resultado.	No disponible en todos los discos.
Log Directory	Relación de logs accesibles y tamaños.	No implica que todos contengan eventos.
Temperature / Device Statistics	Historial térmico y estadísticas ATA.	ATA solo cuando está soportado.

Registro oficial	Qué muestra	Limitación
SATA PHY / SAS PHY Events	Eventos físicos del enlace.	Solo para el bus apropiado.
NVMe Log	Registros de salud y errores NVMe.	Esquema diferente del ATA.
SSD Device Statistics	Desgaste y uso en unidades compatibles.	Significado depende de ATA/SCSI y fabricante.

97.7. Panel Perform self-tests: controles y clases de prueba

«Select a drive and test» determina la unidad y la prueba. El botón «Test» solicita la autoprueba al firmware; antes debe consultarse SMART Capabilities. Si el controlador no permite el comando, la operación puede fallar o quedar sin resultado, aunque el dispositivo aparezca en el selector.

Test Type	Funcionamiento	Cuándo utilizarlo
Offline Test	Recogida de datos interna; puede esperar a periodos inactivos y actualizar atributos.	Investigación inicial con carga controlada.
Short	Autotest relativamente breve de funciones básicas y lectura.	Comprobación rápida, con duración real indicada por la unidad.
Long / Extended	Prueba más exhaustiva de superficie/medio según firmware.	Mantenimiento programado, posible impacto elevado.
Conveyance	Prueba orientada a daños tras transporte, especialmente en ATA.	Solo cuando el dispositivo declara esta capacidad.

PRECAUCIÓN No ejecutar una prueba prolongada en un firewall crítico sin evaluar carga de disco, disponer de copia reciente y establecer una ventana. Las estimaciones y el impacto varían por firmware.

97.8. Panel Abort Tests: detener sin interpretar como éxito

El selector «Device /dev/» identifica la unidad que mantiene una prueba. «Abort Tests» intenta detener las pruebas activas en ese dispositivo. La interrupción no repara errores, no cancela registros históricos y puede dejar un resultado «aborted» en el log de autopruebas. Comprobar la terminación y documentar el motivo.



Figura 97.2. Flujo de uso de los cuatro paneles, diferenciando consultas de operaciones que actúan sobre el firmware.

97.9. eMMC: diagnóstico de salud sin SMART convencional

En sistemas con almacenamiento eMMC, un dispositivo de tipo mmcsdN puede aparecer entre las unidades, pero eMMC no implementa SMART ATA. Netgate documenta la lectura de EXT_CSD mediante mmc-utils, disponible para pfSense Plus y manejado desde consola/SSH, sin interfaz gráfica propia. El almacenamiento debe soportar los campos requeridos por la especificación.

En una consola autorizada, el administrador identifica primero el dispositivo y, solo en el equipo correspondiente, ejecuta la lectura de EXT_CSD. Expresión genérica: «mmc extcsd read /dev/mmcsdNrpmb», donde N se sustituye por el índice correcto. La instalación del paquete, cuando proceda y esté soportada, se realiza siguiendo la documentación oficial de Netgate; no es una acción necesaria para consultar el panel web.

Campo eMMC	Interpretación	Qué hacer
LIFE_TIME_EST_TYP_A	Consumo estimado de bloques SLC/pseudo-SLC, por pasos del 10 %.	Registrar tendencia; no confundir con porcentaje de vida restante.
LIFE_TIME_EST_TYP_B	Consumo estimado de bloques MLC, por pasos del 10 %.	Comparar con lecturas anteriores y OEM.
PRE_EOL_INFO	0x01 normal, 0x02 aviso, 0x03 urgente según bloques de reserva.	Priorizar sustitución/migración según estado.
0x00 o campo ausente	Valor indefinido o sin soporte.	No concluir «sin desgaste» a partir de la ausencia de datos.

97.10. NVMe, controladoras RAID y soportes USB

NVMe informa indicadores específicos de salud, temperatura, errores de medio y desgaste; la estructura no es equivalente a una tabla ATA de IDs normalizados. Las controladoras RAID pueden ocultar la telemetría individual y requieren utilidades del fabricante. Una carcasa USB puede impedir el paso de comandos SMART. La ausencia de unidad o de registros no prueba que el almacenamiento esté sano ni necesariamente averiado.

97.11. Interpretar PASSED, temperatura y tendencia

La evaluación general «PASSED» significa únicamente que el firmware no ha declarado un fallo según su criterio. Un error repetido de E/S, un incremento en sectores irrecuperables o una tendencia abrupta de desgaste justifican investigación aunque el estado general siga siendo correcto. Comprobar fabricante, fecha del último test, evolución de atributos y registros de sistema.

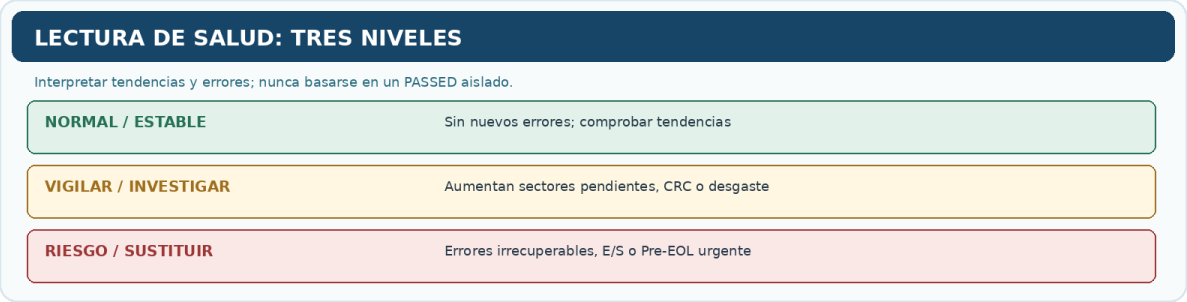


Figura 97.3. Priorización orientativa basada en errores, tendencias y señales de desgaste, no en una lectura aislada.

97.12. Resultados frecuentes y cómo actuar

Hallazgo	Posible explicación	Acción segura
SMART unsupported	eMMC, firmware sin función o controlador incompatible.	Identificar tecnología; consultar herramienta específica del fabricante.
PASSED con errores de lectura	Umbral general no superado pese a errores concretos.	Backup, revisar logs y planificar sustitución según gravedad.
Test aborted	El host o administrador interrumpió la prueba.	Registrar evento; repetir solo cuando sea seguro.
Command failed	Controlador, permisos o test no soportado.	Validar capacidades; evitar repetir indiscriminadamente.
Unidad ausente	Disco no expuesto a SMART a través del controlador.	Revisar dispositivos, RAID/USB y consola.
Escrituras fallidas	Disco dañado, medio solo lectura o falta de espacio.	No forzar reinicios; conservar configuración y diagnosticar almacenamiento.

97.13. Procedimiento 1 — Inventario y evaluación sin modificar nada

1. Acceder a Diagnostics → S.M.A.R.T. Status y registrar la fecha, versión de pfSense y rol del equipo sin incluir números de serie en informes compartidos.

2. Abrir Information y seleccionar la unidad destinada a evaluación, verificando bus y tecnología.

3. Consultar Device Information y Device Health, si el dispositivo los admite.

4. Leer SMART Capabilities para decidir qué pruebas y logs están disponibles.

5. Consultar atributos y Summary Error Log; contrastar con mensajes de E/S del sistema.

6. Conservar evidencias anonimizadas y comparar con registros previos.

97.14. Procedimiento 2 — Ejecutar un test breve controlado

1. Verificar un backup reciente y que el firewall dispone de recuperación fuera de banda cuando sea necesario.

2. Consultar la estimación de duración y el soporte de Short Test en SMART Capabilities.

3. Acordar ventana de mantenimiento y comprobar el nivel de carga del almacenamiento.

4. Seleccionar la unidad, elegir Short y pulsar Test una sola vez.

5. Esperar a la finalización y abrir Self-Test Log: buscar «Completed without error», abortos o LBA de fallo.

6. Documentar cambios respecto de la línea base y escalar si aparece un error.

97.15. Procedimiento 3 — Investigación de desgaste eMMC

1. Identificar el tipo de dispositivo mediante información de sistema y consultar documentación del fabricante.

2. Confirmar que la plataforma permite lectura de salud EXT_CSD; no interpretar un selector SMART como garantía de soporte.

3. En una consola autorizada, verificar el índice de la unidad y utilizar las utilidades MMC documentadas para Plus.

4. Registrar LIFE_TIME_EST_TYP_A/B y PRE_EOL_INFO si están presentes.

5. Comparar con una lectura anterior y preparar sustitución o migración si surge un estado de aviso/urgente.

97.16. Procedimiento 4 — Anomalías de E/S y continuidad operativa

1. Recoger primero copia de configuración y registros relevantes si el soporte sigue siendo accesible.

2. Comprobar si el problema es falta de espacio, corrupción de sistema de archivos, desconexión de controlador o degradación física.

3. Correlacionar SMART/EXT_CSD, logs del sistema, disponibilidad ZFS y fallos de escritura.

4. Evitar pruebas largas y reinicios innecesarios cuando el medio está inestable.

5. Preparar unidad de reemplazo, ventana y procedimiento documentado de restauración.

97.17. Escenarios empresariales y criterio de decisión

Escenario	Observación inicial	Respuesta adecuada
Appliance con eMMC	No devuelve atributos SMART ATA.	Consultar salud EXT_CSD soportada; plan de migración si hay desgaste.
Servidor pfSense con SSD	Aumentan errores de medio/sectores pendientes.	Respaldar, contrastar logs y sustituir preventivamente.
VM en hipervisor	La GUI solo expone disco virtual.	Vigilar salud del almacenamiento desde host/NAS/controladora.
RAID hardware	No aparecen discos físicos en la lista.	Utilizar consola o utilidades del fabricante, no inferir salud.

Escenario	Observación inicial	Respuesta adecuada
Instalación USB	Caja USB no pasa comandos SMART.	Comprobar vía soporte/controladora o herramienta específica.

97.18. Impacto en servicios críticos del firewall

Si el almacenamiento pierde capacidad de escritura, el filtrado ya cargado podría mantenerse temporalmente, pero fallarían operaciones de configuración, logs, instalación de paquetes o recuperación tras reinicio. Esto exige una evaluación coordinada con el responsable de servicios DNS/DHCP, IPsec, OpenVPN y Multi-WAN. No reiniciar por rutina ante anomalías de disco sin conocer el estado del arranque y disponer de medios de recuperación.

97.19. Seguridad de los informes y control de acceso

La información completa puede contener números de serie, identificadores únicos de unidad, rutas de almacenamiento y detalles de hardware. Reducir su difusión, anonimizar antes de adjuntarla a incidencias y restringir el acceso a Diagnostics. Las capturas de diagnósticos se consideran evidencias operativas, no material para publicación sin revisión.

97.20. Planificación preventiva y comprobaciones periódicas

Establecer una línea base de capacidad, temperatura, horas de funcionamiento, bloques defectuosos y salud del medio; revisar periódicamente las tendencias con una frecuencia apropiada a criticidad y carga. Mantener copias de configuración probadas y conocer el procedimiento de reemplazo antes de que se agote el almacenamiento.

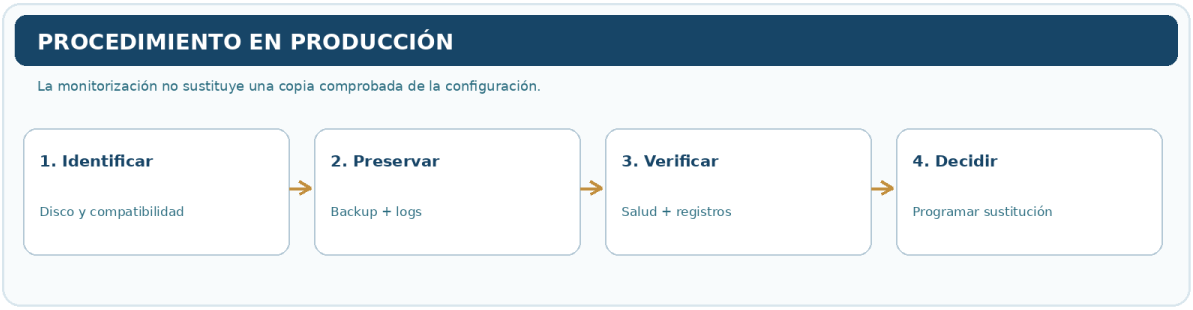


Figura 97.4. Método de intervención: identificar, preservar, verificar y sustituir cuando corresponda.

97.21. Matriz de incidencias y herramientas complementarias

Síntoma	Herramienta / evidencia	Interpretación práctica
Disco no listado	Diagnostics → SMART, sysctl kern.disks	Controlador, bus o soporte de telemetría.
Errores de escritura	System Logs, df -h, zpool status (si ZFS)	Separar falta de espacio de fallo físico o de pool.
SMART PASSED pero fallos	SMART Logs, mensajes del kernel	No confiar solo en el estado resumido.
Desgaste eMMC	mmc-utils y EXT_CSD cuando compatible	Interpretar LIFE y PRE_EOL, contrastar tendencia.
Errores después de traslado	Conveyance cuando declarado	Evaluar daños físicos; no sustituye test completo.
Bajo rendimiento	System Activity y métricas de disco	Correlacionar con CPU, memoria y picos de I/O.

97.22. Lista de validación tras una intervención

1. Verificar arranque estable, discos presentes y sistemas de archivos montados sin errores.
2. Confirmar estado de servicios esenciales y operación de interfaces, rutas y VPN.
3. Comprobar que los cambios de configuración se guardan y que los registros nuevos se escriben.
4. Verificar la disponibilidad de copias y registrar número de incidencia, fecha, evidencia y resultado final.

5. Documentar cualquier acción pendiente y mantener vigilancia reforzada durante el periodo posterior.

97.23. Glosario técnico

Término	Definición
SMART	Telemetría y autopruebas implementadas por ciertos discos; no certifica ausencia de fallos.
EXT_CSD	Registro ampliado de capacidades y vida de unidades eMMC compatibles.
Pre-EOL	Estimación de disponibilidad de bloques de reserva eMMC.
LBA	Dirección lógica de bloque a la que puede referirse una incidencia de un test.
NVMe	Protocolo/interfaz para almacenamiento no volátil, con registros de salud propios.
RAW_VALUE	Valor bruto ATA que puede ser específico del fabricante.
RAID	Agrupación de discos que puede ocultar telemetría individual al sistema operativo.

97.24. Referencias técnicas oficiales

Las opciones adicionales, sus nombres y las diferencias de compatibilidad se han contrastado con documentación de Netgate. La disponibilidad concreta depende de versión, hardware, unidad y controlador.

Netgate — S.M.A.R.T. Hard Disk Status

Netgate — Troubleshooting Disk Lifetime

Netgate — Diagnostics Menu Guide

Netgate — S.M.A.R.T. Dashboard Widget

Netgate — Troubleshooting Multiple Disks

Netgate — Backup and Restore

Netgate — System Monitoring

98 Diagnostics → Sockets

Puertos de escucha · procesos · IPv4 e IPv6 · servicios · auditoría de exposición

Un socket abierto identifica un recurso de red del propio cortafuegos. Determinar si está activo, dónde escucha y quién puede alcanzarlo exige combinar procesos, direcciones, reglas y pruebas de conectividad.

> PRECAUCIÓN La presencia de *:53 o *:443 no demuestra acceso público. Tampoco se debe detener un proceso por aparecer como root ni abrir un puerto WAN para probarlo sin autorización y plan de reversión.

98.1. Objetivo, ámbito y ruta de acceso

Ruta exacta: Diagnostics → Sockets. La página presenta «IPv4 System Socket Information» e «IPv6 System Socket Information». En la información de esta edición se observan tablas de sockets, sin formularios de creación, edición ni acciones sobre cada fila. La consulta es una operación de observación del estado del firewall.

Netgate indica que el origen de los datos es el comando FreeBSD sockstat y que la herramienta muestra sockets de los procesos que ejecuta pfSense. No enumera por sí misma conexiones de equipos que atraviesan el cortafuegos; estas se estudian en Diagnostics → States, pfTop o Packet Capture.

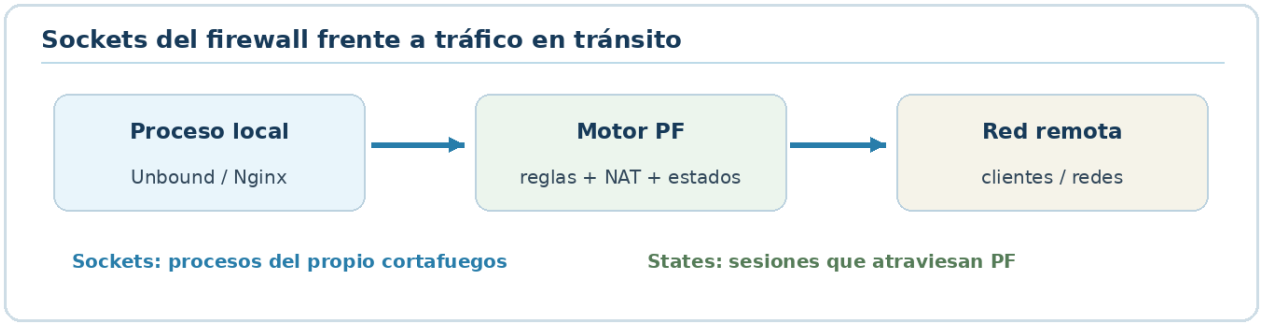


Figura 98.1. Alcance de Sockets frente al análisis de conexiones que atraviesan el motor de filtrado PF.

98.2. Qué es un socket y qué información representa

Un socket es un extremo de comunicación usado por un proceso, habitualmente identificado por familia de direcciones, protocolo y dirección/puerto local; cuando existe comunicación conectada, también puede indicar extremo remoto. Un mismo proceso mantiene múltiples sockets y un mismo puerto puede figurar en varios trabajadores del servicio.

La existencia de un socket indica asignación o uso de un recurso de red por el sistema operativo, no que un servicio responda correctamente a nivel de aplicación. En UDP, la ausencia de negociación de conexión implica que un socket asociado a un puerto puede figurar sin un cliente remoto específico.

98.3. Columnas presentes en ambas tablas

Columna	Significado técnico	Lectura correcta
User	Usuario del sistema propietario del proceso, p. ej., root o unbound.	Es una identidad de ejecución; no identifica al usuario remoto.
Command	Nombre del proceso o daemon que mantiene el socket.	El nombre no garantiza por sí solo la función o salud del servicio.
PID	Identificador del proceso en el sistema operativo.	Puede cambiar al reiniciar y no debe confundirse con el puerto.
FD	File descriptor que el proceso usa para ese socket.	Varios FD del mismo PID no son distintos usuarios conectados.
Proto	Protocolo y familia: tcp4, udp4, tcp6, udp6 y posibles variantes.	TCP y UDP en un mismo puerto no son equivalentes.
Local	IP/interfaz lógica y puerto asociados al extremo local.	Puede ser específica, loopback o comodín de la familia.

Columna	Significado técnico	Lectura correcta
Foreign	Dirección y puerto remoto, si hay extremo asociado.	*:* no significa una conexión con todos los hosts.

98.4. Lectura de IPv4 System Socket Information

La lista IPv4 permite reconocer servicios en direcciones del firewall: por ejemplo, unbound en tcp4/udp4 puerto 53, nginx en tcp4 puerto 443, ntpd en udp4 puerto 123, o un servidor DHCPv4 en udp4 puerto 67. La presencia concreta y su asociación a interfaces dependen de los servicios y paquetes configurados.

Ejemplo ficticio: «unbound 2314 5 udp4 192.0.2.10:53 *:*» indica un socket UDP de Unbound vinculado a esa dirección IPv4 y puerto; no demuestra que un cliente remoto de Internet pueda usarlo. «nginx 1825 7 tcp4 *:443 *:*» muestra un extremo local de escucha sobre todas las direcciones IPv4 elegibles; exige revisar las reglas que controlan el acceso.

98.5. Lectura de IPv6 System Socket Information

Los registros IPv6 se interpretan con la misma estructura y una familia diferente: tcp6 o udp6. [::1] designa loopback IPv6; fe80::/10 denota link-local, cuyo alcance se relaciona con la interfaz. Un servicio puede aparecer en IPv4 e IPv6 con sockets separados, y no siempre está habilitado para recibir tráfico en ambas familias.

Ejemplo ficticio: «unbound 2314 3 udp6 [2001:db8:10::1]:53 *:*». Las direcciones 2001:db8::/32 son reservadas para documentación. No deben tomarse de la instalación examinada ni tratarse como rutas operativas.

98.6. Comodines, loopback y direcciones específicas

Notación	Qué afirma	Qué NO afirma
*:53	El socket está vinculado a un puerto en direcciones de esa familia.	No equivale a puerto abierto desde Internet.
:	Comodín de dirección y, en algunos casos, puerto sin asignación fija.	No demuestra un servicio UDP escuchando públicamente.
127.0.0.1:953	Servicio accesible por loopback IPv4 local.	No es una escucha de la interfaz WAN.
192.0.2.10:53	Escucha sobre la dirección IPv4 indicada.	No valida reglas, DNS, conectividad ni respuesta.
[::1]:123	Socket IPv6 sobre loopback.	No es exposición a clientes IPv6 remotos.



Figura 98.2. Ámbitos de escucha y necesidad de comprobar por separado reglas, rutas y políticas IPv6.

98.7. Puerto en escucha frente a conexión establecida

TCP distingue el socket de escucha de las conexiones aceptadas y de las iniciadas desde el firewall. Por defecto Netgate documenta la lista de sockets en escucha; la opción adicional «Show all socket connections», cuando está disponible en la GUI correspondiente, amplía la vista a conexiones en uso por el propio equipo. No figura entre los controles suministrados y su presencia debe verificarse en la versión concreta.

En UDP no existe un estado LISTEN idéntico a TCP ni una negociación de tres pasos. Un socket UDP comodín y un extremo remoto «*:*» pueden ser normales para un proceso que solicita servicios o recibe datagramas. Para conexiones ajenas al firewall, utilizar la tabla de estados PF.

98.8. Interpretar los procesos y puertos habituales

Proceso	Protocolo/puerto típico	Qué contrastar
unbound	TCP/UDP 53; control local según configuración	Interfaces de escucha, recursión permitida y consultas DNS.
nginx	TCP 443; eventualmente 80	Protocolo de la GUI, certificados, reglas administrativas y redirección.
kea-dhcp4	UDP 67	Interfaz DHCP, rangos, concesiones y clientes de la LAN.
ntpd	UDP 123	Interfaces NTP, servidores de tiempo y políticas de acceso.
openvpn	UDP o TCP; puerto configurable	Modo cliente/servidor, extremo local, handshake y rutas.
syslogd	UDP 514 en configuraciones pertinentes	Receptor/emisor de registros y política de acceso.
php-fpm	Sockets locales o UDP temporales según proceso	Proceso asociado: no inferir que *:* significa servicio público.
Paquetes adicionales	Según aplicación y versión	Documentación del paquete, servicio y reglas de firewall.

98.9. Por qué un mismo puerto aparece repetido

Los procesos de un servidor web pueden compartir sockets de escucha entre trabajadores; por ejemplo, varios PID de nginx pueden figurar con los mismos puertos. Ello no implica necesariamente colisión ni multiplicación de servicios. En cambio, un error de inicio que indique «Address already in use» requiere comprobar qué proceso posee el puerto y si intenta vincularse a la misma combinación de familia, dirección y protocolo.

También es normal que el mismo daemon mantenga múltiples descriptores: IPv4/IPv6, TCP/UDP, loopback y direcciones de interfaces diferentes. FD 4 y FD 7 describen recursos del proceso, no puertos externos.

98.10. IPv6 y los límites de la interpretación dual-stack

Las entradas tcp6/udp6 revelan sockets de la familia IPv6. No debe asumirse automáticamente que un socket IPv6 wildcard atiende también IPv4; depende de la configuración y de las opciones del sistema operativo. Una auditoría real comprueba IPv4 e IPv6 por separado, incluyendo las reglas de firewall, rutas, direcciones publicadas y servicios.

> PRECAUCIÓN No deshabilitar IPv6 globalmente ni cerrar todas las escuchas por el mero hecho de observar entradas tcp6 o udp6. La operación podría afectar NTP, DNS, administración, vecindad y servicios internos.

98.11. Comprobaciones desde consola: sockstat

Para una inspección puntual, los siguientes comandos son de lectura y están documentados por FreeBSD. Usarlos en consola autorizada o en Diagnostics → Command Prompt, evitando procesos interactivos o búsquedas masivas prolongadas.

Comando	Uso
sockstat -4 -l	Sockets IPv4 en escucha.
sockstat -6 -l	Sockets IPv6 en escucha.
sockstat -4 -c	Conexiones IPv4 del propio sistema.
sockstat -6 -c	Conexiones IPv6 del propio sistema.
sockstat -l -P tcp	Sockets TCP en escucha.
sockstat -l -P udp	Sockets UDP listados como escuchas vinculadas.

Comando	Uso
sockstat -l -p 53	Filtrar puertos 53 locales o remotos.
sockstat -l -w	Ampliar el ancho de columnas de direcciones.

Para profundizar en un PID concreto se puede consultar «ps -p PID -o user,pid,comm,args», sustituyendo PID por un identificador obtenido en ese momento y revisando que la salida no incluya secretos en argumentos. Los comandos exactos y sus opciones se contrastan con la versión de FreeBSD incluida en pfSense Plus.

98.12. Auditoría de exposición: cuatro comprobaciones diferentes

Una auditoría adecuada correlaciona (1) proceso y socket, (2) ámbito de la dirección local, (3) configuración del servicio y reglas de firewall, y (4) respuesta desde una red con autorización. El estado del proceso en Status → Services y los registros aportan contexto adicional; ninguna de estas comprobaciones debe sustituirse por una única captura de Sockets.



Figura 98.3. Secuencia de auditoría de un puerto inesperado sin modificar la red para obtener pruebas.

98.13. Interfaz web y administración segura

Un socket nginx en TCP/443 puede corresponder al webConfigurator, pero debe confirmarse en System → Advanced → Admin Access y con las reglas. Netgate aconseja limitar el acceso administrativo mediante reglas apropiadas, con privilegios mínimos y sin publicar la GUI libremente en Internet. El permiso de acceso puede depender de reglas especiales anti-lockout en LAN.

> PRECAUCIÓN No desactivar anti-lockout ni cambiar el puerto de administración sin disponer antes de una regla alternativa válida y un método de recuperación fuera de banda. La modificación puede bloquear de inmediato la sesión de gestión.

98.14. Resolución DNS, NTP y registro remoto

Los sockets Unbound TCP/UDP 53 deben cotejarse con Services → DNS Resolver: puertos de escucha, Network Interfaces y ACL. Netgate indica que Unbound escucha por defecto en interfaces disponibles si no se restringe expresamente. En NTP puede haber sockets por varias direcciones locales para atender clientes y origen de consultas. En Syslog, la existencia de UDP/514 no demuestra recepción remota ni entrega de registros: revisar configuración, reglas, dirección destino y pruebas controladas.

98.15. DHCP y VPN: puertos que requieren contexto

Un proceso DHCPv4 vinculado al puerto 67 y a una dirección del firewall puede ser correcto, pero la tabla no valida la entrega de concesiones. Para diagnosticar, correlacionar con Status → DHCP Leases, configuración de interfaz y registros del daemon. Del mismo modo, un proceso OpenVPN unido a UDP/TCP no verifica que el túnel esté negociado, que existan rutas correctas ni que el servidor remoto responda.

98.16. Sistemas con Multi-WAN y alta disponibilidad

En Multi-WAN, cada dirección de salida e interfaz pueden crear sockets distintos según el servicio; una aplicación que se vincula únicamente a una IP concreta puede quedar afectada por una conmutación de WAN. En HA, las VIP CARP y la asignación de sockets deben revisarse según el rol del nodo. Sincronizar configuración no implica que un proceso haya quedado activo, y una IP virtual en estado BACKUP no convierte al nodo en MASTER.

98.17. Sockets, States, pfTop y Packet Capture: funciones diferentes

Herramienta	Pregunta que responde	Limitación
Sockets	¿Qué procesos locales usan puertos y sockets?	No inventaría conexiones que atraviesan PF.
Status → Services	¿El daemon figura iniciado o detenido?	No certifica funcionamiento de aplicación.
States	¿Qué flujos está siguiendo PF y NAT?	No identifica por sí sola todo socket local.
pfTop	¿Qué estados están activos y cuánto transfieren?	No sustituye análisis por proceso y PID.
Packet Capture	¿Llega/sale realmente un paquete por esta interfaz?	Debe elegirse punto de captura y filtro.
System Logs	¿Qué errores o reinicios se han registrado?	Puede no registrar todos los fallos.

98.18. Procedimiento 1 — Inventariar puertos en escucha

1. Acceder a Diagnostics → Sockets y registrar fecha, versión y rol del equipo de forma no identificativa.
2. Separar IPv4 e IPv6, localizar las filas de servicios esperados y agrupar por proceso, protocolo y puerto.
3. Anotar si la escucha es específica, loopback o wildcard; no interpretar *:* como público.
4. Contrastar servicios principales con Status → Services y las pantallas de configuración.
5. Conservar un inventario anonimizado y compararlo con una línea base aprobada.

98.19. Procedimiento 2 — Identificar un puerto desconocido

1. Localizar Proto, Local, User, Command, PID y FD en la tabla y comprobar si hay múltiples instancias legítimas.
2. Confirmar el PID actual mediante sockstat y ps; no basarse en IDs antiguos.
3. Determinar qué componente o paquete lo inicia y consultar su configuración oficial.
4. Examinar reglas de firewall de entrada y servicios asociados, primero en IPv4 y luego en IPv6.
5. Probar el acceso únicamente desde un origen autorizado y registrar resultado sin exponer secretos.
6. Si la escucha es inesperada, escalar para decisión de deshabilitar, restringir o mantener el servicio.

98.20. Procedimiento 3 — Diagnosticar «Address already in use»

1. Comprobar en Status → Services si el servicio de destino está detenido y revisar System Logs para el mensaje exacto.
2. Localizar en Sockets el mismo puerto, protocolo y dirección de escucha; distinguir TCP/UDP y IPv4/IPv6.
3. Identificar el proceso propietario y validar si es un componente requerido (p. ej., Unbound frente a DNS Forwarder).
4. Modificar la configuración soportada para evitar conflicto, no finalizar procesos críticos a ciegas.
5. Aplicar el cambio en ventana controlada y verificar de nuevo escucha y respuesta efectiva.

98.21. Procedimiento 4 — Verificar DNS con socket presente

1. Comprobar escucha TCP/UDP 53 y la(s) dirección(es) locales de Unbound.
2. Confirmar en Services → DNS Resolver las interfaces autorizadas y las listas de acceso.
3. Lanzar una consulta de prueba desde el firewall y luego desde una red cliente permitida.
4. Examinar Firewall Logs, DNS Resolver Status y Packet Capture si las consultas fallan.
5. Comparar el éxito real de resolución con la mera presencia del socket, antes de reiniciar.

98.22. Procedimiento 5 — Auditoría del webConfigurator en IPv4/IPv6

1. Identificar sockets nginx TCP en puertos de administración por ambas familias.
2. Verificar protocolos, interfaces y puertos configurados en System → Advanced → Admin Access.
3. Revisar las reglas de gestión, aliases y el mecanismo anti-lockout sin modificar aún la configuración.
4. Realizar pruebas desde una red de administración autorizada y una red de prueba no autorizada.
5. Registrar diferencias y conservar acceso alternativo antes de cualquier cierre o cambio.

98.23. Procedimiento 6 — Investigar sockets UDP wildcard

1. Distinguir una línea local «*:*» de una escucha UDP en un puerto específico.
2. Relacionar PID y FD con el proceso vigente y con su función, sin inferir exposición por el nombre del comando.
3. Comprobar si el proceso realiza DNS, NTP, logging, monitorización o solicitudes temporales.
4. Si hay sospecha de tráfico anómalo, usar Packet Capture con un filtro limitado y revisar registros.
5. Evitar eliminar sockets manualmente; corregir la causa mediante configuración soportada.

98.24. Matriz de incidencias habituales

Síntoma	Hipótesis	Verificación segura
Puerto esperado ausente	Daemon detenido, bind fallido o interfaz deshabilitada.	Services + System Logs + sockstat -l.
Port conflict	Dos servicios usan mismo protocolo/IP/puerto.	Correlacionar PID y configuración.
Escucha en *:443	Bind wildcard configurado.	Comprobar reglas y pruebas externas; no inferir exposición.
DNS socket presente, consultas fallan	ACL, firewall, ruta o proceso sin respuesta.	DNS Lookup + captura + logs.
NTP en múltiples direcciones	Bind por interfaz u origen de consultas.	Comprobar configuración NTP, no contar procesos.
Conectividad LAN→WAN sin sockets	Es tráfico en tránsito, no proceso local.	States / pfTop / Packet Capture.
IPv4 responde; IPv6 no	Configuración o reglas distintas por familia.	Sockets IPv6 y prueba autorizada.
Nginx repetido	Workers con sockets compartidos.	Verificar PID y arranque legítimo.

98.25. Escenarios empresariales de aplicación

Escenario A — Servicio DNS corporativo no accesible

En una red de administración ficticia, los clientes de una VLAN no obtienen respuestas DNS. Sockets confirma Unbound en UDP/TCP 53, pero el problema persiste. Tras revisar interfaz de escucha y ACL, se compara con reglas en la VLAN y Packet Capture. Resultado: localizar la causa en el acceso o en el servicio, no asumir que el puerto ya garantiza resolución.

Escenario B — Auditoría de superficie de administración

Un inventario encuentra sockets nginx IPv4/IPv6 sobre un puerto de gestión. El equipo contrasta reglas LAN/WAN, alias de redes autorizadas y configuración anti-lockout. Se valida desde una zona permitida y otra bloqueada, documentando la reducción efectiva de exposición sin cortar la administración legítima.

Escenario C — Cliente VPN conectado sin servicio interno

Un túnel OpenVPN aparece operativo, pero un usuario no alcanza una aplicación. Sockets confirma que el servicio está escuchando en el firewall, lo cual no valida el tránsito hacia un servidor detrás de él. El diagnóstico se desplaza a States, rutas, reglas VPN y captura de paquetes en los puntos de entrada y salida.

98.26. Recomendaciones de seguridad y buenas prácticas

Conservar un inventario de escucha aprobada por servicio y familia IP; revisar puertos tras instalar paquetes o actualizar; evitar exponer interfaces de gestión en redes no confiables; deshabilitar servicios únicamente tras verificar dependencias; realizar pruebas externas controladas; proteger registros y capturas; documentar fecha, motivo y reversión de cambios.

Una escucha válida en loopback para control de un daemon no debe convertirse en acceso WAN. Del mismo modo, servicios básicos como DNS o NTP pueden necesitar interfaces concretas; cerrar todo indiscriminadamente deteriora la operación sin mejorar necesariamente la seguridad.

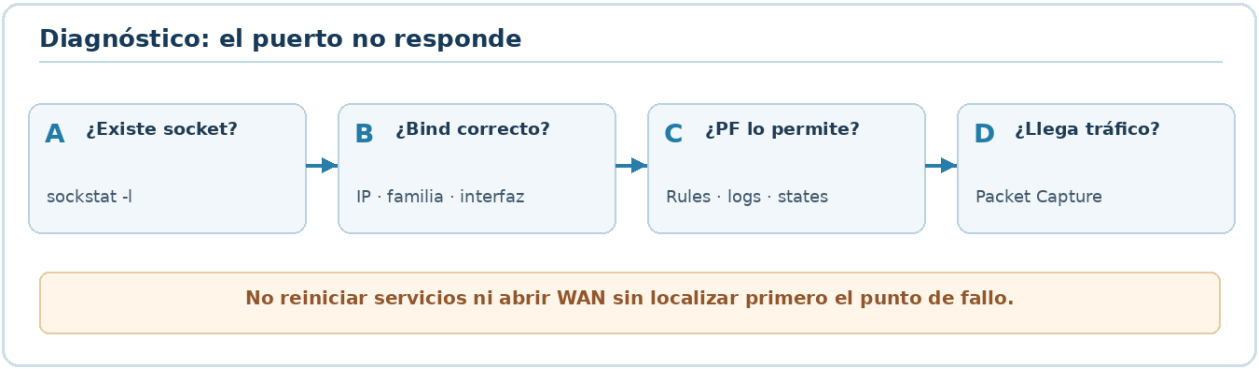


Figura 98.4. Secuencia de diagnóstico antes de modificar reglas, puertos o procesos de un sistema en producción.

98.27. Lista de comprobación antes de cerrar una incidencia

Comprobación	Evidencia mínima
Proceso identificado	Nombre, PID temporal, usuario y servicio asociado, anonimizados.
Socket y ámbito	Protocolo, dirección tipo, puerto y familia IP.
Política de acceso	Regla(s) relevantes y fuente de prueba autorizada.
Función del servicio	Consulta, handshake o respuesta de aplicación verificada.
Cambios y reversión	Responsable, ventana, copia y resultado posterior.
Seguridad de evidencias	Sin contraseñas, IP reales, identidades, certificados ni tokens.

98.28. Glosario técnico esencial

Término	Definición
Socket	Recurso de comunicación asociado a un proceso y protocolo.
Bind	Asociación de un socket a dirección local y, habitualmente, puerto.
Listen	Estado de escucha TCP en espera de conexiones entrantes.
PID / FD	Identificador del proceso / descriptor del socket dentro de él.
Wildcard	Comodín que representa múltiples direcciones o extremos.
Loopback	Comunicación con el propio host: 127.0.0.1 o ::1.
Dual-stack	Convivencia de IPv4 e IPv6 con tratamiento potencialmente distinto.
States	Tabla de sesiones gestionadas por el motor PF, diferente de los sockets del SO.

98.29. Referencias técnicas oficiales

Netgate · Viewing Active Network Sockets — https://docs.netgate.com/pfsense/en/latest/monitoring/status/sockets.html

Netgate · Diagnostics menu guide — https://docs.netgate.com/pfsense/en/latest/menuguide/diagnostics.html

FreeBSD · Manual sockstat(1), 16.0-CURRENT — https://man.freebsd.org/cgi/man.cgi?apropos=0&manpath=FreeBSD+16.0-CURRENT&query=sockstat&sektion=1

Netgate · Service Status — https://docs.netgate.com/pfsense/en/latest/monitoring/status/services.html

Netgate · Firewall States in the GUI — https://docs.netgate.com/pfsense/en/latest/monitoring/status/firewall-states-gui.html

Netgate · DNS Resolver Configuration — https://docs.netgate.com/pfsense/en/latest/services/dns/resolver-config.html

Netgate · Admin Access — https://docs.netgate.com/pfsense/en/latest/config/advanced-admin.html

Netgate · Allowing Remote Access to the GUI — https://docs.netgate.com/pfsense/en/latest/recipes/remote-firewall-administration.html

Netgate · NTP Server Configuration — https://docs.netgate.com/pfsense/en/latest/services/ntpd/server.html

Netgate · Packet Capture GUI — https://docs.netgate.com/pfsense/en/latest/diagnostics/packetcapture/webgui.html

Netgate · Packet Capturing — https://docs.netgate.com/pfsense/en/latest/diagnostics/packetcapture/index.html

99 Diagnostics → States

Tabla de estados · NAT · sesiones activas · filtrado · eliminación selectiva · recuperación

La tabla de estados revela cómo PF conserva y reconoce los flujos permitidos. Su lectura permite investigar rutas, traducciones NAT y conexiones activas sin confundir la existencia de un estado con la disponibilidad de una aplicación.

ADVERTENCIA La eliminación de estados interrumpe conexiones en curso. Para operaciones de alcance amplio, disponer de respaldo, autorización y una vía de acceso alternativa al firewall.

99.1. Objetivo y ruta exacta

Ruta: Diagnostics → States (pestañas States y Reset States). Esta página permite inspeccionar conexiones que atraviesan pfSense Plus y conexiones destinadas al propio firewall. El motor PF mantiene estados que autorizan el tráfico de retorno asociado a una comunicación permitida, sin volver a evaluar todas las reglas para cada paquete.

States permite consultar y eliminar estados. Reset States reúne operaciones de limpieza de la tabla de estados y del seguimiento de orígenes. Revisar el alcance de cada acción: un restablecimiento general puede interrumpir comunicaciones ajenas a la incidencia.

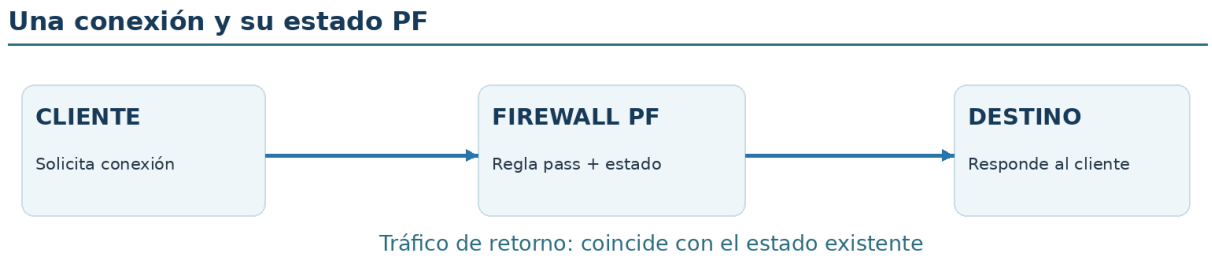


Figura 99.1. Creación y consulta de un estado durante una comunicación permitida.

99.2. Fundamentos de firewall con estado

En un filtrado con estado, la regla que permite el primer paquete crea una entrada en memoria: direcciones, puertos o identificadores, protocolo, dirección, temporizadores y contadores. Los siguientes paquetes que coinciden con esa entrada pueden continuar pasando conforme a la política fijada cuando el estado se creó. Esto explica que modificar una regla no siempre cierre las conexiones ya establecidas.

La tabla de estados no es un registro histórico. Sus entradas aparecen, cambian y caducan; su tamaño depende del tráfico, los temporizadores, el número máximo de estados y las políticas de cada regla. La observación puntual debe combinarse con logs, Packet Capture, Routes y pfTop.

99.3. Pestañas, ruta y controles principales

Elemento	Función	Consecuencia
States	Consultar y filtrar estados activos	La consulta es no disruptiva; la eliminación selectiva sí interrumpe flujos.
Reset States	Limpiar la State Table o la Source Tracking Table	Acción global potencialmente muy disruptiva.
Interface	Restringir la búsqueda a una interfaz o all	No cambia el encaminamiento ni borra estados.
Filter expression	Buscar coincidencia literal de texto	No interpreta expresiones regulares.
Rule ID	Acotar entradas relacionadas con una regla	El identificador debe corresponder a la configuración consultada.

99.4. State Filter: selección de interfaz

El selector Interface muestra, según la configuración del sistema, WAN, LAN, interfaces adicionales, IPsec, loopback y all. También pueden intervenir interfaces de túneles o entradas relacionadas con ellos. La lista exacta varía por hardware, asignaciones y servicios activos.

Elegir all permite investigar la misma comunicación desde diferentes puntos de observación. Seleccionar una interfaz reduce el ruido cuando se revisan estados de VPN, NAT o una red concreta. No debe deducirse que la misma sesión repetida en dos interfaces representa necesariamente dos conexiones de usuario.

99.5. State Filter: Filter expression

El campo Filter expression aplica coincidencias de texto simples a las columnas mostradas. Por ejemplo, una dirección individual de documentación, un puerto o un nombre de protocolo puede localizar filas relacionadas. Según Netgate, este campo NO procesa expresiones regulares: los caracteres especiales de regex no tienen la semántica de un motor regex.

Ejemplo documental: filtrar por 192.0.2.40 para localizar conexiones atribuidas a ese origen; filtrar por 443 para restringir posibles servicios HTTPS, recordando que es una coincidencia textual y conviene verificar las columnas.

El filtrado por una IP o subred puede habilitar una acción Kill States para eliminar estados relacionados con esa dirección o red. La búsqueda por nombre, puerto o texto no debe confundirse con una selección exacta de conexiones que se van a terminar.

99.6. State Filter: Rule ID

Rule ID limita la consulta por identificador de regla y ayuda a correlacionar entradas con Firewall → Rules y sus estadísticas. Las opciones y el identificador efectivo pueden cambiar al modificar las reglas. Los números del motor no son una etiqueta administrativa inmutable.

CONSEJO Antes de eliminar estados por una regla, revisar sus coincidencias, el sentido de la interfaz y las traducciones NAT; evitar actuar únicamente a partir de un identificador sin contexto.

99.7. Estados: columnas y unidades

Columna visible	Interpretación técnica	Cómo debe leerse
Interface	Interfaz asociada a la entrada de estado	No prueba por sí sola la ruta de extremo a extremo.
Protocol	TCP, UDP, ICMP, ICMPv6 y otros	Determina el significado de estados y puertos.
Origen → destino	Direcciones, puertos o tipos ICMP; puede reflejar NAT	Paréntesis: dirección original o traducida según el tipo de NAT.
State	Valores a ambos lados separados por dos puntos	El lado izquierdo corresponde al origen y el derecho al destino.
Packets	Contadores de paquetes observados por ambos lados	No es una tasa en paquetes por segundo.
Bytes	Volumen acumulado que coincide con el estado	No es una medición instantánea del ancho de banda.
Actions	Icono de papelera por fila	Elimina ese estado con efecto sobre la comunicación.

99.8. Interpretación de Packets y Bytes

Los dos contadores separados por “/” expresan observaciones de ambos sentidos de un estado. Por ejemplo, «42 / 37» paquetes y «31 KiB / 44 KiB» muestran tráfico observado hacia cada lado; el dato no representa una velocidad ni permite atribuir la diferencia por sí solo a pérdida o a congestión.

Una misma sesión puede figurar asociada a más de una interfaz por el trayecto y la traducción. Para estimar consumo no se deben sumar indiscriminadamente las filas duplicadas. El análisis de tasas actuales

se complementa con Diagnostics → pfTop (vista Speed) o Status → Traffic Graph; para histórico se consulta Monitoring.

99.9. Estados TCP más habituales

Estado	Interpretación	Comprobación recomendada
SYN_SENT:CLOSED	Hay intento de apertura sin respuesta observada en el lado remoto	Revisar destino, ruta de retorno, reglas y SYN/SYN-ACK.
ESTABLISHED:ESTABLISHED	El firewall ha observado el establecimiento en ambos lados	Comprobar aplicación, TLS, DNS y respuesta real.
FIN_WAIT / TIME_WAIT	La comunicación está cerrándose o esperando expiración	No asumir avería si desaparece al vencer el timer.
CLOSED	El lado indicado está cerrado o carece de tráfico relevante	Comparar temporizadores y registros.

99.10. Estados UDP, ICMP e ICMPv6

Estado	Caso típico	Matiz
SINGLE:NO_TRAFFIC	Datagrama UDP transmitido sin respuesta observada	UDP no usa handshake; puede ser normal.
SINGLE:MULTIPLE	Una solicitud y varias respuestas	Frecuente en determinados intercambios UDP.
MULTIPLE:MULTIPLE	Paquetes en ambos sentidos	No garantiza que el contenido sea correcto.
NO_TRAFFIC:SINGLE	Tráfico sin respuesta de retorno registrada	Común en multicast, broadcast y descubrimiento.
NO_TRAFFIC:NO_TRAFFIC	Estado sin nivel bidireccional de tráfico en algunos protocolos	Interpretar junto a contadores y protocolo.
0:0	Sin niveles TCP/UDP asociados	Normal en determinados estados ICMP.

99.11. Ejemplo didáctico de una conexión TCP con NAT de salida

En un ejemplo totalmente ficticio, el equipo 192.0.2.40:51680 inicia una sesión TLS con 203.0.113.20:443; pfSense utiliza 198.51.100.2:49120 como dirección y puerto de salida. Es habitual encontrar una representación del lado interno y otra del lado externo; en la traducción NAT, la dirección original puede aparecer entre paréntesis.

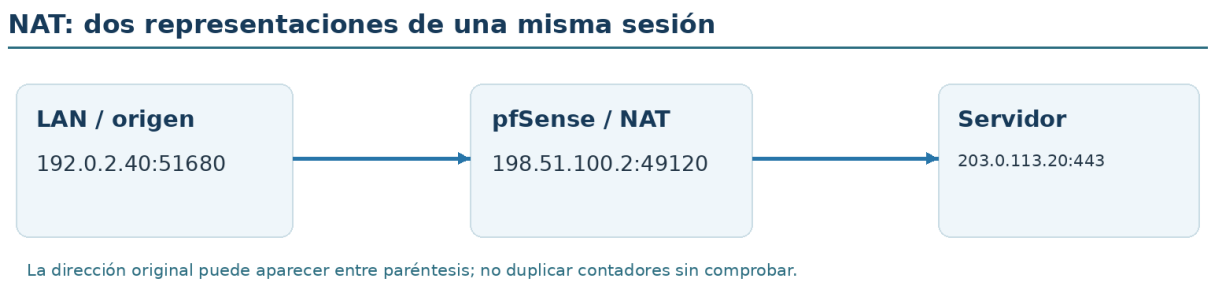


Figura 99.2. Correspondencia conceptual entre origen, traducción y destino utilizando redes TEST-NET.

En el tráfico con redirección entrante, la traducción afecta al destino; por tanto, la posición de la dirección entre paréntesis cambia. Nunca identificar una IP entre paréntesis como “IP de origen” sin comprobar la modalidad de NAT.

99.12. Conexiones internas, VPN y interfaces

Al observar una comunicación desde LAN hacia una subred remota mediante OpenVPN pueden aparecer filas asociadas a LAN y a la interfaz del túnel con contadores semejantes. Para distinguirlas, consultar la interfaz, el estado y las rutas reales, y contrastar con Status → OpenVPN.

En IPsec convencional basado en políticas, la relación con SPD y SAD exige un análisis diferente del usado para interfaces de túnel asignadas o VTI. La ausencia de una interfaz VPN concreta en la tabla no demuestra que el túnel esté caído.

99.13. Filtrado práctico reproducible

Objetivo	Filtro inicial	Segunda evidencia
Conexiones de una estación	IP 192.0.2.40	Regla implicada y estados por interfaz
Comprobación HTTPS	Puerto 443 y dirección de destino	Captura TCP y prueba de aplicación
Servidor interno publicado	IP 203.0.113.50 y puerto documentado	NAT y logs de firewall
Túnel remoto	Subred 198.51.100.0/24	Estado de VPN, rutas y retorno
Tráfico sin respuesta	Estado SINGLE:NO_TRAFFIC	Packet Capture y reachability del destino

99.14. Acciones individuales: eliminar un estado

La papelera situada al final de una fila elimina la entrada de estado concreta. La comunicación puede interrumpirse y la aplicación iniciar otra sesión; con las reglas vigentes, el siguiente flujo puede recrear estado. La eliminación no modifica permanentemente las reglas ni los objetos NAT.

Procedimiento seguro: (1) registrar hora, origen, destino y servicio; (2) filtrar y comprobar el estado exacto; (3) obtener autorización si el flujo es crítico; (4) eliminar exclusivamente la fila necesaria; (5) observar la recreación y validar el servicio; (6) conservar la evidencia del resultado.

PRECAUCIÓN Una conexión hacia la propia GUI, una VPN de administración o una sesión remota puede depender del estado que se elimina. Tener otro acceso de gestión antes de actuar.

99.15. Pestaña Reset States: opciones documentadas

Control oficial	Qué elimina	Riesgo principal
State Table	Entradas activas de conexión y sus asociaciones	Caída temporal o total de sesiones TCP, VPN y aplicaciones.
Source Tracking	Tabla de seguimiento de fuentes empleada por límites y políticas	Pérdida de seguimiento anterior y alteración de límites activos.
Reset	Ejecuta el borrado seleccionado tras confirmación	La GUI puede desconectarse hasta reabrir sesión.

La documentación vigente describe el proceso: Diagnostics → States → Reset States; marcar State Table y/o Source Tracking, pulsar Reset y confirmar con OK. La forma exacta de la pantalla puede variar según la revisión de pfSense Plus. Esta explicación procede de Netgate, no de una captura adicional.

99.16. Cuándo se justifica Reset States

Tras cambios relevantes de NAT, reglas de bloqueo o Traffic Shaping, las sesiones existentes pueden conservar el tratamiento anterior hasta que caduquen. En situaciones controladas, el borrado global obliga a que los nuevos flujos se evalúen con las reglas actuales.

No usarlo como primera reacción ante “Internet lento”. Antes deben investigarse gateways, DNS, rendimiento de interfaces, rutas, reglas, estado de VPN y recursos del sistema. En producción, preferir borrado por IP o conexión específica cuando el fallo esté acotado.

99.17. Procedimiento de Reset States planificado

- Confirmar ventana de mantenimiento, alcance, dependencia de VPN, VoIP, sesiones de terminal y acceso administrativo.
- Exportar la configuración vigente y registrar los servicios críticos que deberán reconectarse.
- Verificar acceso por consola o vía alternativa y disponibilidad de responsables de aplicaciones.
- Consultar States y pfInfo; anotar recuento de estados y resultados del filtro relevante.
- En Reset States seleccionar exclusivamente State Table o Source Tracking según la necesidad.
- Pulsar Reset, confirmar y asumir la pérdida momentánea de la sesión de administración.
- Volver a conectar, comprobar gateways/VPN/DNS y verificar que nuevas sesiones se establecen.
- Documentar incidentes, hora de intervención y resultados; si persisten, investigar la causa raíz.

99.18. Importancia de Source Tracking

La Source Tracking Table mantiene información auxiliar sobre orígenes para controles de sesiones, límites por fuente y decisiones asociadas. Su borrado no es equivalente a eliminar reglas de firewall ni a vaciar la lista de concesiones DHCP. En condiciones normales no hace falta reiniciarla al investigar una sola conexión.

Si se aplican max-src-conn, max-src-states, rate limits u otras protecciones por origen, observar pfInfo y las estadísticas de reglas antes de vaciar Source Tracking: puede cambiar temporalmente el comportamiento de contadores y restricciones.

Comprobaciones antes de limpiar Source Tracking

Situación	Qué consultar	Decisión prudente
Exceso de sesiones desde un mismo origen	pfInfo y contadores por regla	Aplicar límites tras investigar la causa.
Bloqueo por max-src-states	Regla con límite de estados por fuente	Corregir política o cliente, no limpiar indiscriminadamente.
Sospecha de saturación por conexiones nuevas	Tasa de inserciones y registros de firewall	Identificar IP origen o aplicación afectada.

99.19. Diagnóstico guiado: existe estado pero no hay servicio

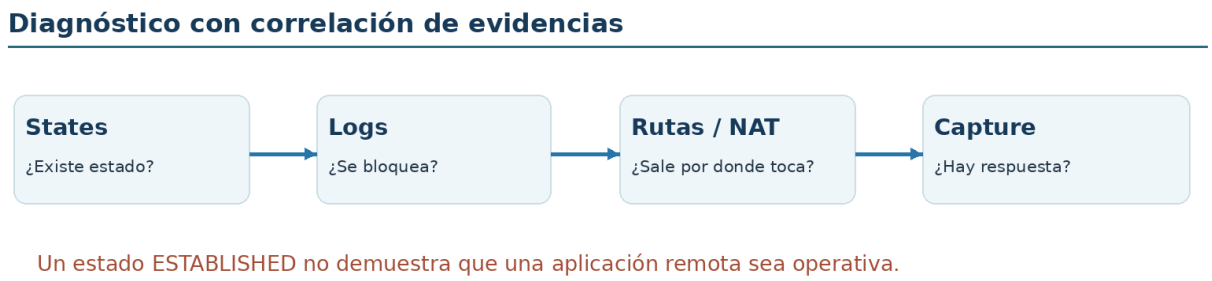


Figura 99.3. Secuencia de corroboración: States, Logs, Routes/NAT y Packet Capture.

Un estado ESTABLISHED:ESTABLISHED indica que el firewall ha observado la negociación TCP, no que la aplicación haya respondido correctamente. Comprobar DNS, certificado TLS, permisos del servicio, negociación de aplicación y problemas de MTU/MSS; emplear pruebas del mismo origen real cuando corresponda.

99.20. Diagnóstico guiado: no se crea estado

Si no aparece la conexión esperada, comprobar primero que el equipo realmente genera tráfico. Después verificar interfaz de entrada, destino, VLAN, ruta, reglas de firewall y eventuales bloqueos anteriores a la creación de estado. Netgate recomienda combinar un intento de conexión con la consulta inmediata de States y los registros del firewall.

Observación crucial: la inexistencia de un estado no identifica por sí sola la causa. Puede deberse a que el paquete no llegó, fue bloqueado, se trató sin estado, terminó antes de consultar, o el filtro está demasiado restringido.

99.21. Multi-WAN y estados anteriores al cambio de enlace

Cuando cambia el gateway de salida, los estados que conservan información de routing/NAT de la ruta anterior pueden impedir una recuperación fluida. En entornos Multi-WAN, las opciones de eliminación por fallo de gateway y el policy routing influyen en qué estados se purgan; no es correcto borrar la tabla completa por defecto.

Antes de forzar el failover, consultar Status → Gateways, la política de la regla, la traducción NAT y la ruta de retorno. Después del cambio, validar con nuevas conexiones hacia destinos de prueba y comprobar que realmente salen por el enlace esperado.

99.22. VPN, comunicaciones persistentes y sesiones sensibles

Servicio	Efecto potencial del borrado	Validación posterior
OpenVPN / WireGuard / IPsec	Interrupción de tráfico de administración y túneles activos	Handshake, rutas, retorno y recursos remotos.
RDP / SSH	Desconexión o reconexión de sesión	Reestablecer sesión y comprobar transferencia.
VoIP / streaming	Cortes de media o control	Llamada de prueba y métricas de calidad.
ERP / bases de datos	Reintentos o transacciones interrumpidas	Log de aplicación y operaciones de lectura/escritura.
Monitorización y DNS	Pérdida puntual de sondeos o consultas	Nuevos tests desde clientes autorizados.

99.23. Comandos de inspección sin cambios

Comando orientativo	Qué inspecciona	Precaución
pfctl -ss	Listado de estados actuales	Puede generar mucha salida; limitar en sistemas cargados.
pfctl -si	Estadísticas y número de estados PF	Lectura acumulada desde el último reinicio/limpieza de contadores.
pfctl -vvs rules	Reglas cargadas con contadores e identificadores	La sintaxis de salida varía con versión y configuración.
netstat -rn	Rutas del sistema	No revela por sí solo policy routing PF.

No se incluyen comandos destructivos de consola como receta genérica: el borrado se realiza preferentemente desde el control específico de la GUI y tras confirmar su alcance.

99.24. Matriz de incidencias y decisiones

Síntoma	Hipótesis	Comprobación no disruptiva	Acción proporcional
SYN_SENT:CLOSED persistente	Sin respuesta SYN-ACK	Capture, firewall remoto y rutas	Corregir ruta o filtrado.
SINGLE:NO_TRAFFIC UDP	Respuesta ausente	Capturar dos extremos y revisar DNS/UDP	Corregir retorno; evitar reset global.
Sesión antigua usa NAT anterior	Estado heredado	NAT actual y par original/traducido	Eliminar estados del equipo afectado.
VPN levanta pero no pasa tráfico	Ruta, NAT o firewall	States + status VPN + Routes	Corregir reglas antes de reiniciar.

Síntoma	Hipótesis	Comprobación no disruptiva	Acción proporcional
Tras cambio de WAN no reconecta	Estado asociado al gateway previo	Gateway, policy routing, fuente NAT	Borrado selectivo si es preciso.
Tabla cerca del límite	Alta concurrencia o ataque	pfInfo, State Summary y Logs	Investigar causa y dimensionar.

99.25. Buenas prácticas de seguridad y disponibilidad

• Priorizar inspección y filtrado antes de cualquier acción destructiva.
• Registrar hora, origen, destino y regla; no compartir exportaciones sin anonimizar.
• Evitar Reset States a través de una VPN cuyo estado dependa del propio firewall.
• Aplicar control de cambios para servicios críticos, alta disponibilidad y enlaces redundantes.
• Separar la evidencia de estado de la evidencia de conectividad real de aplicación.
• Conservar un camino de recuperación y un plan de validación pre/post intervención.

99.26. Glosario técnico

Término	Definición
State	Entrada PF que sigue un flujo permitido y sus respuestas.
NAT	Traducción de direcciones y/o puertos; puede modificar origen o destino.
Source Tracking	Tabla de seguimiento de orígenes para políticas y límites.
Rule ID	Identificador de regla que ayuda a correlacionar un estado.
ESTABLISHED	Condición TCP de conexión negociada desde la perspectiva del estado.
Timeout	Tiempo de expiración de un estado si no recibe nuevo tráfico.
Policy routing	Selección de gateway mediante reglas PF, distinta de ruta predeterminada.

99.27. Ficha operativa de comprobación y reversión

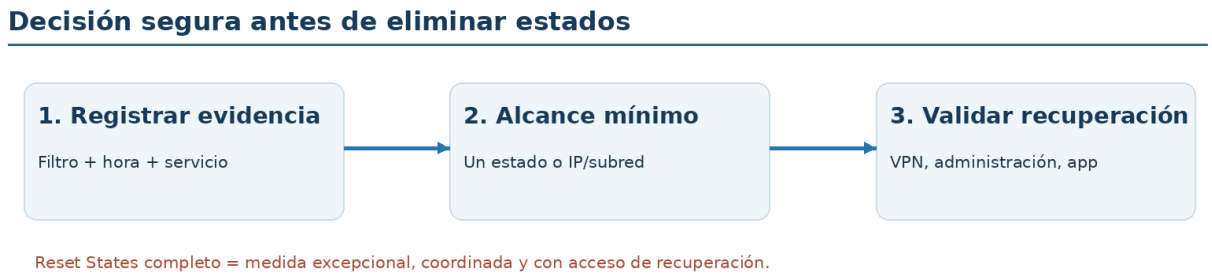


Figura 99.4. Ruta de actuación proporcionada: evidenciar, limitar alcance y validar la recuperación.

Antes	Durante	Después
Confirmar ventana de cambio y soporte	Aplicar filtro y comprobar IP/regla	Repetir consulta y probar comunicación
Registrar estado original y servicios	Eliminar solo lo necesario	Comprobar retorno, DNS, VPN, GUI
Verificar consola alternativa	Evitar simultanear cambios de NAT	Guardar ticket, resultado y tiempos

99.28. Caso práctico: sesión que conserva un NAT anterior

Supóngase que un técnico modifica una regla de NAT para que las nuevas conexiones desde 192.0.2.40 utilicen 198.51.100.3. La tabla de estados sigue mostrando una sesión antigua traducida a 198.51.100.2. Esto no significa que la nueva regla se haya aplicado incorrectamente: el flujo ya establecido puede conservar la traducción que tenía cuando se creó.

Primero se confirma que la configuración NAT vigente es correcta y se identifican solo las conexiones del origen afectado. A continuación se registra la evidencia, se advierte al usuario de la reconexión necesaria y se eliminan únicamente los estados de la IP o de la sesión concreta. El cliente inicia otra conexión y se verifica que la nueva traducción aparece en States y que el servicio responde desde el extremo remoto.

99.29. Caso práctico: la VPN figura conectada pero el recurso falla

Una VPN puede mostrar su túnel activo mientras una aplicación remota falla. El administrador debe comparar el flujo en las interfaces LAN y VPN, consultar la política de enrutamiento y comprobar que el tráfico de retorno vuelve por el camino previsto. Los estados ESTABLISHED o MULTIPLE:MULTIPLE son indicios de intercambio de paquetes, no prueba concluyente de que los permisos de aplicación o el servicio remoto sean correctos.

Observación	Interpretación posible	Prueba proporcionada
No aparece el flujo	El tráfico no llega o lo bloquea una regla	Packet Capture y System Logs
Solo aparece en LAN	No se encamina correctamente al túnel	Routes y reglas de gateway
Aparece en LAN y VPN	Hay tránsito, pero puede faltar retorno	Captura en ambos sentidos
Estado con tráfico bidireccional	Red funcional a nivel de paquetes	Validar aplicación y autenticación

En los dos escenarios, restablecer toda la tabla sería una medida desproporcionada antes de conocer el alcance del problema. El objetivo es identificar la causa y aplicar el cambio mínimo que permita reproducir y verificar la corrección.

99.30. Referencias oficiales y normativas

Netgate. Viewing Firewall States in the GUI — https://docs.netgate.com/pfsense/en/latest/monitoring/status/firewall-states-gui.html

Netgate. Reset State Table / Source Tracking Table — https://docs.netgate.com/pfsense/en/latest/monitoring/status/firewall-states-reset.html

Netgate. Firewall States — https://docs.netgate.com/pfsense/en/latest/monitoring/status/firewall-states.html

Netgate. Troubleshooting Firewall Rules — https://docs.netgate.com/pfsense/en/latest/troubleshooting/firewall.html

Netgate. Rule Methodology — https://docs.netgate.com/pfsense/en/latest/firewall/rule-methodology.html

Netgate. Advanced Firewall & NAT — https://docs.netgate.com/pfsense/en/latest/config/advanced-firewall-nat.html

Netgate. Advanced Networking — https://docs.netgate.com/pfsense/en/latest/config/advanced-networking.html

Netgate. Gateway Status — https://docs.netgate.com/pfsense/en/latest/monitoring/status/gateways.html

Netgate. Firewall States Summary — https://docs.netgate.com/pfsense/en/latest/monitoring/status/firewall-states-summary.html

Netgate. pfInfo — https://docs.netgate.com/pfsense/en/latest/monitoring/status/pfinfo.html

Netgate. pfTop — https://docs.netgate.com/pfsense/en/latest/monitoring/status/pftop.html

Netgate. Miscellaneous: State Killing on Gateway Failure — https://docs.netgate.com/pfsense/en/latest/config/advanced-misc.html

100 Diagnostics → States Summary

Análisis agregado de estados · IP y pares · protocolos · puertos · diagnóstico

El resumen de estados transforma una tabla de conexiones individuales en cuatro perspectivas de actividad por dirección, por destino y por parejas. Su valor está en orientar una investigación sin confundir actividad con amenaza ni recuentos con volumen de tráfico.

PRECAUCIÓN Esta pantalla es de consulta, pero puede exigir mucha memoria y tiempo de proceso cuando la tabla PF es grande. Un número elevado de estados no acredita por sí solo un ataque; antes de bloquear o limpiar estados, verificar servicio, usuarios y efecto operativo.

100.1. Finalidad y ruta de acceso

Ruta de administración: Diagnostics → States Summary. El informe se obtiene a partir de las conexiones registradas en la tabla de estados PF; no es una estadística histórica ni el equivalente de un flujo NetFlow. La página documentada muestra cuatro bloques de resumen y, en cada uno, un desglose por protocolo y puertos.

Es distinta de Diagnostics → States, que permite estudiar y eliminar entradas individuales o agrupadas, y de Diagnostics → pfTop, orientado a observar los estados con vistas y ordenaciones alternativas. Los cuadros de este capítulo representan exclusivamente la información agregada.

100.2. Cómo se genera el resumen

PF mantiene una entrada de estado para reconocer tráfico de una conexión y permitir las respuestas correspondientes sin repetir toda la evaluación de reglas. States Summary analiza esa tabla e identifica direcciones participantes, protocolo, número de estados y diversidad de puertos. El resultado es una instantánea variable: un navegador que abre varias sesiones puede alterar los valores de una consulta a la siguiente.

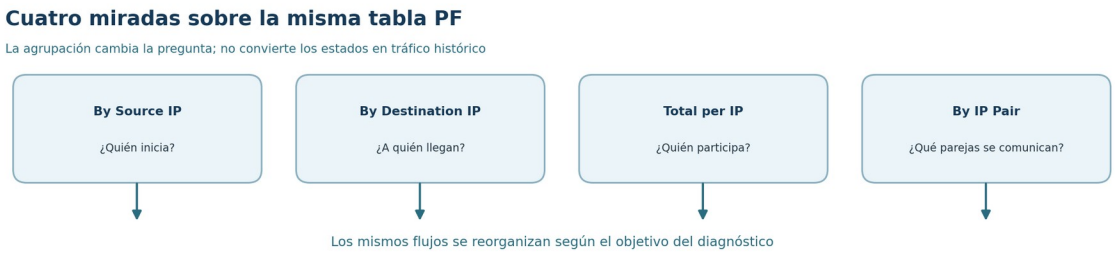


Figura 100.1. Cuatro agrupaciones para investigar una misma tabla de conexiones.

100.3. Estructura general de la pantalla

Bloque visible	Agrupación	Pregunta de diagnóstico
By Source IP	Dirección IP de origen	¿Qué origen acumula más conexiones?
By Destination IP	Dirección IP de destino	¿Qué host o servicio recibe más conexiones?
Total per IP	Dirección IP participante como origen o destino	¿Qué equipos concentran actividad en conjunto?
By IP Pair	Pareja de direcciones origen → destino	¿Entre qué extremos existe una concentración de estados?

Estas agrupaciones son vistas de lectura. Para localizar o eliminar un estado concreto se utiliza Diagnostics → States. La disponibilidad de filtros o detalles adicionales puede cambiar con la versión de pfSense Plus.

100.4. Columnas comunes: IP y # States

IP identifica la dirección o el par que agrupa las entradas. En By IP Pair se presenta con una flecha direccional; en las otras vistas aparece una dirección individual. # States a la derecha de IP es el número total de entradas atribuidas a esa agrupación. Una misma dirección puede figurar en varios bloques porque las agrupaciones responden a preguntas diferentes.

No debe sumarse el total de By Source IP con By Destination IP como si representaran conexiones independientes: cada flujo puede contribuir a ambas categorías, y su representación a través de NAT y distintas interfaces requiere contrastar la vista original de States.

100.5. Subencabezado Protocol counts y segunda columna # States

Protocol counts despliega uno o varios protocolos bajo una misma IP o pareja. La columna Protocol identifica tcp, udp, icmp, ipv6-icmp u otros protocolos presentes; el segundo # States expresa cuántas entradas del grupo pertenecen a cada protocolo, no el total global del firewall. Si una dirección tiene varios protocolos, cada uno puede aparecer en una fila separada.

IP de documentación	# States (IP)	Protocol	# States (protocolo)
192.0.2.15	7	tcp	5
		udp	2
203.0.113.20	3	tcp	3

Ejemplo didáctico: el primer equipo tiene siete estados asociados: cinco TCP y dos UDP. Las cifras son inventadas. Si el diseño de la tabla combina celdas visualmente, no debe atribuirse el total de la IP a la última línea de protocolo.

100.6. Source Ports y Dest. Ports: diversidad de puertos

Las dos columnas indican el número de puertos de origen y destino representados por las conexiones del grupo y protocolo. No son contadores de paquetes ni el número de puertos actualmente abiertos en escucha. Al pasar el cursor sobre las cifras, la interfaz puede mostrar la relación completa de puertos de acuerdo con la documentación oficial de Netgate.



Figura 100.2. Cinco conexiones TCP pueden usar cinco puertos de origen y un solo puerto de destino.

Una cifra Source Ports alta y Dest. Ports baja es compatible con muchas sesiones hacia un servicio conocido (por ejemplo, HTTPS). Una cifra Dest. Ports alta merece estudiar si se trata de múltiples aplicaciones, descubrimiento, sondeo o una actividad legítima de administración; por sí sola no confirma un escaneo.

100.7. By Source IP: localizar orígenes activos

Agrupa los estados según la IP de origen. Es útil para encontrar clientes que abren muchas sesiones, aplicaciones con reconexiones frecuentes, equipos con numerosas conexiones de acceso remoto o fuentes potenciales de sondeos. Primero compare el número total; después revise la proporción TCP/UDP y la diversidad de puertos.

Patrón observado	Hipótesis posible	Verificación
Muchos estados TCP y un destino de servicio	Cliente que abre numerosas conexiones normales	By IP Pair y puertos del servicio

Patrón observado	Hipótesis posible	Verificación
Múltiples puertos de destino y estados de corta duración	Escaneo o herramienta de administración	pfTop, logs, autorización del origen
Muchos estados UDP persistentes	Aplicación multimedia, VPN o consulta repetitiva	Puertos, tiempo de vida y capturas

100.8. By Destination IP: identificar servicios receptores

Agrupa los estados por el destino. Permite detectar servidores internos muy utilizados, servicios externos que concentran conexiones o un destino único que recibe numerosas solicitudes de orígenes distintos. Un servidor DNS, un proxy o un concentrador de aplicaciones puede ser legítimamente un gran destino.

Para investigar un supuesto ataque a un servidor, combine el recuento con Firewall Logs, errores de aplicación, picos de conexiones, uso de CPU y capturas. La tabla no mide por sí sola solicitudes HTTP, autenticaciones fallidas ni volumen de bytes.

100.9. Total per IP: participación global de cada dirección

Reúne la actividad de una dirección como participante de los estados, independientemente de que aparezca como origen o destino. Resulta útil para encontrar equipos muy comunicativos o pasarelas y servidores centrales. No es correcto equiparar el valor con la suma de los campos By Source IP y By Destination IP sin comprobar cómo representa el sistema las conexiones y las traducciones.

100.10. By IP Pair: relaciones entre dos extremos

Agrupa los estados entre parejas de direcciones orientadas como origen → destino. Este bloque permite responder a una pregunta más precisa que las vistas anteriores: ¿quién habla con quién? Es adecuado para localizar un cliente que mantiene muchas sesiones con un servidor específico, analizar una aplicación entre sedes o investigar patrones de puertos de un mismo par.

Pareja ilustrativa	Estados	Interpretación inicial
192.0.2.15 → 203.0.113.20	5	Un cliente hacia un servidor; contrastar servicio/puertos
192.0.2.30 → 198.51.100.25	11	Relación concentrada que requiere verificar legitimidad
2001:db8:1::10 → 2001:db8:2::20	2	Par IPv6 global de documentación; revisar protocolo

100.11. IPv4, IPv6 y protocolos sin puertos TCP/UDP

Las direcciones IPv6 pueden figurar junto a IPv4. Las direcciones fe80::/10 son link-local y solo se interpretan con su contexto de interfaz; ff02::/16 es multicast de ámbito local. En ICMP e ICMPv6 la presentación puede emplear identificadores y tipos de mensajes en campos equivalentes a puertos: no deben leerse como puertos TCP/UDP de escucha.

Las entradas multicast o broadcast tampoco prueban una comunicación individual con un servidor remoto. Para determinar el mensaje concreto, su periodicidad y su legitimidad, utilice Packet Capture y consulte los tipos ICMPv6, destinos multicast y protocolos implicados.

100.12. Contabilización y correlación con NAT

La traducción NAT puede modificar las direcciones o los puertos visibles en el recorrido. Por eso, un mismo flujo puede requerir más de una observación en Diagnostics → States para distinguir el cliente original de la dirección traducida. No debe atribuirse una dirección pública automáticamente a un equipo interno, ni sumarse una visualización por interfaz como nuevas sesiones de aplicación.



Figura 100.3. Correspondencia conceptual entre cliente, traducción NAT y destino de documentación.

En acceso entrante con Port Forward, la transformación afecta al destino. En Outbound NAT, al origen. Antes de identificar el equipo o modificar una regla, correlacione ambas direcciones y puertos con la entrada original, la regla NAT y la interfaz pertinente.

100.13. Relación con VPN y conexiones entre sedes

Los túneles OpenVPN y WireGuard pueden originar o transportar flujos que aparecen asociados a direcciones de redes remotas y a la interfaz del túnel. IPsec en modo túnel tradicional usa políticas de IPsec; los túneles VTI se integran más directamente con rutas. States Summary no describe toda esa topología ni prueba que los servicios finales funcionen.

Un número elevado de estados entre un cliente y un servidor remoto puede ser normal en administración remota, RDP, bases de datos o aplicaciones que abren varias sesiones. Si la VPN está “conectada” pero la aplicación falla, verificar rutas, reglas, retorno, MTU y estados concretos antes de culpar a la cantidad de sesiones.

100.14. Multi-WAN y persistencia de estados

En Multi-WAN, una sesión puede conservar una traducción o gateway determinado mientras su estado continúe activo. Los grupos de gateway, policy routing, NAT de salida y sticky connections influyen en el comportamiento, pero States Summary no indica por sí solo el gateway real elegido. Para eso deben consultarse los estados concretos y las herramientas de gateways y rutas.

ADVERTENCIA Un cambio de reglas NAT o policy routing no necesariamente modifica conexiones ya establecidas. Eliminar estados selectivos o limpiar la tabla completa puede ser necesario para reproducir un cambio, pero esta última operación interrumpe sesiones y debe tener autorización y plan de recuperación.

100.15. Qué no permiten concluir los recuentos

Dato visible	Lo que sí indica	Lo que NO demuestra
# States alto	Muchas entradas asociadas a un grupo	Ataque, saturación o caudal alto
Source Ports alto	Variedad de puertos de origen	Muchos usuarios ni muchos servicios
Dest. Ports alto	Variedad de puertos de destino	Escaneo sin evidencia adicional
TCP abundante	Diversas sesiones TCP	Que el servicio responde correctamente
Una dirección ausente	Sin estados visibles para ese valor en la instantánea	Que el equipo esté desconectado

100.16. Ejemplo 1: equipo con muchos estados

Procedimiento de investigación no disruptiva

1. Abrir Diagnostics → States Summary y localizar la dirección bajo By Source IP o Total per IP.
2. Registrar la hora de observación, el total, los protocolos y los recuentos de puertos sin copiar identificadores sensibles a informes compartidos.
3. Examinar By IP Pair para determinar los destinos dominantes y comprobar si los servicios corresponden al trabajo esperado.

4. Consultar pfTop para distinguir estados antiguos de actividad reciente; correlacionar con los registros de firewall y aplicaciones.

5. Si persiste la sospecha, obtener una captura acotada y documentar el origen; intervenir solo sobre estados concretos previa autorización.

100.17. Ejemplo 2: servidor con destinos de puertos anómalos

Validación de un posible escaneo o sondeo

1. Localizar el servidor en By Destination IP; observar protocolos y variedad de puertos de destino.
2. Revisar pares de direcciones para determinar si el patrón proviene de un origen o de muchos.
3. Consultar System Logs → Firewall para identificar bloqueos, permisos y reglas activadas.
4. Confirmar mediante Packet Capture: SYN sin completar, TCP RST, repetición o comportamiento de la aplicación.
5. Si existe evidencia y autorización, aplicar controles de firewall específicos y verificar que no se interrumpe un escáner corporativo legítimo.

100.18. Ejemplo 3: tráfico multicast e ICMPv6

Si el informe contiene direcciones multicast o link-local IPv6, primero identifique si se trata de Neighbor Discovery, Router Solicitation, Router Advertisement u otro protocolo legítimo. El hecho de aparecer como origen, destino o parte de una pareja no es suficiente para determinar si es normal o anómalo.

La comprobación correcta combina interfaces, captura del protocolo adecuado y conocimiento del diseño de la red. Bloquear indiscriminadamente ICMPv6 puede interrumpir el funcionamiento de IPv6, incluida la detección de vecinos y la gestión de MTU.

100.19. Ejemplo 4: una VPN activa sin acceso útil

Prueba escalonada para localizar el fallo

1. Corroborar el estado de la VPN en Status → OpenVPN / IPsec / WireGuard, según la tecnología.
2. Buscar en By IP Pair la relación entre cliente de documentación y servidor remoto de documentación.
3. Revisar en Diagnostics → States los puertos y el retorno de paquetes de esa sesión; no confundir estado con validación de aplicación.
4. Contrastar rutas, selectors o Allowed IPs según el tipo de VPN, además del firewall de ambos extremos.
5. Probar el servicio real; si falla, capturar tráfico en ambos extremos y documentar dónde cesa el intercambio.

100.20. Ejemplo 5: concentración súbita de sesiones en Multi-WAN

Compare States Summary en un momento normal y durante la incidencia; anote qué orígenes y parejas aumentaron. Verifique después en Status → Gateways la pérdida de paquetes, el RTT y la disponibilidad, en Diagnostics → States la interfaz/ruta efectiva, y en pfInfo el consumo global de estados. Si hay cambio de WAN, confirme las traducciones NAT y la persistencia de los estados.

El resumen por IP no muestra la capacidad remanente del enlace ni distingue exactamente ancho de banda de número de conexiones: una sola transferencia puede consumir más caudal que cientos de sesiones ligeras.

100.21. Rendimiento: límites del informe en tablas grandes

Netgate advierte que la elaboración del resumen puede tardar y consumir gran cantidad de memoria, particularmente si PF mantiene una tabla muy extensa o si el appliance tiene recursos ajustados. Con tablas grandes, la página puede fallar por memoria o no terminar de mostrarse; no debe insistirse repetidamente durante una avería con alta carga.

Síntoma	Causa plausible	Respuesta conservadora
Página tarda mucho	Gran número de estados / CPU limitada	Usar States filtrados y pfTop con límites
Fallo de memoria	Procesamiento del informe excesivo	Revisar pfInfo y consumo de memoria; no repetir consultas masivas
Cifras cambian entre cargas	Estados nuevos o caducados	Tomar instantáneas con marcas de tiempo
No aparece IP conocida	No tiene estados en ese instante	Generar tráfico de prueba y consultar States

100.22. Correlación con herramientas complementarias

Herramienta	Responde mejor a...	Relación con States Summary
Diagnostics → States	¿Qué conexión exacta, interfaz, NAT, estado y bytes?	Desciende del agregado al detalle
Diagnostics → pfTop	¿Qué estados concentran bytes o actividad?	Prioriza estados según la vista
Diagnostics → pfInfo	¿Hay saturación o alta tasa de altas de estado?	Aporta visión global de PF
Status → System Logs	¿Qué regla permitió o bloqueó tráfico registrado?	Explica eventos observables
Diagnostics → Packet Capture	¿Qué paquetes atravesaron cada punto?	Confirma intercambio real
Status → Monitoring	¿Cómo evoluciona la tabla de estados?	Añade contexto temporal

100.23. Árbol de decisión para un diagnóstico reproducible

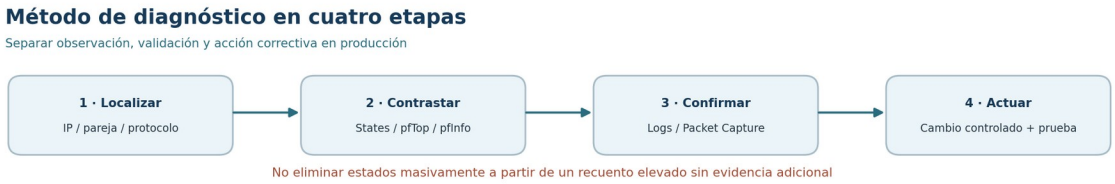


Figura 100.4. Secuencia recomendada: identificar, correlacionar, confirmar y actuar.

Los datos del resumen solo deben conducir a una intervención si se dispone de contexto suficiente. Cuando una regla de bloqueo está correctamente configurada pero existe un estado anterior que sigue permitiendo la conexión, puede requerirse la terminación selectiva del estado en Diagnostics → States. Evitar el Reset States completo salvo que el alcance y las consecuencias se hayan aceptado expresamente.

100.24. Seguridad, privacidad y trazabilidad

Las direcciones, parejas y puertos pueden describir relaciones operativas entre sistemas y constituyen metadatos sensibles de red. Para informes, auditorías o soporte deben sustituirse los IP reales, hostnames y otros identificadores por direcciones de documentación. Los ejemplos de este capítulo usan exclusivamente los rangos 192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24 y 2001:db8::/32.

Al revisar un supuesto escaneo, descartar primero sistemas autorizados de monitorización, inventario, respaldo, supervisión o descubrimiento. Mantener los hallazgos separados de las hipótesis y registrar las pruebas que sustentan cada conclusión.

100.25. Lista de comprobación operativa

Comprobación	Criterio de aceptación
Hora y alcance del informe	Se registra ventana temporal y contexto de carga
Dirección/pareja significativa	Se identifica el servicio esperado sin datos reales en documentación
Protocolo y puertos	Se distingue cardinalidad de puertos frente a conexiones y bytes
Correlación	Se revisan States, pfTop y registro/captura si procede
Impacto de acción	Existe autorización y plan de reversión antes de interrumpir sesiones
Validación final	La aplicación y las rutas operan correctamente tras cualquier cambio

100.26. Glosario operativo

Término	Definición precisa
Estado PF	Registro temporal de un flujo seguido por el firewall.
Cardinalidad de puertos	Número de valores de puerto diferentes observados en el grupo.
Par IP	Relación origen y destino utilizada para agrupar estados.
NAT	Traducción de direcciones o puertos en un trayecto.
IP link-local	Dirección IPv6 limitada al enlace; requiere contexto de interfaz.
Snapshot / instantánea	Vista de la tabla en un momento concreto, no un historial.
Rate / tasa	Eventos por unidad de tiempo; no equivale a número acumulado de estados.

100.27. Referencias técnicas verificables

Referencias R1–R6	Referencias R7–R12
R1 · Netgate — Firewall States Summary	R7 · Netgate — Troubleshooting Firewall Rules
R2 · Netgate — Viewing Firewall States in the GUI	R8 · Netgate — Reset State Table / Source Tracking Table
R3 · Netgate — Diagnostics Menu Guide	R9 · Netgate — Multi-WAN and NAT
R4 · Netgate — Firewall Fundamentals	R10 · Netgate — NAT Port Forwards Troubleshooting
R5 · Netgate — pfTop	R11 · Netgate — Advanced Firewall & NAT
R6 · Netgate — pfInfo	R12 · Netgate — Graph Category List

Los nombres y las opciones de presentación pueden variar según la versión y los paquetes de pfSense Plus. Contrastar los detalles adicionales con la documentación oficial correspondiente.

101 Diagnostics → System Activity

Procesos y subprocesos · CPU · carga · memoria y ZFS ARC · diagnóstico de rendimiento

System Activity muestra una fotografía que se renueva de la actividad interna del firewall. Permite diferenciar falta de CPU, espera por recursos, presión de memoria y comportamiento normal de servicios del sistema, antes de adoptar medidas que podrían interrumpir la red.

ADVERTENCIA Una línea con WCPU alto no significa necesariamente sobrecarga. En particular, los hilos [idle] representan tiempo de CPU libre. Evite terminar procesos, modificar tunables o reiniciar sin pruebas complementarias.

101.1. Finalidad, ruta y alcance

Ruta exacta: Diagnostics → System Activity. Esta página presenta la salida del monitor top del sistema FreeBSD, que Netgate documenta como equivalente a top -aSH en la consola. Se actualiza automáticamente cada pocos segundos. La información es una observación casi en tiempo real: no sustituye a un registro histórico, un perfilador de CPU ni a una prueba de extremo a extremo.

CPU Activity presenta la cabecera de carga, los hilos, el uso de CPU, la memoria, ZFS ARC y los procesos ordenados por actividad. Las operaciones avanzadas descritas en el capítulo se ejecutan desde consola y deben distinguirse de los controles de esta página de consulta.

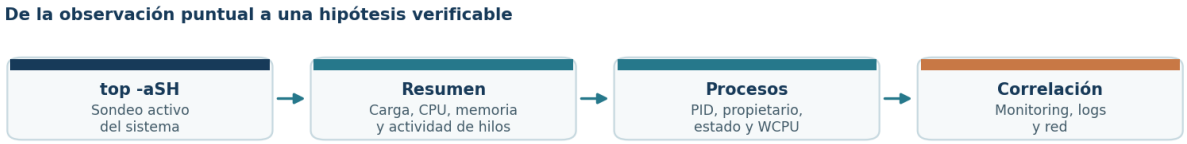


Figura 101.1. Relación entre observación, procesos y correlación diagnóstica.

101.2. Lectura de la cabecera de top

Indicador mostrado	Significado técnico	Interpretación correcta
last pid	Último identificador de proceso asignado	No es un contador de procesos activos ni una medida de carga.
load averages	Promedio de carga de 1, 5 y 15 minutos	No son porcentajes de CPU; compare tendencias y capacidad del equipo.
up y hora	Tiempo desde el último arranque y reloj del sistema	Útil al correlacionar incidencias y eventos de reinicio.
threads	Hilos en ejecución, dormidos o esperando	No confundir hilo con proceso ni muchos hilos con saturación.
CPU	Reparto del tiempo CPU entre categorías	Las categorías suman aproximadamente el 100 % del tiempo muestreado.
Mem / ARC / Swap	Memoria física, caché ZFS y paginación si existe	Las métricas no son partidas independientes que puedan sumarse sin más.

101.3. Load average: carga no es porcentaje

Load average refleja trabajo ejecutable y, según las condiciones del sistema, tareas que contribuyen a la carga. Los tres valores corresponden a ventanas aproximadas de uno, cinco y quince minutos. Un valor de 2 no significa 2 % de CPU: debe analizarse junto con el número de CPU lógicas, porcentaje idle, latencia y tendencia.

La relación con el número de núcleos es orientativa, no un umbral universal: con múltiples núcleos, una carga de varias unidades puede ser normal; un único hilo saturado puede afectar a una VPN aun cuando la carga media global parezca moderada. No interprete un pico aislado como prueba de insuficiencia de hardware.

101.4. Estados de hilos: running, sleeping y waiting

Running identifica hilos ejecutables; sleeping suele indicar tareas detenidas a la espera de un evento o temporizador, algo habitual en servicios de red; waiting recoge esperas según la clasificación del kernel. Un total elevado de hilos durmientes es normal cuando existen muchos demonios y workers. Deben preocupar más las esperas persistentes acompañadas de bloqueo funcional, colas de entrada o problemas de I/O.

101.5. Desglose de CPU: user, nice, system, interrupt e idle

Categoría	Qué representa	Si aumenta de forma mantenida
user	Código en espacio de usuario	Investigar procesos como servicios VPN, PHP u otros demonios.
nice	Ejecución con prioridad nice ajustada	Verificar tareas de fondo y consumo real, no inferir error por sí solo.
system	Trabajo del kernel, red y sistema	Correlacionar con reglas PF, tablas de estados, tráfico y kernel.
interrupt	Procesamiento de interrupciones hardware	Revisar tasas de paquetes, NIC, drivers, offloads y mbufs.
idle	Tiempo sin utilización efectiva de CPU	Un valor alto representa capacidad disponible, no un proceso que «consume» CPU.

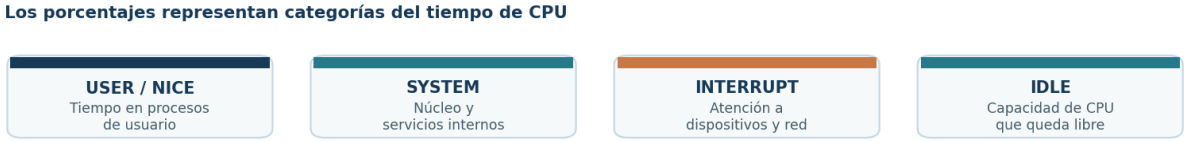


Figura 101.2. Cinco componentes de la medida de CPU y su interpretación.

ACLARACIÓN Dos hilos [idle{idle: cpuN}] con WCPU próximo a 100 % son coherentes con CPU mayormente desocupada. No se suman esos porcentajes para obtener consumo.

101.6. Memoria física: Active, Inact, Wired y Free

Campo	Explicación	Precaución
Active	Páginas utilizadas recientemente	No es la única memoria ocupada.
Inact	Páginas inactivas y susceptibles de reutilización	No implica fuga ni inutilidad.
Wired	Memoria fijada, no paginable, incluidas áreas kernel y ARC en top	Puede incluir ZFS ARC; no sumar ARC otra vez.
Free	RAM inmediatamente libre	Un valor pequeño no es malo sin presión real de memoria.
Swap (si existe)	Espacio para páginas trasladadas a almacenamiento	Distinguir uso ocasional de paginación sostenida o fallos.

FreeBSD busca aprovechar RAM disponible como caché. La evaluación profesional considera fallos de asignación, actividad sostenida de swap, tiempos de respuesta, crecimiento de procesos y comportamiento en el tiempo. La comparación de una única instantánea no permite diagnosticar una fuga de memoria.

101.7. ZFS ARC: desglose, compresión y doble contabilización

Cuando existe un pool ZFS activo, top muestra ARC y sus componentes: Total, MFU (Most Frequently Used), MRU (Most Recently Used), Anon (datos en tránsito), Header y Other. La línea adicional de compresión compara tamaño comprimido y sin comprimir de los datos cacheados; una razón mayor que 1 representa ahorro de espacio de datos almacenados, no memoria libre garantizada.

En System Activity, la caché ARC forma parte de la memoria Wired informada por top. No sume «Wired + ARC Total» como consumo físico. ARC intenta ceder memoria cuando es necesaria, pero bajo cargas

repentinas puede no liberarla con suficiente rapidez; un límite demasiado alto puede empeorar situaciones de escasez.



Figura 101.3. Relación entre memoria Wired y desglose ZFS ARC.

Métrica ARC	Interpretación	Qué comprobar
Total	Tamaño ocupado por la caché ARC	Evolución, memoria libre y procesos demandantes.
MFU / MRU	Bloques frecuentes / recientes	Proporción según patrón de acceso; no son fallos.
Anon / Header / Other	Datos temporales y metadatos de caché	No deben interpretarse como memoria ajena a ARC.
Compressed / Uncompressed	Tamaños de información cacheada	No equivalen al espacio utilizado por el sistema de archivos.
Ratio	Relación de compresión	No mide rendimiento de la VPN ni utilización de CPU.

101.8. Columnas de la tabla de procesos e hilos

Columna	Descripción	Lectura profesional
PID	Identificador de proceso	Cambia al reiniciar el proceso; no es identidad persistente.
USERNAME	Cuenta propietaria	root o usuarios de servicio no implican fallo.
PRI / NICE	Prioridad efectiva / ajuste de prioridad	No modificar sin comprender planificación FreeBSD.
SIZE / RES	Memoria virtual del proceso / memoria residente	SIZE no es RAM usada; sumar RES sobreestima memoria compartida.
STATE	Estado o evento de espera (RUN, CPUx, accept, kqread…)	Una espera en socket no supone un bloqueo patológico.
C	CPU lógica en la que corre el hilo	Es un identificador de procesador, no porcentaje.
TIME	CPU acumulada consumida	No equivale al tiempo transcurrido ni a tasa instantánea.
WCPU	Porcentaje de CPU ponderado	Útil para ordenar actividad; mirar junto a CPU global.
COMMAND	Nombre del proceso o hilo del kernel	Correlacionar con servicio, logs y síntomas.

101.9. Interpretación de procesos frecuentes en pfSense Plus

Proceso o hilo	Función habitual	Cuándo investigar
[idle{idle: cpuN}]	Hilo ocioso de una CPU	No investigar como consumo; refleja disponibilidad.
php-fpm: pool nginx	Ejecución de lógica PHP de GUI y páginas dinámicas	Uso sostenido alto sin usuarios o GUI muy lenta.
nginx: worker process	Servidor HTTP(S) de administración	Errores de GUI, sockets o excesivo tráfico de gestión.

Proceso o hilo	Función habitual	Cuándo investigar
[kernel{…}]	Hilos internos FreeBSD (p. ej. de ZFS)	Espera/I-O sostenidos y síntomas de almacenamiento.
openvpn / strongSwan / wireguard	Procesos o componentes relacionados con VPN	Aumento al cifrar tráfico con bajos caudales.
unbound / kea / ntpd	DNS, DHCP y sincronización NTP	Errores de servicio comprobados con registros y pruebas funcionales.

Algunas etiquetas de STATE, como piperd, accept y kqread, nombran el evento de espera en el kernel y no son códigos de error. Un nombre o hilo puede cambiar entre versiones, arquitecturas, paquetes o modos de ejecución.

101.10. Uso correcto de la página y actualización

Observe al menos varias muestras bajo condiciones comparables. Las salidas de top se actualizan a intervalos cortos y pueden incluir su propia carga y la de la página web que se está visualizando. Si se requiere guardar evidencias, anote fecha, versión, evento de negocio y condiciones de la prueba sin conservar identificadores sensibles innecesarios.

La página es de consulta y no ofrece controles para terminar procesos, modificar prioridades o asignar CPU. La ausencia de un proceso de corta duración no prueba que nunca se ejecutara: una muestra puede no coincidir con su actividad.

101.11. Procedimiento 1 — línea base de CPU y memoria

1. Abrir Diagnostics → System Activity y registrar la hora, carga de 1/5/15 minutos y porcentaje de CPU idle.

2. Anotar número de CPU lógicas y comprobar los procesos activos, sin atribuir saturación a [idle].

3. Repetir la observación durante una operación habitual y comparar con Status → Monitoring para obtener tendencia.

4. Registrar memoria Active, Inact, Wired, Free y, si existe, ARC sin duplicar los totales.

5. Concluir si existe problema real solo al asociar las métricas con un síntoma medible de servicio.

101.12. Procedimiento 2 — localizar CPU elevada sostenida

1. Confirmar la degradación mediante tasa de tráfico, tiempos de respuesta o pérdida de paquetes.

2. Revisar system, user e interrupt y los procesos con WCPU elevado en varias muestras.

3. Si domina interrupt, contrastar interfaces, controlador NIC, errores y contadores mbuf; si domina VPN, revisar el rendimiento cifrado.

4. En consola autorizada, consultar top -aSH y systat -vmstat 1 para ampliar el diagnóstico.

5. Evitar modificar afinidad, prioridades o servicios sin una copia de configuración, ventana y plan de reversión.

101.13. Procedimiento 3 — presión de memoria y ZFS

1. Correlacionar la lentitud con Free, Wired y ARC; observar si la carga coincide con escaneos de archivos o tareas periódicas.

2. Comprobar si existe swap y si hay entradas/salidas sostenidas, no solo algunos MB ocupados.

3. Inspeccionar memoria de los procesos que crecen y consultar registros por fallos de asignación.

4. Revisar guía de ZFS Tuning únicamente si hay pruebas de presión; no establecer vfs.zfs.arc.max por una instantánea aislada.

5. Tras cualquier cambio autorizado, validar latencia, servicios críticos y estabilidad a lo largo de varios ciclos de carga.

101.14. Herramientas complementarias y comandos de consulta

Comando (consola autorizada)	Objetivo	Observación
top -aSH	Visualizar procesos y hilos, incluido CPU de sistema	Equivalente documentado por Netgate para esta pantalla.
systat -vmstat 1	Actividad de CPU, interrupciones y sistema	Adecuado para observar diferencias entre segundos.
netstat -m	Consumo y fallos asociados a mbufs	Útil si hay interrupciones y pérdidas de tráfico.
systat -iostat 1	Actividad de entrada/salida	Ayuda a identificar espera vinculada a disco.
swapinfo -h	Consultar uso de dispositivos swap, si están configurados	Presencia o ausencia depende de la instalación.
sysctl kstat.zfs.misc.arcstats.size	Tamaño de ARC, si existe ZFS	No usar si la variable no está disponible.

PRECAUCIÓN Las herramientas de monitorización repetitiva pueden ejecutarse indefinidamente. Úselas desde consola o SSH autorizados, no como comandos interactivos sin fin desde Diagnostics → Command Prompt.

101.15. Matriz de diagnóstico: síntoma, pista y validación

Síntoma	Lectura orientativa	Comprobación adicional
VPN lenta	openvpn/crypto con WCPU alto, user elevado	Throughput, MTU, cifrado, interfaces y errores.
Pérdida de tráfico bajo carga	interrupt/system alto o mbufs al límite	netstat -m, errores NIC y Packet Capture.
GUI lenta	php-fpm o nginx activo de forma persistente	Logs PHP/web, sesiones, carga y consultas DNS.
RAM libre baja	Wired/ARC elevado sin swap ni fallos	Puede ser normal; observar presión real.
Almacenamiento lento	Hilos ZFS y actividad I/O	SMART, ZFS, errores y registros del sistema.
CPU parece al 100 %	WCPU elevado de [idle]	No es saturación; comprobar CPU idle global.

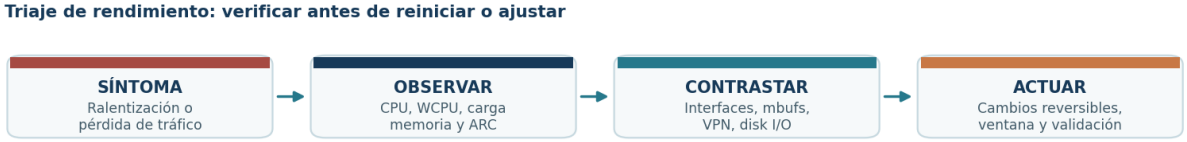


Figura 101.4. Procedimiento de triaje reversible ante problemas de rendimiento.

101.16. Escenarios empresariales prácticos

Sede con enlace limitado y VPN lenta

Durante una copia de datos se aprecia lentitud, pero el monitor muestra capacidad de CPU libre. La hipótesis de CPU insuficiente pierde fuerza; corresponde examinar RTT, pérdida, MTU, shaping y capacidad WAN. Solo si los hilos de cifrado permanecen ocupados y la tasa se estabiliza por debajo de lo esperado se profundiza en CPU y cifrados.

Firewall que deja de resolver DNS después de una intervención

Unbound puede aparecer dormido porque espera consultas. Este estado es normal. Antes de reiniciarlo debe contrastarse la escucha en sockets, una consulta DNS real desde LAN, la ruta de salida y los registros. La actividad de top por sí sola no demuestra disponibilidad del servicio.

Incremento de Wired tras una actualización

Una operación de actualización puede llenar temporalmente la ARC con datos recientes. Si el firewall conserva memoria disponible y los servicios funcionan, la mera subida de Wired no justifica reiniciar. Si se reproduce presión real de memoria, revisar ZFS Tuning y evaluar un ajuste documentado con reversión.

Paquetes perdidos con CPU interrupt alta

Si durante tráfico sostenido crece interrupt y existen errores o descartes de interfaz, el cuello de botella puede estar en controladores, interrupciones o capacidad NIC. Deben recogerse evidencias con contadores de interfaces, netstat -m y una prueba acotada antes de modificar offloads o parámetros hardware.

101.17. Seguridad operativa y cambios de alto riesgo

No se deben finalizar procesos esenciales (pf, DNS, DHCP, GUI o VPN) basándose en su WCPU sin identificar el impacto. Los reinicios borran información volátil útil para diagnosticar y pueden producir cortes en todas las sedes. Modificar tunables de memoria, drivers o planificación sin un plan de vuelta atrás puede agravar la incidencia.

Al compartir capturas de System Activity, anonimice hostnames y cualquier dato que aparezca en argumentos de procesos. Registre versiones, síntomas y métricas agregadas; no copie rutas o comandos que contengan secretos.

101.18. Checklist de validación y escalado

Comprobación	Resultado a registrar
Sistemas críticos	VPN, DNS, DHCP y navegación funcionan desde un cliente de prueba.
CPU / carga	Sin CPU bloqueada sostenidamente; tendencia estable 1/5/15 min.
Memoria	ARC/Wired interpretadas sin doble suma; sin presión ni swap anómalo.
Red	Sin incremento significativo de errores o mbufs fallidos.
Evidencias	Muestras repetidas, periodo, carga de prueba, firmware, acciones.
Reversión	Cambio documentado y condición para volver al estado anterior.

101.19. Glosario técnico

Término	Definición breve
Load average	Promedio de demanda del planificador para 1, 5 y 15 minutos; no % de CPU.
Thread	Unidad de ejecución que puede pertenecer a proceso o kernel.
WCPU	Porcentaje ponderado de tiempo CPU mostrado por top.
Wired	Páginas de RAM fijadas, incluida ARC en top.
ARC	Adaptive Replacement Cache de ZFS.
MFU / MRU	Datos consultados frecuentemente / recientemente.
mbuf	Buffer de memoria del subsistema de red FreeBSD.
I/O	Entrada/salida de dispositivos o almacenamiento.

101.20. Errores frecuentes de interpretación y lectura correcta

Inferencia equivocada	Qué indica realmente	Cómo confirmarlo
«idle al 95 % = CPU saturada»	El hilo idle contabiliza capacidad no utilizada.	Comprobar porcentaje idle global y actividad del proceso real.
«Wired + ARC = RAM total ocupada»	En top, ARC ya se incluye en Wired.	Ver Mem y desglose ARC; no duplicar importes.
«Load 4 = CPU al 4 %»	Load no es porcentaje y depende de capacidad/concurrencia.	Comparar CPU lógica, 1/5/15 minutos y respuesta del servicio.
«SIZE = RAM física del proceso»	SIZE describe espacio virtual del proceso.	Usar RES con cautela por memoria compartida.
«Sleeping implica fallo del daemon»	Lo normal es esperar tráfico o un evento.	Repetir prueba funcional del servicio y revisar logs.
«La primera fila siempre es el problema»	El orden refleja la métrica seleccionada; puede ser idle.	Examinar COMMAND, CPU global y tendencia.
«Free bajo exige reiniciar»	La caché puede ocupar RAM de forma útil.	Investigar swap, fallos de memoria y respuesta real.

101.21. Cómo comparar antes y después de una incidencia

Una observación reproducible debe comenzar con una línea base y continuar durante una prueba delimitada. Emplee el mismo periodo de muestreo, las mismas condiciones de red y la misma operación. En cada punto registre CPU user/system/interrupt/idle, load 1/5/15, ARC, memoria libre, síntoma observado y caudal o latencia. Una mejora de un único contador aislado no demuestra que la incidencia esté resuelta.

Momento de prueba	Datos mínimos	Criterio de validación
Antes	Carga 1/5/15, reparto CPU, procesos, Mem/ARC.	Guardar línea base y síntomas observados.
Durante tráfico controlado	WCPU del servicio, CPU interrupt, mbufs, I/O.	Relacionar consumo con el volumen de trabajo.
Después	Mismos indicadores con idéntico procedimiento.	Exigir mejora funcional, sin errores nuevos.
Día posterior	Monitoring, logs, rendimiento y estabilidad.	Confirmar que no aparece regresión o fuga gradual.

Si existe riesgo de perder acceso de administración, el procedimiento de validación debe efectuarse con acceso fuera de banda disponible y una configuración de respaldo. Priorice el diagnóstico frente al reinicio cuando aún no se haya capturado suficiente evidencia.

101.22. Referencias técnicas oficiales

Netgate — System Activity (Top) — abrir documento oficial

Netgate — Troubleshooting High CPU Load — abrir documento oficial

Netgate — Memory Management — abrir documento oficial

Netgate — ZFS Tuning — abrir documento oficial

Netgate — Troubleshooting Low Interface Throughput — abrir documento oficial

Netgate — Graph Category List — abrir documento oficial

FreeBSD — Handbook: ZFS (ARC) — abrir documento oficial

FreeBSD — top(1) manual — abrir documento oficial

102 Diagnostics → Tables

Tablas activas de PF · aliases · bloqueos dinámicos · verificación y diagnóstico

Las tablas de PF representan conjuntos de direcciones que el motor de filtrado puede consultar para aplicar reglas con eficacia. La vista Diagnostics → Tables permite examinar el contenido efectivo cargado en memoria, comprender los bloqueos dinámicos y detectar discrepancias entre los aliases definidos y las direcciones que realmente utiliza el cortafuegos.

CRITERIO DE SEGURIDAD Una tabla vacía no implica que el cortafuegos esté desprotegido. Eliminar una entrada puede recuperar conectividad, pero también retirar temporalmente un bloqueo necesario. Documentar, autorizar y verificar antes de actuar.

102.1. Objetivo, alcance y ruta exacta

Ruta: Diagnostics → Tables. La pantalla es una consulta del contenido de tablas PF definidas por el sistema o por el administrador. Una tabla puede responder a un alias cargado, una defensa de autenticación, una función VPN, una política NAT o un módulo adicional. No debe confundirse la lista de IP con las reglas que deciden permitir o bloquear tráfico.

En la vista presentada figura la sección «Table to Display», el selector «Table» con «sshguard» seleccionado y el aviso «No entries exist in this table». Es una situación de lista vacía, no una demostración de fallo ni de desactivación de la protección. Otros controles descritos a continuación se documentan oficialmente cuando hay entradas u otras tablas activas.

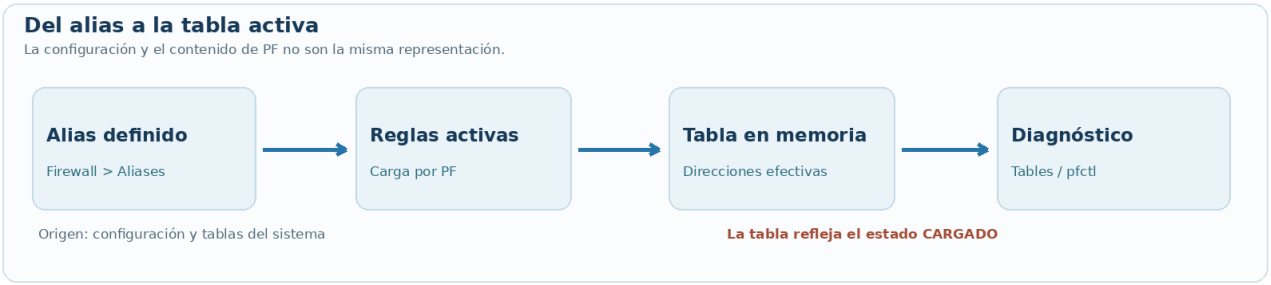


Figura 102.1. Origen de datos y visualización del contenido activo de PF.

102.2. Campos y controles visibles de la pantalla

Elemento	Función visible	Consecuencia o interpretación
Breadcrumb Diagnostics / Tables	Ubica la herramienta bajo Diagnostics.	Permite volver al menú de diagnóstico.
Table to Display	Título del bloque de selección.	No modifica por sí mismo ninguna regla.
Table	Selector desplegable de tabla de sistema o alias.	Al cambiar la selección se carga el contenido correspondiente.
sshguard	Nombre seleccionado en el ejemplo de interfaz.	Tabla de bloqueo de intentos reiterados de acceso a GUI/SSH.
No entries exist in this table	Aviso de ausencia de entradas visibles.	No demuestra que el demonio de protección haya sido detenido.
Iconos superiores	Accesos contextuales del entorno gráfico.	La función exacta depende de la versión y del destino de cada enlace.

CONTROLES CONDICIONALES Cuando una tabla tiene entradas puede ofrecer una papelera por fila. Determinadas tablas bogons incorporan Update. Comprobar la función y el alcance del control antes de eliminar o actualizar entradas.

102.3. Fundamentos de las tablas PF y su relación con los aliases

PF gestiona tablas de direcciones IP y prefijos para realizar búsquedas rápidas. En pfSense, un alias de hosts o redes utilizado por el filtrado puede convertirse en una tabla activa cuando se carga el ruleset. Los

aliases de puertos son otro tipo de agrupación y no deben interpretarse como si el listado de esta página fuera siempre una relación de puertos. El contenido de PF es el que debe comprobarse cuando una regla parece comportarse de forma inesperada.

Concepto	Representa	Dónde se comprueba
Alias configurado	Nombre, miembros declarados, FQDN o fuente URL.	Firewall → Aliases
Tabla PF activa	Direcciones y redes cargadas en el motor de filtrado.	Diagnostics → Tables / pfctl
Regla del firewall	Decisión pass/block y otras condiciones de coincidencia.	Firewall → Rules; System Logs
Estado existente	Conexión previamente admitida con información persistente.	Diagnostics → States / pfTop

Un alias puede parecer correcto en la configuración y, sin embargo, contener direcciones diferentes en la tabla por resolución DNS, actualización de URL, error de carga o dependencia de una función que no esté habilitada. La comprobación debe recorrer los cuatro niveles: origen, tabla, reglas y estados existentes.

102.4. Qué significa que la tabla sshguard esté vacía

sshguard forma parte de los mecanismos de protección ante intentos de autenticación fallidos en la interfaz web y en SSH. Cuando se supera el umbral de protección, la IP de origen puede incorporarse temporalmente a la tabla sshguard y quedar bloqueada por las reglas correspondientes. Si «No entries exist in this table», no se observan direcciones bloqueadas en ese instante por esta tabla; pueden seguir existiendo otras capas de protección, reglas y registros de autenticación.



Figura 102.2. Ciclo de protección y consulta de una tabla dinámica de autenticación.

NO CONFUNDIR Vacío no equivale a «SSH/GUI expuestos», ni a «no hay ataques», ni a «sshguard está desactivado». La interpretación debe corroborarse con System → Advanced → Admin Access y con los registros de autenticación.

102.5. Tablas integradas y tablas de paquetes: inventario funcional

Tabla posible	Finalidad de referencia	Observación
sshguard	Direcciones temporalmente bloqueadas tras intentos de acceso.	Dinámica; caducidad según protección.
bogons / bogonsv6	Bloques no asignados o reservados para filtrado de bogons.	Disponibilidad según opciones de interfaces.
snort2c	Direcciones bloqueadas por paquetes IDS/IPS cuando se utilizan.	Depende de paquetes instalados y activos.
virusprot	Fuentes que han rebasado límites avanzados de reglas.	Puede actualizarse por eventos de conexión.
vpn_networks	Redes remotas asociadas a servicios VPN.	No es un inventario universal de rutas dinámicas.
tonatsubnets	Redes comprendidas en NAT de salida automático/híbrido.	Útil para problemas de NAT inesperado.
negate_networks	Destinos a excluir de determinados encaminamientos por políticas.	Ayuda a diagnosticar policy routing.

Tabla posible	Finalidad de referencia	Observación
cpzoneid*	Tablas internas de zonas Captive Portal.	No editar manualmente sin conocer su ciclo de vida.

La presencia y los nombres concretos varían según la versión de pfSense Plus, la configuración y los paquetes. Algunas tablas pueden no existir hasta activar la función correspondiente. El listado anterior es un catálogo de mecanismos documentados, no una reproducción de las opciones existentes en la captura.

102.6. Contenido dinámico: DNS, aliases de URL y actualizaciones

Los aliases que contienen FQDN se resuelven mediante registros A y AAAA; las direcciones devueltas se introducen en PF y se revisan periódicamente. Netgate documenta por defecto un intervalo de cinco minutos para los nombres de aliases, modificable en System → Advanced → Firewall & NAT. Un alias FQDN no filtra por nombre HTTP ni por certificado TLS: filtra por las direcciones que resultaron de DNS.

Los URL Table aliases se abastecen de listas externas almacenadas en el firewall y se actualizan según su calendario. Si la descarga falla, el fichero está vacío o el origen cambia, la tabla efectiva puede diferir de la configuración esperada. Deben revisarse la fuente, el formato, TLS/certificados si procede, DNS, registros y reglas realmente cargadas.



Figura 102.3. De la resolución o descarga externa al conjunto efectivo de direcciones PF.

102.7. Actualización, borrado de entradas y permanencia

Con entradas visibles, Netgate documenta el icono de papelera para retirar una dirección individual. Esta acción es especialmente útil para desbloquear una IP en una tabla dinámica como sshguard una vez confirmado que corresponde a un usuario legítimo. Sin embargo, una tabla configurada por alias manual o fichero puede repoblarse en la siguiente recarga del filtro, y una tabla alimentada automáticamente puede volver a incluir la misma dirección al repetirse el evento.

Acción	Resultado inmediato esperado	Riesgo y persistencia
Seleccionar otra tabla	Cambia la información presentada.	Consulta; impacto operativo mínimo.
Eliminar fila en tabla dinámica	Retira la dirección concreta del bloqueo actual.	Puede volver a incluirse; evaluar la causa.
Editar alias en Firewall → Aliases	Modifica la configuración declarada.	Requiere aplicar/recargar para surtir efecto.
Actualizar bogons (si aparece)	Solicita una obtención anticipada de listas bogons.	Cambio potencial de cobertura; revisar registros.
Recargar filtro	Regenera reglas y tablas según configuración.	Puede alterar el tratamiento de nuevas conexiones.

PRECAUCIÓN No utilizar procedimientos de vaciado masivo para resolver un caso individual. Vaciar tablas de seguridad puede retirar bloqueos legítimos y abrir temporalmente servicios protegidos.

102.8. Comandos de inspección desde consola (lectura)

La GUI debe ser el punto de entrada habitual. Para una comprobación administrativa avanzada, desde una consola autorizada se pueden consultar tablas mediante PF. Los ejemplos siguientes no modifican entradas; el resultado depende de que la tabla exista y esté cargada en el sistema.

Comando	Objetivo	Advertencia
pfctl -s Tables	Enumerar tablas cargadas en PF.	La salida exacta depende del ruleset.

Comando	Objetivo	Advertencia
pfctl -t sshguard -T show	Consultar direcciones bloqueadas por sshguard.	Solo lectura; requiere acceso administrativo.
pfctl -t EJEMPLO_ACCESO -T show	Examinar un alias de ejemplo cargado como tabla.	Sustituir por el nombre real autorizado.
pfctl -s info	Comprobar información global del filtro PF.	Correlacionar con pfInfo y estados.

El acceso a consola y a Command Prompt puede disponer de privilegios elevados. No copiar la salida sin revisarla: nombres de tablas, direcciones y configuraciones pueden revelar detalles sensibles de la instalación.

102.9. Procedimiento 1 — interpretar una tabla vacía

1. Abrir Diagnostics → Tables y seleccionar la tabla cuya función se está revisando.
2. Identificar si se trata de una tabla dinámica (por ejemplo, sshguard) o de una tabla proveniente de alias/servicio.
3. Para una tabla dinámica vacía, comprobar registros y configuración del servicio sin presuponer una avería.
4. Para un alias configurado que debería tener miembros, revisar Firewall → Aliases, resolución o fuente y reglas que lo utilizan.
5. Corroborar con System Logs, Filter Reload y, si procede, inspección PF de solo lectura.
6. Documentar hora, tabla, síntoma y conclusión, evitando revelar direcciones reales en informes públicos.

102.10. Procedimiento 2 — desbloquear de forma controlada un acceso legítimo

1. Confirmar por un canal alternativo que el origen bloqueado pertenece a una persona autorizada.
2. Revisar el motivo del bloqueo en Authentication/System Logs y corregir contraseña, MFA o causa de los fallos.
3. Acceder desde otra dirección administrativa autorizada o mediante consola, manteniendo una vía de recuperación.
4. En Diagnostics → Tables seleccionar sshguard; si existe la entrada, utilizar la papelera de esa fila únicamente.
5. Repetir un acceso autorizado y verificar que la entrada no reaparece inmediatamente; registrar el incidente.

SEGURIDAD No incluir indiscriminadamente direcciones en listas de excepción de protección de accesos. Es preferible corregir la causa y limitar la exposición de la GUI y SSH.

102.11. Procedimiento 3 — alias FQDN que no coincide con el destino

1. Confirmar el FQDN definido en Firewall → Aliases y la regla que referencia dicho alias.
2. Obtener la resolución DNS desde pfSense con Diagnostics → DNS Lookup y verificar A/AAAA.
3. Consultar el contenido efectivo en Diagnostics → Tables; comparar familia IP y direcciones.
4. Comprobar el registro filterdns y el intervalo de actualización; considerar resultados variables de CDN.
5. Cuando esté autorizado, corregir fuente DNS o diseño del filtrado y aplicar los cambios.
6. Validar una nueva conexión y, si un estado antiguo mantiene el comportamiento anterior, investigar su tabla de estados.

102.12. Procedimiento 4 — verificar NAT y redes VPN

1. Identificar el destino y la función: NAT de salida automático/híbrido, policy routing o red VPN.
2. Consultar tonatsubnets, negate_networks o vpn_networks si la instalación dispone de ellas.
3. Correlacionar el resultado con Firewall → NAT, Firewall → Rules, Gateways y Diagnostics → Routes.

4. Comprobar el estado de la conexión y NAT mediante Diagnostics → States y, si hay dudas, Packet Capture.

5. Evitar editar tablas internas directamente; modificar la función propietaria y aplicar su configuración.

6. Repetir pruebas desde el origen afectado y documentar la ruta de ida y retorno.

102.13. Tablas y estados existentes: consecuencias sobre sesiones

El contenido de una tabla influye en la coincidencia de reglas para el tráfico que pasa por PF. Sin embargo, las conexiones que ya disponen de estado pueden continuar utilizando decisiones anteriores mientras se mantengan sus estados. Por tanto, después de eliminar una entrada de bloqueo o modificar un alias, es necesario comprobar tanto la carga de reglas como la existencia de estados relacionados antes de concluir que el cambio ha surtido efecto sobre sesiones activas.

No se recomienda borrar todos los estados para «forzar» una regla. Si hace falta retirar un estado antiguo, debe estudiarse una eliminación selectiva con Diagnostics → States y una vía de recuperación previamente acordada.

102.14. Errores frecuentes y matriz de diagnóstico

Síntoma	Hipótesis que investigar	Siguiente prueba
sshguard sin entradas	Ausencia de bloqueos temporales; no necesariamente fallo.	Logs de autenticación y protección GUI/SSH.
Alias declarado, tabla vacía	No cargado, lista vacía o resolución fallida.	Alias, DNS, filterdns, Filter Reload.
Acceso bloqueado tras retirar IP	Estado previo, regla distinta o bloqueo aguas arriba.	States, reglas, captura en interfaces.
URL Table desactualizada	Descarga, calendario, TLS o formato erróneo.	Fuente, registros y recarga controlada.
NAT omitido en red concreta	Ausencia de red en tonatsubnets o política manual.	Firewall → NAT y rutas.
Exceso de entradas	Límite de tablas/memoria insuficiente.	System Logs y Maximum Table Entries.

102.15. Seguridad, capacidad y rendimiento de las tablas

Las tablas de gran tamaño consumen memoria y recursos durante su carga. Netgate documenta un límite de Firewall Maximum Table Entries, por defecto 400 000 en las versiones descritas, y la necesidad de margen adicional al regenerar los aliases durante una recarga. El valor adecuado depende de RAM, cardinalidad, frecuencia de actualización y paquetes instalados; aumentarlo sin dimensionar el equipo no es una solución universal.

Desde System → Advanced → Firewall & NAT puede revisarse la capacidad máxima de tablas y la frecuencia de resolución de nombres. Los ajustes se deben justificar con mediciones y registros, considerando el riesgo de no cargar el ruleset, el incremento de consumo y el impacto de recargas en un firewall de producción.

102.16. Escenarios empresariales de uso

Situación	Comprobación decisiva	Recomendación
Administrador bloqueado por fallos de acceso	IP en sshguard y evento correspondiente.	Liberación individual y revisión de causa.
FQDN de proveedor cambia de IP	DNS actual frente a tabla cargada.	Evitar confiar en nombres de CDN muy variables.
Lista externa de bloqueo desactualizada	Origen remoto, logs, periodicidad.	Revisar TLS, disponibilidad y plan de reversión.
Tráfico de sede sale por WAN inesperada	negate_networks, reglas gateway, rutas.	Correlacionar con estados y failover.

Situación	Comprobación decisiva	Recomendación
Bloqueos tras límites de conexión	virusprot u otra tabla dinámica.	Revisar límites por regla antes de retirarlos.



Figura 102.4. Secuencia de investigación antes de cualquier modificación de tablas.

102.17. Lista de verificación previa y posterior a cambios

Antes de intervenir	Al concluir
Identificar función propietaria y alcance de la tabla.	Confirmar tabla y reglas cargadas.
Obtener copia de configuración y registrar evidencia segura.	Validar únicamente los servicios afectados.
Mantener acceso alternativo y ventana autorizada.	Verificar acceso administrativo y conectividad remota.
Definir reversión sin vaciados masivos.	Revisar System Logs y estados pertinentes.
Confirmar fuente DNS/URL y cambios esperados.	Documentar el resultado con datos anonimizados.

102.18. Diagnóstico cruzado: decidir dónde está la anomalía

Cuando una dirección esperada no aparece en una tabla, el problema no se resuelve necesariamente cambiando una regla. La investigación debe separar cuatro niveles: origen de la lista, mecanismo de actualización, carga efectiva en PF y coincidencia de reglas. El análisis de estados completa la validación para las sesiones que ya estaban abiertas.

Etapa	Señal objetiva	Acción proporcionada
Fuente	FQDN no resuelve o URL devuelve lista vacía.	Revisar DNS, HTTPS, disponibilidad y formato.
Actualización	La fuente cambió, pero la tabla sigue igual.	Comprobar filterdns, calendario y registros.
Carga en PF	Alias definido y tabla ausente o sin miembros.	Investigar errores de reglas y recarga controlada.
Decisión de regla	Tabla correcta, tráfico bloqueado o permitido.	Revisar Rule ID, orden y dirección de evaluación.
Sesión existente	La regla cambió, pero la sesión aún continúa.	Inspeccionar States y valorar retirada selectiva.

102.19. Criterios de escalado y trazabilidad de incidencias

Si hay fallo de recarga, pérdida de acceso o una tabla de protección repoblándose de forma continua, conservar evidencias antes de intervenir. Registrar el nombre funcional de la tabla, la hora, el cambio esperado y el resultado observado. En informes externos anonimizar las IP y no adjuntar exportaciones originales sin revisión de confidencialidad.

Escalar a mantenimiento programado cuando sea necesario cambiar límites globales de tablas, fuentes masivas de URL o políticas que afecten a varios servicios. Un ajuste de capacidad solo es justificable si la evidencia confirma consumo de memoria, errores de carga o insuficiencia del límite configurado.

102.20. Glosario técnico

Término	Definición aplicada
PF	Motor de filtrado con estado utilizado por pfSense Plus.
Table	Estructura de PF con direcciones o redes consultadas por el ruleset.
Alias	Nombre declarativo utilizado para agrupar valores en configuración.
filterdns	Servicio que mantiene actualizados nombres de aliases y otras referencias.
sshguard	Mecanismo de protección de intentos de autenticación fallidos.
URL Table	Alias cuya lista procede de una fuente externa periódicamente consultada.
State	Entrada que mantiene el seguimiento de una comunicación admitida.
Bogon	Dirección/prefijo según listas de redes reservadas o no asignadas, dependiente de la lista vigente.

102.21. Referencias oficiales y documentación de contraste

Netgate — Firewall Table Contents

Netgate — Aliases

Netgate — Alias Types

Netgate — Alias Configuration

Netgate — Alias Features and Limitations

Netgate — Firewall Maximum Table Entries

Netgate — Admin Access / Login Protection

Netgate — Recuperación de acceso bloqueado

Netgate — Filter Reload Status

Netgate — Registros de DNS Resolver / filterdns

Netgate — Diagnostics Menu

103 Diagnostics → Test Port

Pruebas de conectividad TCP y diagnóstico de servicios

Test Port permite comprobar si el propio firewall consigue establecer una conexión TCP con un destino y un puerto concretos. Es una herramienta útil para separar problemas de resolución de nombres, rutas, filtrado y servicios en escucha. Su resultado debe interpretarse desde la dirección de origen utilizada y completarse con una prueba de la aplicación cuando corresponda.

Idea principal. Que un puerto acepte una conexión desde pfSense no demuestra que funcione desde un equipo de la LAN, que esté publicado en Internet o que la aplicación responda correctamente. [1]

103.1. Objetivo y alcance

La ruta de acceso es **Diagnostics → Test Port**. Se utiliza para investigar un servicio determinado: por ejemplo, un panel HTTPS, un servidor SSH o una aplicación interna que escucha en TCP. El destino puede indicarse por nombre o dirección IP. La prueba proporciona una observación puntual de esa combinación de origen, destino, familia IP y puerto.

El proceso comienza con la resolución del nombre cuando se utiliza un hostname. Después intenta establecer la sesión TCP. Si se activa Remote text, también espera la información que el servidor envíe espontáneamente. No ejecuta una transacción de negocio ni comprueba credenciales, permisos, certificados o contenido web.

Límite de transporte. Esta página comprueba TCP. No sirve para validar un puerto UDP de la misma forma: abrir una conexión TCP a un número de puerto no comprueba el servicio UDP que utiliza ese mismo número. [1]

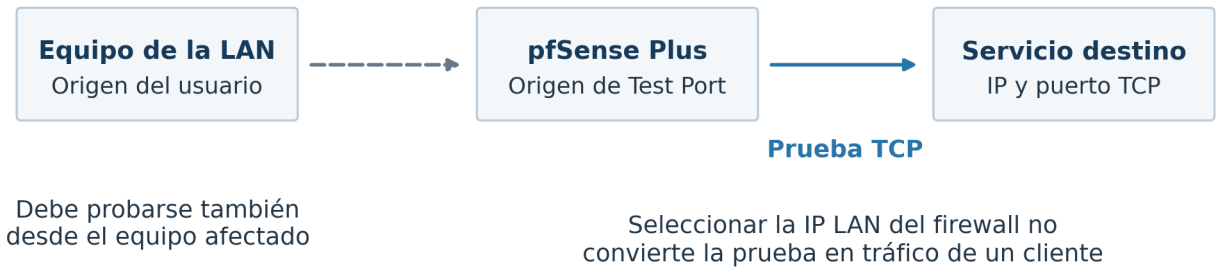


Figura 103.1. Origen de la prueba y diferencia respecto al tráfico de un equipo de la LAN.

103.2. Campos y controles del formulario

El formulario contiene dos datos imprescindibles, Hostname y Port, y varias opciones para concretar la prueba. Los nombres de campo siguientes corresponden a la interfaz en inglés. Las direcciones disponibles en los desplegables dependen de las interfaces y direcciones configuradas en cada firewall.

Campo o control	Qué determina	Uso habitual
Hostname	Nombre DNS o IP del destino.	Nombre completo o dirección sin URL, ruta ni puerto añadido.
Port	Puerto TCP de destino.	Número entero entre 1 y 65535.
Source Port	Puerto TCP local de origen.	Dejar vacío para la selección automática.
Remote text	Lectura del texto enviado por el servidor al conectar.	Activar si interesa observar un saludo o banner.
Source Address	Dirección local del firewall usada como origen.	Any o una IP local apropiada para el trayecto.
IP Protocol	Familia de direcciones de la prueba.	IPv4 o IPv6, de forma coherente con el destino.

Campo o control	Qué determina	Uso habitual
Test	Inicia una prueba con los valores indicados.	Revisar después el resultado y la IP probada.

Lectura del formulario. Los textos orientativos dentro de las cajas no son valores de configuración. El selector Source Address define la IP de origen; la frase de ayuda que menciona un «trace» no convierte esta herramienta en un traceroute.

103.3. Qué significa establecer una conexión TCP

En una conexión TCP normal, el iniciador envía un segmento SYN, el extremo que acepta responde con SYN y ACK, y el iniciador confirma con ACK. Este intercambio prepara la sesión de transporte. El protocolo de aplicación se ejecuta después y puede requerir más mensajes, negociación criptográfica o autenticación. [2]



Figura 103.2. Intercambios TCP simplificados para aceptación, rechazo y ausencia de respuesta.

Un rechazo activo suele observarse como un RST. Puede generarlo el sistema de destino o un dispositivo que rechace la comunicación. La ausencia de respuesta útil puede acabar en tiempo de espera, pero no identifica por sí sola dónde se pierden los paquetes. La figura resume comportamientos; una captura concreta puede incluir retransmisiones, mensajes ICMP u otros eventos.

La conexión aceptada demuestra que un extremo TCP respondió en ese trayecto y momento. Un proxy, un balanceador o un dispositivo intermedio puede ser ese extremo. Para identificar el servicio real se necesita una comprobación adicional mediante el cliente apropiado.

103.4. Hostname y resolución DNS

En Hostname se escribe un nombre como **portal.lab.example** o una dirección como **10.64.10.20**. No se introduce «https://», una ruta web, una cadena de conexión ni «:443» al final. El puerto tiene su propio campo. Si se usa una IP literal, se elimina la resolución del nombre como requisito de esa prueba.

Para separar DNS de conectividad, consultar primero el nombre en **Diagnostics → DNS Lookup**, anotar los registros devueltos y probar después una de esas direcciones con el mismo puerto y familia. DNS Lookup permite comparar respuestas y tiempos de los servidores que incluye en su consulta. Sus resultados deben contrastarse con la dirección que utiliza realmente Test Port. [3]

Si la conexión por IP funciona y por nombre falla, investigar resolución, familia seleccionada o elección de otra dirección. Si ambas funcionan, pero el navegador sigue fallando, comprobar la negociación TLS, el nombre del certificado, el proxy y la respuesta HTTP con herramientas de aplicación.

Varios destinos para un nombre. Un FQDN puede devolver varias IP por balanceo, redundancia o distribución de contenido. Un éxito contra una dirección no valida todas las demás. Anotar la IP efectiva evita comparar pruebas que terminaron en servidores distintos.

103.5. IPv4 e IPv6

El campo IP Protocol fija la familia de direcciones de la prueba. Un registro A contiene una dirección IPv4 y un registro AAAA contiene una dirección IPv6. Si se fuerza una familia para la que el nombre no tiene

resultado, la prueba no dispone de una dirección utilizable de ese tipo; no es evidencia de que el puerto esté filtrado.

Selección	Destino disponible	Interpretación
IPv4	Registro A o IP IPv4 literal.	Comprueba únicamente el trayecto IPv4.
IPv6	Registro AAAA o IP IPv6 literal.	Comprueba únicamente el trayecto IPv6.
IPv4 sin registro A	Solo existe AAAA.	Resolver la incompatibilidad antes de investigar TCP.
IPv6 con dirección válida	Falta ruta o retorno IPv6.	DNS puede funcionar y aun así fallar la conexión.

Para comparar ambas familias, realizar dos pruebas independientes y conservar sus resultados. IPv4 e IPv6 pueden utilizar rutas, reglas y condiciones de acceso diferentes. Que una familia funcione no demuestra la disponibilidad de la otra.

103.6. Port y Source Port

Port es el puerto del servicio remoto. Source Port es el puerto local con el que comienza la conexión. En una comprobación de HTTPS se utiliza 443 en Port; Source Port suele permanecer vacío. No es necesario poner 443 en ambos campos.

Con Source Port vacío, el sistema selecciona un puerto de origen disponible. Fijarlo solo tiene sentido para investigar una condición concreta de filtrado o reproducir un caso conocido. No determina el puerto de destino ni garantiza conservar ese número si una traducción NAT posterior lo modifica.

Parámetro	Valor de ejemplo	Significado
IP de origen	10.64.10.1	Dirección local del firewall en el laboratorio.
Puerto de origen	Selección automática	Extremo local de una nueva conexión.
IP de destino	10.64.10.20	Servidor al que se intenta llegar.
Puerto de destino	443 TCP	Extremo remoto que debe aceptar la sesión.

Conflicto local. El mensaje «nc: bind failed: Address already in use» puede aparecer si se solicita un puerto de origen ocupado en el firewall. Dejar Source Port vacío y consultar **Diagnostics** → **Sockets** si es necesario. Este error local no demuestra que el servicio remoto esté detenido. [1]

103.7. Remote text y los banners de servicio

Al marcar **Show remote text**, la herramienta intenta mostrar el texto que el servidor envía al aceptar la conexión. La ayuda del formulario advierte de una espera de al menos unos diez segundos. Una duración mayor con esta opción no significa necesariamente que haya empeorado la red.

Un saludo puede aportar una pista sobre el protocolo o la aplicación que responde. Su ausencia también puede ser normal: algunos servicios esperan primero un mensaje del cliente, y otros requieren una negociación cifrada antes de intercambiar contenido interpretable.

Servicio TCP	Comportamiento orientativo	Qué falta verificar
SSH	Puede enviar una identificación inicial.	Identidad del servidor y autenticación del cliente.
SMTP o FTP sin TLS implícito	Pueden presentar un saludo de texto.	Comandos, permisos y operación del servicio.
HTTP	Normalmente espera una solicitud del cliente.	Respuesta a una petición HTTP válida.
HTTPS o servicio con TLS implícito	Requiere negociación TLS del cliente.	Certificado, nombre y funcionamiento de la aplicación.

Interpretación. Una conexión TCP aceptada con Remote text vacío no equivale a un fallo del servicio. Tampoco un banner constituye una comprobación de seguridad o una garantía de que la aplicación complete su trabajo.

103.8. Source Address y elección de la ruta

Source Address selecciona una dirección perteneciente al firewall. **Any** permite la selección automática apropiada para la conexión. Cuando se necesita un origen específico, se elige una IP local disponible, incluidas las direcciones virtuales que admita la configuración. No se utiliza este campo para suplantar la IP de un puesto de usuario.

La IP elegida puede afectar a una lista de acceso remota, a la selección de tráfico de una VPN o a la ruta de retorno. Si se usa un origen que el destino no sabe alcanzar, la conexión puede fallar aunque exista un camino de ida válido.

Seleccionar una dirección WAN no garantiza elegir esa WAN como salida. El origen y el encaminamiento son decisiones relacionadas, pero distintas. En tráfico generado por el firewall intervienen las rutas específicas y, cuando no existe otra ruta aplicable, la puerta de enlace predeterminada de la familia correspondiente. Verificarlo en **Diagnostics → Routes** y **System → Routing → Gateways**. [4]

En una instalación con varias WAN, las reglas con gateway aplicadas al tráfico entrante de LAN no se reproducen automáticamente en una prueba originada por pfSense. Para saber por dónde sale de verdad, observar la captura en la interfaz pertinente. No cambiar rutas globales solo para obtener un resultado favorable en una prueba aislada.

103.9. Procedimiento básico de comprobación

1. Definir el servicio que se quiere comprobar y confirmar su puerto TCP real.
2. Abrir Diagnostics → Test Port y escribir el hostname o la IP de destino.
3. Introducir el puerto del servicio en Port y dejar Source Port vacío.
4. Mantener Remote text desmarcado en la primera comprobación, salvo que se necesite un saludo.
5. Elegir Any o una dirección local justificada por el escenario y seleccionar IPv4 o IPv6.
6. Pulsar Test y leer el resultado completo, incluida la dirección efectiva si se muestra.
7. Si hay un fallo con nombre, comparar con la IP literal y revisar DNS.
8. Si TCP funciona, probar el servicio con su cliente. Si el problema afecta a un equipo, repetir desde ese equipo.

Registrar cada prueba antes de modificar el siguiente parámetro. Cambiar a la vez nombre, IP de origen, familia y puerto impide saber cuál de esas diferencias explica el nuevo resultado.

103.10. Interpretación de resultados y errores

Los textos concretos pueden variar según versión, idioma y herramienta subyacente. La tabla agrupa significados habituales y propone una comprobación siguiente; no atribuye una causa definitiva a un único mensaje.

Resultado o señal	Qué permite concluir	Siguiente comprobación
Conexión aceptada	Un extremo aceptó TCP desde este origen.	Cliente de aplicación y prueba desde el equipo afectado.
Connection refused	Hubo un rechazo activo.	Servicio en escucha, IP correcta y posible regla reject.
Timeout o tiempo de espera	No se completó la conexión en el plazo disponible.	Captura de ida y retorno, rutas y filtrado.
Error de resolución	No se obtuvo una dirección adecuada para el nombre.	DNS, escritura del nombre y familia seleccionada.
No route to host o Network is unreachable	Se informó una condición de alcance de red.	Tabla de rutas, gateway y posible mensaje ICMP recibido.
Address already in use	No pudo reservarse el extremo local solicitado.	Dejar Source Port vacío y revisar Sockets.
TCP aceptado sin texto remoto	El puerto respondió, sin banner visible.	Determinar si el protocolo espera hablar primero con el cliente.

Un rechazo no identifica automáticamente al dispositivo que lo genera. Un tiempo de espera tampoco equivale a «pfSense bloquea». Para localizar el punto de fallo se necesita observar el intercambio y relacionarlo con las reglas y los registros.

103.11. Caso práctico de acceso HTTPS

Un panel de laboratorio se ofrece como **portal.lab.example** en **10.64.10.20**, puerto **443 TCP**. El nombre solo funcionará si existe en el DNS del laboratorio. Estas direcciones y nombres son ejemplos didácticos; deben sustituirse por los del entorno de prueba autorizado.

1. Comprobar el registro A con DNS Lookup y anotar la dirección devuelta.
2. En Test Port, usar Hostname 10.64.10.20, Port 443, Source Port vacío, Remote text desmarcado, Source Address Any e IPv4.
3. Repetir con portal.lab.example manteniendo los demás parámetros.
4. Si ambas conexiones se aceptan, abrir el nombre con un navegador o cliente HTTPS desde el equipo que presenta el problema.

Si el panel falla solo al usar el nombre en el navegador, investigar DNS del cliente, certificado, SNI o configuración del servidor web. Test Port no envía una petición HTTPS ni selecciona un sitio virtual mediante SNI. Tampoco valida la confianza del certificado. Si el cliente utiliza HTTP/3 sobre QUIC, este ensayo de TCP 443 no prueba ese trayecto UDP.

103.12. Caso práctico de SSH y lectura de un banner

Un servidor de administración del laboratorio escucha en **10.64.10.30**, puerto **22 TCP**. La primera prueba se realiza sin Remote text; una segunda, con la casilla activada, permite observar si aparece una identificación inicial.

Configuración: Hostname 10.64.10.30, Port 22, Source Port vacío, Source Address Any e IPv4. Un texto ilustrativo como «SSH-2.0-servidor-lab» aporta una pista del servicio alcanzado. La cadena no sustituye la validación de la clave del servidor por el cliente SSH.

Si aparece rechazo, confirmar que el servicio escucha en la interfaz correcta y en ese puerto. Si solo se acepta desde determinados orígenes, comparar la IP de origen usada por Test Port con la permitida en el servidor. Un cambio de Source Address puede revelar una restricción por origen sin demostrar por sí mismo cómo se comportará un puesto de usuario.

La comprobación funcional posterior consiste en una conexión SSH autorizada, validando identidad y autenticación. No es necesario abrir el servicio a otros segmentos ni publicarlo en Internet para completar el diagnóstico.

103.13. Caso práctico de un servicio a través de VPN

En el laboratorio, la red local es **10.64.10.0/24** y la remota **10.64.20.0/24**. El firewall dispone de **10.64.10.1** y el servicio remoto se encuentra en **10.64.20.40**, puerto **8443 TCP**. Se supone que la VPN y las políticas del laboratorio deben comunicar esas redes.

1. Comprobar que el túnel está establecido y que la ruta o política de la VPN incluye el destino.
2. Probar 10.64.20.40 en Port 8443, IPv4 y Source Port vacío.
3. Si el diseño requiere un origen de la red local protegida, seleccionar 10.64.10.1 en Source Address.
4. Verificar que el extremo remoto permite ese origen y que sabe devolverle tráfico.
5. Repetir desde un cliente autorizado de 10.64.10.0/24 para validar el uso real.

En IPsec basado en políticas, el origen debe encajar en los selectores aplicables. En túneles basados en rutas también importan las rutas y políticas de ambas partes. La elección de una IP local coherente puede ser necesaria para probar desde el firewall, pero no sustituye la revisión del túnel. [5]

Si Any falla y el origen local protegido funciona, se ha encontrado una diferencia de contexto que debe contrastarse con los selectores, la ruta y el retorno. Evitar la conclusión general de que «la VPN funciona para toda la red» a partir de ese único resultado.

103.14. Caso práctico de una publicación mediante NAT

Se desea publicar un servidor HTTPS del laboratorio. La dirección externa documental es **203.0.113.25** y el servidor interno es **10.64.10.20**. Una prueba de Test Port al servidor interno en 443 comprueba su accesibilidad desde pfSense; la publicación externa requiere un ensayo desde una red independiente.

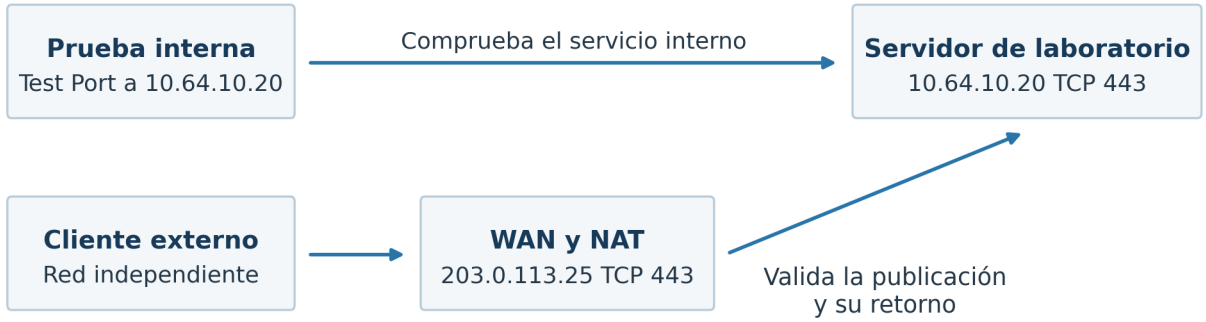


Figura 103.3. La conectividad interna del servidor y la publicación externa son comprobaciones diferentes.

1. Comprobar primero el servicio interno con Test Port a 10.64.10.20 y puerto 443.
2. Desde un cliente externo autorizado, intentar llegar a la dirección y puerto publicados.
3. Observar si el intento entra por WAN y si sale hacia el servidor con el destino traducido.
4. Revisar la respuesta del servidor y su ruta de retorno, junto con la regla asociada y los estados.

Si el tráfico no llega a WAN, investigar el destino utilizado, el equipo situado aguas arriba, doble NAT, CGNAT o filtrado del operador según el caso. Una prueba desde dentro a la IP pública puede depender de reflexión NAT o DNS dividido y no reproduce necesariamente el acceso desde Internet. [6]

Probar una dirección propia del firewall puede alcanzar un servicio local en lugar del servidor publicado. Identificar siempre qué extremo respondió antes de dar la publicación por validada.

103.15. Caso práctico de una aplicación interna

Una aplicación utiliza un servicio configurado en **10.64.20.50**, puerto **15433 TCP**. El número es un puerto fijo elegido para este ejemplo; debe comprobarse el puerto real en la configuración del servidor. No se deduce el puerto únicamente a partir del nombre comercial de la aplicación.

Si Test Port acepta la conexión, el siguiente paso consiste en utilizar el cliente de la aplicación con el mismo destino. Un fallo posterior puede estar en autenticación, permisos, cifrado, nombre lógico de la instancia o dependencias adicionales. Para investigar un servicio de base de datos, un éxito TCP no equivale a ejecutar una consulta correctamente.

Si el sistema utiliza descubrimiento por UDP, puertos dinámicos o conexiones auxiliares, una única prueba TCP no cubre esas funciones. Identificar cada dependencia y su transporte antes de diseñar la batería de comprobaciones. Comparar también el nombre e IP que resuelve el equipo afectado con los usados por el firewall.

103.16. Correlación con captura y otras herramientas

Cuando el mensaje no permite localizar la causa, utilizar **Diagnostics → Packet Capture** con un filtro limitado al host, protocolo y puerto que se investigan. Iniciar la captura, ejecutar una única prueba identificable y detenerla. En una entrada de interfaz, una captura puede mostrar paquetes antes del filtrado; observar un paquete entrante no demuestra que haya sido permitido. [7]

Evidencia observada	Hipótesis que investigar	Comprobación adicional
No se observa el SYN esperado	Error anterior al envío, interfaz observada incorrecta o destino distinto.	Resultado DNS, IP efectiva, ruta y parámetros.
Sale SYN y no vuelve respuesta	Filtrado, servidor inaccesible, pérdida o retorno incorrecto.	Captura remota y ruta de vuelta.

Evidencia observada	Hipótesis que investigar	Comprobación adicional
Vuelve RST	Rechazo activo por algún extremo del trayecto.	Origen del paquete, servicio y políticas reject.
Llega SYN al servidor, sin respuesta	Escucha, filtrado local o problema del servidor.	Sockets y registros del sistema remoto.
Vuelve SYN y ACK, sin completarse la sesión	Pérdida, asimetría o tratamiento del retorno.	Capturas correlacionadas y estados.
Handshake completo y falla la aplicación	La capa TCP se establece; falta validar capas superiores.	Cliente de aplicación, TLS y logs del servicio.

Herramientas relacionadas. DNS Lookup ayuda a investigar nombres; Routes y Gateways, el camino de salida; Sockets, los servicios locales; States, el seguimiento de conexiones; System Logs, los eventos registrados. La ausencia de un evento en el log no demuestra ausencia de tráfico: el registro de la regla o del servicio puede no estar habilitado.

Una captura debe interpretarse en su interfaz y dirección. Si hay NAT, las direcciones y puertos pueden diferir entre WAN y la interfaz interna. En VPN cifrada, observar el tráfico exterior del túnel no siempre permite leer el intercambio TCP interior.

103.17. Comprobaciones desde consola y desde el cliente

La consola permite reproducir una prueba TCP concreta con **nc**. Estos comandos generan conexiones de diagnóstico; no cambian reglas ni rutas. Los ejemplos se aplican al laboratorio descrito. [8]

```
nc -4 -vz -w 5 10.64.10.20 443
nc -4 -s 10.64.10.1 -vz -w 5 10.64.20.40 8443
```

Las opciones -4 y -6 seleccionan familia; -z comprueba la conexión sin intercambio de datos de aplicación; -v solicita información; -w establece un tiempo de espera, y -s fija una IP de origen local. El plazo de cinco segundos corresponde a estos comandos y puede diferir del utilizado por la página web.

Desde un equipo Windows, una prueba equivalente del puerto TCP puede realizarse con PowerShell. El comando se ejecuta en el equipo afectado para conservar su contexto de red. [9]

```
Test-NetConnection -ComputerName 10.64.10.20 -Port 443
```

Revisar **TcpTestSucceeded** y la dirección remota utilizada. La respuesta ICMP de PingSucceeded es una comprobación distinta. Un host puede aceptar TCP aunque no responda a ping. Del mismo modo, responder a ping no demuestra que el puerto de la aplicación esté disponible.

103.18. Errores frecuentes y límites del diagnóstico

Error de interpretación	Corrección práctica
El puerto responde desde pfSense y por tanto desde la LAN.	Repetir desde el equipo afectado con su DNS y recorrido.
TCP 443 funciona y por tanto la web está bien.	Comprobar TLS, nombre del certificado y petición HTTPS.
TCP 53 responde y por tanto DNS UDP funciona.	Utilizar una consulta DNS y verificar su transporte.
No hay banner y por tanto el servicio está parado.	Determinar si el servidor espera primero datos del cliente.
Seleccionar WAN2 como origen obliga a salir por WAN2.	Comprobar rutas y capturar la salida efectiva.
Timeout significa que una regla local bloquea.	Localizar el fallo con evidencia de ida y retorno.
Probar la IP pública desde dentro valida la publicación.	Comprobar desde una red externa independiente.
Un ensayo correcto cubre todas las IP de un nombre.	Registrar y, si procede, comprobar cada dirección necesaria.

Test Port es una comprobación puntual de conexión. No mide por sí sola capacidad de transferencia, pérdida bajo carga, disponibilidad continua, vulnerabilidades o comportamiento de todas las funciones del servicio. Su utilidad aumenta cuando cada resultado responde a una pregunta concreta.

103.19. Registro de la incidencia y verificación final

Conservar la hora con zona horaria, el origen utilizado, el nombre consultado, la IP efectiva, la familia, el puerto de destino, el uso o no de Remote text y el resultado. Separar lo observado de la hipótesis. «TCP aceptado desde el firewall» es una evidencia; «todos los usuarios tienen acceso» requiere otras pruebas.

Dato de la prueba	Ejemplo de registro
Destino y familia	portal.lab.example / 10.64.10.20 / IPv4
Origen	IP local 10.64.10.1; puerto de origen automático.
Puerto y lectura	443 TCP; Remote text desmarcado.
Observación	Conexión aceptada desde pfSense.
Validación posterior	Comprobar HTTPS desde el cliente afectado.

Antes de cerrar el caso, confirmar que se probó el puerto real, que la resolución corresponde al destino esperado y que el trayecto de retorno es coherente. Validar la aplicación desde su origen de uso. Si hubo cambios, documentarlos y retirar únicamente los ajustes temporales introducidos para el diagnóstico.

En informes compartidos, anonimizar direcciones, nombres y banners. Los ejemplos utilizan redes privadas ficticias, el bloque documental 203.0.113.0/24 y nombres bajo .example.

103.20. Glosario técnico

Término	Definición aplicada
TCP	Transporte orientado a conexión utilizado por esta prueba.
Puerto de destino	Número del servicio remoto que se intenta alcanzar.
Puerto de origen	Número que identifica el extremo local de la conexión.
Handshake	Intercambio que establece una sesión TCP.
SYN y ACK	Indicadores TCP de sincronización y confirmación.
RST	Indicador TCP de reinicio o rechazo de una conexión.
Banner	Identificación o saludo que un servicio envía al conectar.
FQDN	Nombre DNS completo utilizado para identificar un destino.
A y AAAA	Registros DNS de direcciones IPv4 e IPv6, respectivamente.
SNI	Nombre de servidor indicado por un cliente durante la negociación TLS.
NAT	Traducción de direcciones y, según el caso, puertos.

103.21. Referencias oficiales

Referencias para ampliar los conceptos y contrastar el comportamiento de la herramienta. La documentación de pfSense puede cambiar con la versión; los campos y opciones concretos deben verificarse en la instalación administrada.

[1] Netgate Testing a TCP Port
https://docs.netgate.com/pfsense/en/latest/diagnostics/test-port.html

[2] IETF RFC 9293 Transmission Control Protocol
https://www.rfc-editor.org/rfc/rfc9293.html

[3] Netgate DNS Lookup
https://docs.netgate.com/pfsense/en/latest/diagnostics/dns.html

[4] Netgate Gateways
https://docs.netgate.com/pfsense/en/latest/routing/gateways.html

[5] Netgate Testing IPsec Connectivity
https://docs.netgate.com/pfsense/en/latest/vpn/ipsec/test-connectivity.html

[6] Netgate Troubleshooting NAT Port Forwards
https://docs.netgate.com/pfsense/en/latest/troubleshooting/nat-port-forwards.html

[7] Netgate Packet Capturing
https://docs.netgate.com/pfsense/en/latest/diagnostics/packetcapture/index.html

[8] FreeBSD Manual de nc
https://man.freebsd.org/cgi/man.cgi?query=nc&sektion=1

[9] Microsoft Test NetConnection
https://learn.microsoft.com/en-us/powershell/module/nettcpip/test-netconnection?view=windowsserver2025-ps

104 Diagnostics → Traceroute

Análisis de rutas y diagnóstico de saltos de red

Traceroute permite observar las respuestas de los equipos de capa IP que aparecen en el trayecto desde el firewall hasta un destino. Ayuda a investigar rutas inesperadas, diferencias entre conexiones y puntos a partir de los cuales dejan de recibirse respuestas. Sus resultados deben leerse junto con las rutas, las políticas de filtrado y el funcionamiento del servicio afectado.

Idea principal. Una fila de asteriscos indica que no se recibió la respuesta esperada dentro del plazo de las sondas. Por sí sola no demuestra que ese equipo esté bloqueando el tráfico de los usuarios ni que el destino sea inaccesible.

104.1. Objetivo y alcance

La ruta de acceso es **Diagnostics → Traceroute**. La herramienta genera sondas desde el propio pfSense y utiliza las respuestas de la red para construir una relación de saltos. La lista muestra lo que ha sido posible observar para esa dirección de destino, familia IP, origen y tipo de sonda. [1]

La traza explora respuestas de la red. Para comprobar un puerto TCP, utilizar Test Port; para validar una web o una aplicación, su cliente correspondiente. Un servicio puede funcionar aunque la traza no se complete.

Los ejemplos utilizan redes privadas ficticias, direcciones reservadas para documentación y nombres bajo .example. Las trazas y los tiempos son ilustrativos.

104.2. Campos y controles de la pantalla

La pantalla inicial contiene el destino, la familia IP, la dirección de origen, el máximo de saltos y las opciones Reverse Address Lookup y Use ICMP. Revisar sus valores efectivos antes de ejecutar la prueba: el número de saltos y el protocolo condicionan la interpretación.

Campo o control	Función	Criterio de uso
Hostname	Nombre o IP que se quiere investigar.	Escribir únicamente el destino, sin URL, ruta ni puerto.
IP Protocol	Selecciona IPv4 o IPv6.	Mantener la misma familia al comparar pruebas.
Source Address	Dirección local del firewall que origina las sondas.	Any o una IP local adecuada para la ruta o VPN.
Maximum number of hops	Límite de saltos que se explorarán.	18 es el valor seleccionado en el ejemplo de interfaz.
Reverse Address Lookup	Consulta PTR para mostrar nombres de las IP de los saltos.	Dejar desmarcado al comenzar para evitar esperas DNS.
Use ICMP	Sustituye las sondas UDP por sondas ICMP de eco.	Comparar ambos métodos cuando la traza no sea concluyente.
Traceroute	Inicia la exploración con los parámetros elegidos.	Esperar el resultado y conservar la configuración de la prueba.

El formulario no contiene un selector de puerto TCP de aplicación ni un control de timeout por sonda. No se deben atribuir a esta página opciones que pertenecen a otros programas de trazado o a la consola.

104.3. Cómo se descubren los saltos

En IPv4, el campo **TTL** limita el recorrido de un paquete. Cuando un router lo reenvía, reduce ese valor; si el límite se agota durante el reenvío, descarta el paquete y puede devolver un mensaje ICMP Time Exceeded al origen. Traceroute aprovecha este comportamiento aumentando el límite de las sondas. [2]

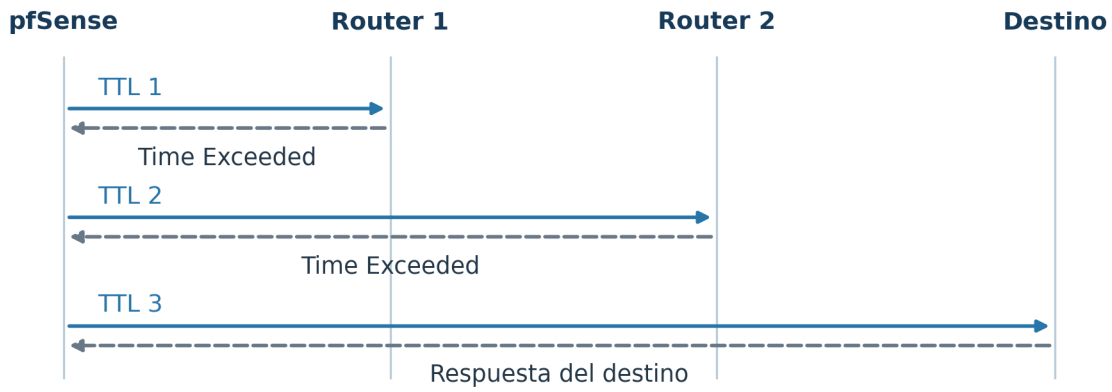


Figura 104.1. Descubrimiento de dos routers y un destino mediante sondas con límites crecientes.

Una sonda con TTL 1 permite obtener la respuesta del primer router; otra con TTL 2 puede alcanzar el segundo. El proceso continúa con paquetes nuevos hasta reconocer el destino, agotar el límite o terminar la ejecución. Normalmente se envían varias sondas para cada valor, de ahí que una fila pueda contener varios tiempos.

En IPv6, el campo equivalente se denomina **Hop Limit** y las respuestas utilizan ICMPv6. Su reducción durante el reenvío cumple la misma función práctica de limitar los saltos. [3] El límite no representa la distancia geográfica ni los milisegundos de espera.

104.4. Hostname y familia IP

Hostname admite un nombre como **portal.lab.example** o una dirección como **203.0.113.80**. No se introduce «https://», una carpeta web ni «:443». La traza trabaja con una dirección IP; no solicita un documento web ni comprueba que el servidor escuche en un puerto concreto.

Si se usa un nombre, el sistema necesita resolverlo antes de explorar el trayecto. Un registro A proporciona una dirección IPv4 y un registro AAAA una dirección IPv6. Seleccionar una familia que no tiene respuesta utilizable puede impedir el inicio de la prueba, sin que haya llegado a investigarse el encaminamiento.

Ante una duda de DNS, consultar **Diagnostics → DNS Lookup**, anotar los resultados y repetir la traza hacia la dirección literal. Si el nombre devuelve varias IP, comprobar cuál se está utilizando. Un cambio de dirección por balanceo o distribución de contenido puede explicar diferencias entre trazas. [4]

Comparación correcta. Mantener la IP efectiva, la familia y el origen al comparar dos ejecuciones. Una traza IPv4 y otra IPv6 pueden recorrer redes distintas, aunque se haya escrito el mismo hostname en ambas.

104.5. Source Address y alcance de la prueba

Source Address determina la IP local con la que pfSense genera las sondas. **Any** permite la selección automática del sistema. Un origen concreto puede ser necesario para que una VPN o una lista de acceso remota reconozca la prueba, y debe disponer de un retorno válido.

Elegir la dirección LAN del firewall no convierte la prueba en una traza de un equipo de esa LAN. Tampoco seleccionar una dirección WAN garantiza por sí solo utilizar esa WAN como salida. El encaminamiento debe comprobarse con las rutas aplicables y la puerta de enlace de la familia IP. [5]

Las reglas con gateway aplicadas a conexiones que entran desde clientes pueden producir un recorrido diferente del utilizado por el tráfico generado por el propio firewall. Si el síntoma lo presenta un puesto de trabajo, la investigación debe incluir una traza desde ese puesto.

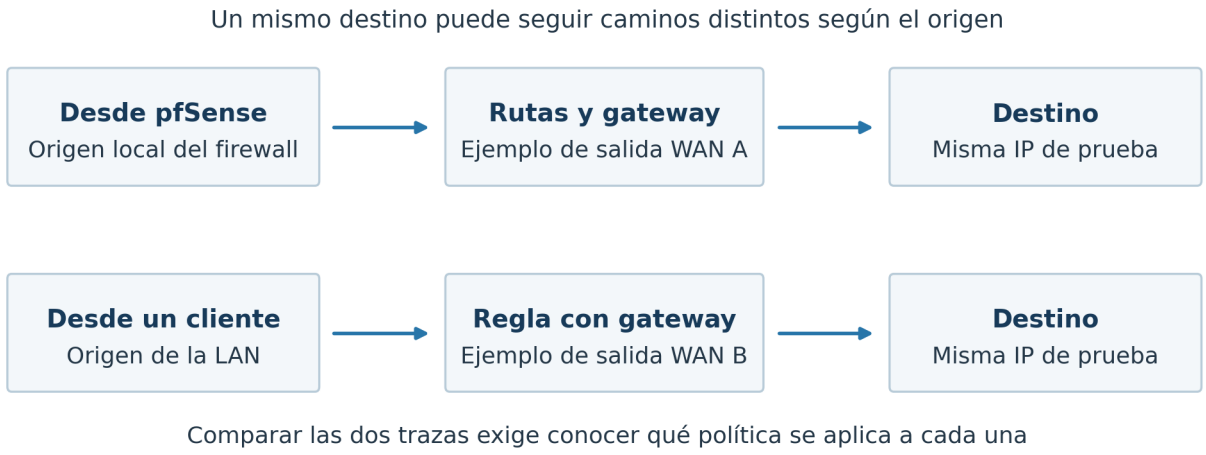


Figura 104.2. Ejemplo de rutas diferentes para tráfico originado por el firewall y por un cliente.

104.6. Límite de saltos y finalización

Maximum number of hops fija hasta dónde se continúa aumentando el límite de las sondas. El valor **18** del formulario limita la exploración de esa ejecución. No representa dieciocho segundos, dieciocho paquetes ni una afirmación de que el destino esté exactamente a dieciocho routers.

Si se alcanza el límite sin reconocer el destino, solo se sabe que la exploración no lo identificó dentro de ese alcance. Puede existir un camino más largo, un destino silencioso, filtrado de respuestas o un problema real de conectividad. Aumentar el límite puede ayudar en el primer caso, pero no resuelve los demás.

Una traza con muchas sondas sin respuesta puede tardar por las esperas acumuladas. Netgate documenta que el resultado se presenta al finalizar y que el control **Stop**, durante una ejecución que lo ofrezca, permite detenerla y consultar lo obtenido. Una salida interrumpida debe conservarse como parcial. [1]

104.7. Reverse Address Lookup y consultas PTR

Reverse Address Lookup intenta traducir las IP de los saltos a nombres mediante consultas DNS inversas de tipo PTR. Esta opción es independiente de la resolución inicial del destino: desmarcarla no evita resolver el hostname escrito en el primer campo.

Para una primera comprobación suele ser preferible trabajar con direcciones numéricas. Al activar las consultas inversas puede aumentar el tiempo total de ejecución por las esperas a DNS. La opción añade etiquetas a la salida; no cambia por sí misma el camino que deben seguir las sondas.

Un nombre que parece indicar una ciudad, un operador o una función es una pista, no una localización física verificada. Un PTR ausente no implica que el router haya fallado. En un informe conviene conservar la IP y utilizar el nombre como información complementaria, evitando deducir propietarios o ubicaciones solo por su texto.

104.8. Diferencias entre UDP e ICMP

Con Use ICMP desmarcado, el formulario utiliza sondas **UDP**. Al marcarlo, emplea solicitudes de eco **ICMP** o su equivalente ICMPv6. Ambos métodos necesitan recibir las respuestas correspondientes; un filtro puede permitir uno y limitar el otro.

Método	Respuesta de un salto intermedio	Reconocimiento habitual del destino
UDP	ICMP o ICMPv6 de tiempo excedido al agotarse el límite.	Mensaje de puerto inalcanzable si no hay una aplicación escuchando en el puerto de la sonda.
ICMP de eco	ICMP o ICMPv6 de tiempo excedido al agotarse el límite.	Respuesta de eco del propio destino.

El traceroute UDP clásico utiliza puertos de destino altos; FreeBSD documenta una base de 33434 para su comando. Esto no constituye una prueba de DNS, HTTPS ni del servicio de usuario. Un mensaje de puerto inalcanzable del destino puede ser precisamente la señal esperada para terminar la traza. [6]

ICMP no tiene puertos TCP o UDP. Cambiar el método puede modificar qué filtros y políticas se aplican y qué caminos se observan. Una traza ICMP más completa no demuestra que el tráfico UDP de una aplicación esté permitido ni que ambos métodos reproduzcan su recorrido.

104.9. Procedimiento básico de trazado

1. Definir el destino y el síntoma que se investiga; anotar la hora y la zona horaria.
2. Abrir Diagnostics → Traceroute y escribir un hostname o una dirección IP.
3. Seleccionar IPv4 o IPv6 y mantener Source Address en Any, salvo que se necesite una IP local concreta.
4. Usar un límite de saltos adecuado; 18 permite reproducir la selección del formulario de referencia.
5. Mantener Reverse Address Lookup desmarcado en la primera ejecución.
6. Iniciar con Use ICMP desmarcado, pulsar Traceroute y conservar la salida.
7. Si el resultado es incompleto, repetir marcando Use ICMP y dejando iguales los demás parámetros.
8. Comparar el trayecto observado y verificar por separado el servicio desde el origen afectado.

Cambiar un parámetro cada vez permite atribuir las diferencias a una condición concreta. Si se cambia simultáneamente de nombre, IP, familia y origen, las dos salidas dejan de representar una comparación controlada.

104.10. Cómo leer una salida

La siguiente traza es un ejemplo numérico simplificado. El destino documental se reconoce en la cuarta fila, aunque la tercera no haya contestado:

```
traceroute to portal.lab.example (203.0.113.80), 18 hops max
 1  192.0.2.1       1.2 ms   1.1 ms   1.3 ms
 2  198.51.100.9    4.8 ms   4.7 ms   4.9 ms
 3  * * *
 4  203.0.113.80   12.2 ms  12.5 ms  12.4 ms
```

Elemento	Lectura correcta
Número de fila	Valor del límite que se está explorando, asociado al orden de salto observado.
IP o nombre	Dirección desde la que se recibió una respuesta identificada para esa sonda.
Varios tiempos	Medidas independientes para varias sondas enviadas con ese límite.
ms	Milisegundos de ida y vuelta desde el origen hasta quien responde.
Asterisco	La sonda no recibió una respuesta utilizable dentro de su plazo.
Destino al final	Se reconoció una respuesta terminal para el método empleado.

Las filas no son las etapas sucesivas de un único paquete que va siendo observado en cada router. Son resultados de sondas distintas. La dirección que responde también puede ser una dirección elegida por el equipo para generar ICMP, y no un inventario completo de todas sus interfaces.

104.11. Asteriscos y trazas incompletas

Si aparecen asteriscos y después responden saltos posteriores, algunas sondas sí han alcanzado puntos más alejados. La ausencia de respuesta intermedia no equivale a un corte absoluto del camino. Puede deberse a filtrado del diagnóstico, límites de generación de ICMP o pérdida de la respuesta de retorno.

Si los asteriscos continúan hasta el límite y no se reconoce el destino, la salida es insuficiente para distinguir entre un destino silencioso y una interrupción del tráfico. El último router que respondió delimita una observación; no identifica automáticamente al responsable de la incidencia.

El destino puede aceptar HTTPS y, al mismo tiempo, no responder al método de trazado utilizado. La comprobación adecuada consiste en contrastar UDP e ICMP, probar el servicio real y, cuando haga falta, capturar tráfico. Una sola traza tampoco proporciona un porcentaje fiable de pérdida de datos de usuario.

104.12. Interpretación de los tiempos de respuesta

Cada tiempo es un **RTT**, es decir, una medida de ida y vuelta desde el origen. Incluye el trayecto de ida, el tiempo necesario para producir la respuesta y el retorno. Restar el tiempo de una fila al de la anterior no proporciona una medida fiable de la latencia del enlace entre ambos routers.

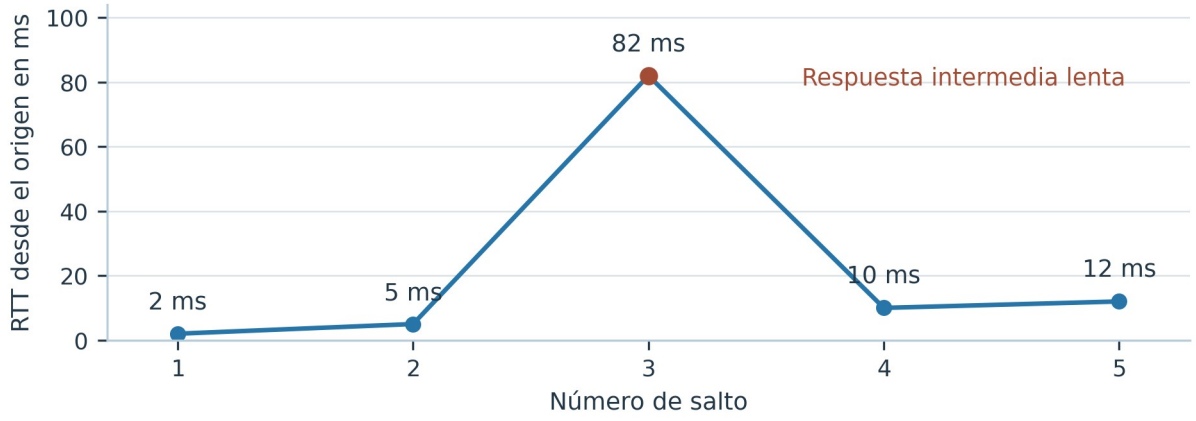


Figura 104.3. Valores didácticos de RTT con una respuesta lenta intermedia y tiempos menores hacia el destino.

En la figura, la sonda del salto 3 devuelve 82 ms y la del destino 12 ms. El dato intermedio no demuestra por sí solo que el router retrase todo el tráfico en 82 ms. Los equipos pueden atender las respuestas de diagnóstico con una prioridad distinta del reenvío de paquetes. [7]

Si el aumento se repite y persiste hasta el destino, existe una señal que merece investigación. Aun así, el problema puede estar en la ida, en el retorno o en la respuesta de los equipos. Comparar varias ejecuciones y el comportamiento de la aplicación permite valorar su relevancia; no existe un umbral universal de milisegundos que identifique una avería.

104.13. Balanceo y límites de la topología observada

Varias IP en una misma posición de salto pueden aparecer cuando sondas distintas atraviesan caminos diferentes. El balanceo por flujo o por paquete y los cambios de encaminamiento pueden producir una salida que mezcla respuestas de más de un recorrido. No implica necesariamente un bucle. [8]

Una secuencia repetida de direcciones y la imposibilidad de alcanzar el destino puede sugerir un bucle, pero la hipótesis debe contrastarse con rutas y capturas. Tampoco debe dibujarse cada par de filas consecutivas como un enlace físico demostrado: las sondas no tienen por qué haber seguido un camino idéntico.

Traceroute no presenta un mapa completo del retorno. Además, los switches de capa 2 no aparecen como saltos IP y los túneles pueden ocultar parte del recorrido subyacente. Según la encapsulación y el tratamiento del límite de saltos, la distancia observada puede diferir de la infraestructura física real.

104.14. Caso práctico de una traza UDP incompleta

Se investiga el destino documental **203.0.113.80**. La traza UDP muestra respuestas iniciales y después asteriscos hasta el límite seleccionado. Antes de cambiar reglas, se conserva la IP efectiva y se repite únicamente con Use ICMP activado.

1. Anotar origen, destino, familia y límite de la ejecución UDP.
2. Repetir con ICMP manteniendo esos datos.
3. Si ICMP alcanza el destino, registrar que ese método obtiene una respuesta terminal.
4. Comprobar el puerto real con Test Port y después el servicio con su cliente.
5. Si la incidencia persiste, revisar filtrado y capturas para el tráfico de la aplicación.

Un resultado posible es que ICMP complete el recorrido y HTTPS funcione, mientras UDP siga sin mostrar el destino. La conclusión es que los métodos tienen distinta visibilidad en ese contexto. No se justifica abrir un rango de puertos en producción únicamente para que la salida del diagnóstico tenga todas sus filas completas.

104.15. Caso práctico de una ruta a través de VPN

El laboratorio utiliza la red local **10.64.10.0/24** y la remota **10.64.20.0/24**. El firewall dispone de **10.64.10.1** y el equipo investigado es **10.64.20.40**. Si la política de la VPN cubre ambas redes, ese origen local puede ser el adecuado para una prueba generada por el firewall.

1. Revisar el estado del túnel y las rutas o selectores que deben incluir el destino.

2. Trazar hacia 10.64.20.40 y utilizar 10.64.10.1 como origen cuando lo requiera el diseño.

3. Verificar que el extremo remoto permite las sondas y puede devolver las respuestas.

4. Comparar con una prueba desde un cliente de la red local.

5. Probar el puerto y la aplicación remotos antes de dar por resuelto el caso.

Los selectores de IPsec basado en políticas y las rutas de una VPN basada en interfaces requieren comprobaciones diferentes. El tráfico iniciado por el firewall puede necesitar un origen protegido coherente. [9] Los saltos internos de un túnel no tienen por qué mostrar todos los routers de Internet que transportan sus paquetes cifrados.

104.16. Caso práctico con varias WAN

Un cliente del laboratorio utiliza una regla con gateway hacia WAN B, mientras el tráfico generado por pfSense sigue una ruta predeterminada por WAN A. Ambas trazas pueden ser correctas y mostrar primeros saltos diferentes. Ese resultado no demuestra que el balanceo esté averiado.

Para investigar, mantener el mismo destino y familia, consultar la política que se aplica al cliente y comprobar la ruta de salida del firewall. Una captura puede confirmar por qué interfaz se envían las sondas. Comparar también el método: UDP e ICMP pueden coincidir con reglas distintas.

Netgate señala una particularidad del encaminamiento por políticas: PF puede reenviar sin reducir el TTL en ese caso y pfSense puede no aparecer como salto intermedio en la traza del cliente. [1] La ausencia de su dirección en la lista no demuestra que el tráfico haya evitado el firewall.

Cuando una incidencia coincide con conmutación de WAN, registrar la hora de la traza y el estado de los gateways. La salida que se obtuvo antes del cambio no representa necesariamente el trayecto activo después de la conmutación.

104.17. Mensajes especiales y errores de ejecución

Además de asteriscos, pueden aparecer errores locales o anotaciones asociadas a mensajes de la red. La forma exacta varía con la implementación y la familia IP. Los símbolos de la tabla corresponden a convenciones documentadas para traceroute de FreeBSD; no se atribuyen todos a cada salida de la interfaz. [6]

Señal	Significado orientativo	Comprobación siguiente
Error al resolver el nombre	No hay una dirección utilizable para esa consulta.	DNS, escritura del destino y familia IP.
Network is unreachable	El sistema informa de falta de alcance de red.	Ruta y gateway de la familia seleccionada.
!H	Mensaje de host inalcanzable.	Equipo que lo genera y alcance del destino.
!N	Mensaje de red inalcanzable.	Ruta hacia la red y estado del siguiente salto.
!X	Comunicación prohibida administrativamente.	Identificar la política y el dispositivo que informa.
!F con un valor de MTU	Necesidad de fragmentación en el contexto indicado.	MTU y captura; no sustituye una prueba específica.
Límite alcanzado sin destino	La exploración termina sin reconocer el destino.	Distinguir alcance insuficiente, silencio y conectividad.

Un mensaje explícito de prohibición aporta una evidencia distinta del silencio. En ambos casos conviene conservar la IP de quien responde y el contexto de la prueba, evitando atribuir el evento al último router visible sin más datos.

104.18. Comprobaciones desde consola y desde Windows

En una consola de FreeBSD pueden fijarse de forma explícita parámetros equivalentes para investigar el mismo destino. Los valores siguientes son ejemplos y no describen necesariamente los parámetros internos que utiliza la interfaz web. [6]

```
traceroute -n -m 18 203.0.113.80
traceroute -n -I -m 18 203.0.113.80
traceroute -n -s 10.64.10.1 -m 18 10.64.20.40
```

La opción -n evita las consultas inversas, -m fija el límite, -I utiliza eco ICMP y -s selecciona una dirección de origen local. Para IPv6 se utiliza traceroute6 con las opciones que admita la versión instalada. [10]

```
traceroute6 -n -m 18 2001:db8:64:20::40
```

Desde Windows, tracert emplea solicitudes de eco. El comando siguiente conserva un límite de 18 saltos y evita la resolución inversa. Debe ejecutarse desde el equipo afectado si se quiere estudiar su contexto de red. [11]

```
tracert /d /4 /h 18 203.0.113.80
```

La salida de Windows sitúa las columnas en otro orden y puede utilizar otros plazos de espera. Comparar la IP efectiva, el método y el origen antes de interpretar las diferencias como un cambio de ruta.

104.19. Captura y método de diagnóstico conjunto

La captura permite comprobar si salen las sondas y si regresan respuestas de la red. En **Diagnostics → Packet Capture**, elegir la interfaz pertinente y limitar la captura al período de una prueba identificable. El tráfico observado debe interpretarse teniendo en cuenta su dirección y las traducciones NAT. [12]

Filtro suficiente. Al buscar mensajes Time Exceeded de routers intermedios, un filtro limitado exclusivamente a la IP del destino puede excluir respuestas relevantes: sus cabeceras IP exteriores contienen la dirección del router y la del origen. Hay que contemplar ICMP o ICMPv6 además de las sondas que se envían.

Pregunta	Evidencia útil
¿Qué IP se está investigando?	Resolución del nombre y dirección efectiva de la salida.
¿Por dónde se envía?	Rutas, gateway y captura de la interfaz de salida.
¿Responden los saltos?	Mensajes ICMP o ICMPv6 y su correspondencia con las sondas.
¿Se reconoce el destino?	Respuesta terminal compatible con el método utilizado.
¿Funciona el servicio?	Test Port para TCP y cliente de la aplicación.
¿Afecta a los usuarios?	Pruebas desde los equipos que presentan el síntoma.

Para escalar una incidencia, conservar hora y zona horaria, origen local, IP de destino, familia, método, límite y salida completa o parcial. Registrar observaciones concretas, como «sin respuesta terminal por UDP; servicio TCP accesible», y separar las hipótesis que todavía necesitan comprobación. Anonimizar direcciones, nombres y detalles de rutas antes de compartirlos.

104.20. Glosario técnico

Término	Definición aplicada
Salto u hop	Posición IP explorada con un valor de límite de la sonda.
TTL	Campo IPv4 utilizado para limitar el recorrido del paquete.
Hop Limit	Campo IPv6 que limita el número de reenvíos.
Sonda	Paquete de diagnóstico enviado para obtener una respuesta.
Time Exceeded	Mensaje de control que puede informar de un límite agotado.
RTT	Tiempo medido de ida y vuelta entre el origen y quien responde.
PTR	Registro DNS utilizado para la resolución inversa de una IP.
UDP	Transporte utilizado por las sondas del método inicial del formulario.

Término	Definición aplicada
ICMP e ICMPv6	Protocolos de control que transportan ecos y mensajes de error.
Ruta asimétrica	Situación en la que el retorno sigue un camino distinto de la ida.
Encaminamiento por políticas	Selección de camino condicionada por reglas, además del destino.

104.21. Referencias oficiales y técnicas

Las opciones concretas deben contrastarse con la versión instalada. Las referencias de FreeBSD describen sus comandos; las de Netgate explican su integración y el comportamiento de pfSense.

[1] Netgate Traceroute
https://docs.netgate.com/pfsense/en/latest/diagnostics/traceroute.html

[2] IETF RFC 1812 Requirements for IP Version 4 Routers
https://www.rfc-editor.org/rfc/rfc1812.html

[3] IETF RFC 8200 IPv6 Specification
https://www.rfc-editor.org/rfc/rfc8200.html

[4] Netgate DNS Lookup
https://docs.netgate.com/pfsense/en/latest/diagnostics/dns.html

[5] Netgate Gateways
https://docs.netgate.com/pfsense/en/latest/routing/gateways.html

[6] FreeBSD Manual de traceroute
https://man.freebsd.org/cgi/man.cgi?query=traceroute&sektion=8

[7] Netskope Traceroute Analysis
https://docs.netskope.com/en/traceroute-analysis

[8] ThousandEyes Traceroute and MTR Limitations
https://www.thousandeyes.com/blog/caveats-of-popular-network-tools-traceroute

[9] Netgate Testing IPsec Connectivity
https://docs.netgate.com/pfsense/en/latest/vpn/ipsec/test-connectivity.html

[10] FreeBSD Manual de traceroute6
https://man.freebsd.org/cgi/man.cgi?query=traceroute6&sektion=8

[11] Microsoft tracert
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/tracert

[12] Netgate Packet Capturing
https://docs.netgate.com/pfsense/en/latest/diagnostics/packetcapture/index.html

Parte VIII Help

105 Help

Ayuda contextual documentación y canales de soporte

El menú Help reúne accesos para comprender la interfaz, consultar referencias técnicas, investigar problemas conocidos y solicitar ayuda. Utilizar el recurso adecuado permite distinguir una duda de configuración, una incidencia operativa y un posible defecto del software. La documentación explica el funcionamiento; el diagnóstico y el soporte ayudan a aplicar ese conocimiento a un caso concreto.

Criterio de uso. Comenzar por la ayuda del tema que se está revisando y comprobar su correspondencia con la versión instalada. Si existe una incidencia, describir lo observado y conservar las pruebas antes de atribuirla a un error de pfSense.

105.1. Función del menú Help

Help se encuentra en la navegación superior de la interfaz web. Sus opciones abren recursos de ayuda y servicios relacionados; el menú no constituye una página de configuración del firewall. Consultar una referencia no sustituye la revisión de los valores aplicados en la instalación.

La ayuda contextual se relaciona con la página desde la que se abre. El resto de accesos permite ampliar la búsqueda hacia documentación general, conocimientos del sistema base, comunidad, seguimiento de incidencias y asistencia profesional. Netgate reúne estas vías en su orientación sobre cómo encontrar información y obtener ayuda. [1]

105.2. Opciones del desplegable

El desplegable Help contiene siete entradas. La tabla conserva sus nombres en inglés y resume la función de cada una:

Entrada	Recurso principal	Cuándo utilizarla
About this Page	Ayuda relacionada con la página actual.	Comprender un campo o una función que se está consultando.
Bug Database	Registro y seguimiento de incidencias del proyecto.	Buscar defectos conocidos y revisar su estado.
Documentation	Documentación oficial de pfSense.	Consultar configuración, conceptos y diagnóstico.
FreeBSD Handbook	Manual del sistema operativo FreeBSD.	Ampliar conocimientos del sistema base.
Paid Support	Información y acceso a soporte profesional de Netgate.	Solicitar asistencia conforme a la cobertura disponible.
pfSense Book	Acceso de referencia al libro o documentación de pfSense.	Estudiar un tema con una estructura más amplia.
User Forum	Foro de la comunidad de Netgate.	Plantear dudas y contrastar un diagnóstico con otros usuarios.

Los destinos de estos accesos pueden utilizar redirecciones administradas por Netgate. Su dirección final o presentación puede evolucionar sin que cambie el nombre del menú. El recurso About this Page, además, depende del contexto de la página. [2]

105.3. About this Page y ayuda contextual

About this Page es el primer recurso cuando la duda afecta a la pantalla abierta. Por ejemplo, desde Diagnostics → Traceroute permite buscar la explicación relacionada con ese diagnóstico, en lugar de comenzar por el índice completo de documentación. En muchas páginas también existe un icono de ayuda con una función equivalente. [1]

1. Situarse en la página sobre la que se necesita información.
2. Abrir Help → About this Page o el icono de ayuda disponible.

3. Leer la descripción de la función y localizar el campo o apartado que plantea la duda.

4. Contrastar la explicación con la edición y versión instaladas antes de realizar cambios.

El enlace no es la pantalla de identificación del producto ni un inventario del equipo. Su objetivo es proporcionar ayuda sobre la función actual. Si el destino resulta demasiado general, utilizar los títulos y términos de la página para continuar la búsqueda en Documentation.

105.4. Documentation y consulta de referencias

Documentation conduce a la referencia oficial de pfSense. Su contenido abarca instalación, interfaces, filtrado, NAT, rutas, VPN, servicios, monitorización, diagnóstico y recuperación, entre otros temas. Conviene combinar el índice por materias con la búsqueda de una función o un mensaje concreto. [3]

Una consulta eficaz incluye el nombre del componente y el síntoma. «OpenVPN no conecta» es una búsqueda amplia; «OpenVPN error de resolución del servidor» ayuda a centrar el análisis. Los nombres exactos de los campos en inglés también facilitan encontrar el apartado correspondiente.

Antes de aplicar un procedimiento, revisar los requisitos, la versión a la que se refiere y sus efectos. La documentación puede tratar pfSense Plus y pfSense CE, además de distintas versiones de paquetes. Un texto técnicamente correcto para otra combinación no garantiza el mismo resultado en el sistema administrado.

105.5. pfSense Book y lectura por temas

pfSense Book mantiene un acceso identificado como libro de referencia. Es útil cuando se necesita estudiar un tema con continuidad: primero los conceptos, después el diseño y finalmente las opciones de configuración. La documentación oficial contiene precisamente ese recorrido entre fundamentos y administración. [3]

No debe deducirse del nombre que el enlace descargue siempre un PDF, abra una edición estática o conduzca a un contenido independiente de Documentation. El destino depende de la redirección vigente. Si ambos accesos terminan en una misma base documental, utilizar su índice y comprobar la versión del contenido consultado.

Para preparar una implantación de VLAN, por ejemplo, conviene estudiar la relación entre interfaces, etiquetado, direccionamiento y reglas, además de leer los campos de una pantalla. Esta lectura por temas ayuda a comprender las dependencias que una ayuda contextual breve no desarrolla por completo.

105.6. FreeBSD Handbook y el sistema base

FreeBSD Handbook abre el manual de FreeBSD, sistema sobre el que se construye pfSense. Aporta contexto sobre procesos, permisos, almacenamiento, redes, interfaces, herramientas de consola y otros conceptos de administración. Es una referencia del sistema operativo, con un alcance diferente al de la interfaz de pfSense. [4]

Resulta útil para comprender qué representa un proceso, cómo interpretar una herramienta del sistema o qué significa un concepto de red. Sin embargo, un procedimiento genérico de FreeBSD no se convierte automáticamente en un procedimiento de mantenimiento de pfSense.

Aplicación práctica. Las actualizaciones, los paquetes y la configuración deben seguir las vías documentadas para pfSense. Netgate advierte de incompatibilidades y problemas de soporte al incorporar software o repositorios externos. No trasladar instrucciones generales de instalación o actualización del sistema base sin comprobar su compatibilidad. [5]

105.7. Bug Database y seguimiento de errores

Bug Database da acceso al seguimiento de incidencias del proyecto, basado en Redmine. Permite buscar si un comportamiento ya se ha comunicado, identificar el componente y consultar el análisis o la corrección asociados. El sitio distingue proyectos relacionados con el sistema base, pfSense Plus, paquetes y documentación. [6]

Antes de concluir que una entrada coincide con el caso investigado, comparar el síntoma, los pasos que lo provocan y el entorno afectado. Dos problemas con el mismo mensaje pueden tener causas diferentes. El estado de una incidencia tampoco demuestra que su solución esté instalada en el firewall que se administra.

Redmine no es el canal para preguntar cómo configurar una función o para iniciar un diagnóstico abierto. La guía de Netgate orienta esas consultas hacia el foro y reserva los informes para defectos concretos que puedan reproducirse. Antes de remitir uno, leer sus requisitos completos. [7]

105.8. User Forum y consultas a la comunidad

User Forum abre el foro de Netgate, que contiene categorías sobre pfSense, paquetes, hardware y otros productos. Es adecuado para dudas de uso, contraste de configuraciones y análisis compartido de un problema. La categoría debe corresponder al componente investigado. [8]

Una consulta útil indica qué se pretende conseguir, qué ocurre realmente y qué pruebas se han realizado. Es preferible un título como «El firewall resuelve un nombre y los clientes no» a un título genérico como «DNS no funciona». La descripción debe permitir distinguir el origen de la prueba y su resultado.

Las respuestas reflejan su contexto y fecha. Una experiencia publicada por otro usuario necesita contrastarse con la documentación y la versión actual del entorno antes de aplicar comandos o modificar reglas. El foro no equivale a un compromiso contractual de atención ni garantiza un plazo de respuesta.

105.9. Paid Support y asistencia profesional

Paid Support conduce a la oferta de asistencia profesional de Netgate y a sus canales de acceso. El centro de asistencia técnica se identifica como **TAC**. La cobertura, los canales disponibles y los objetivos de respuesta dependen de la suscripción o contrato aplicable. [9]

En una incidencia con impacto operativo, revisar la cobertura del equipo y utilizar el canal previsto. No es necesario esperar a que un hilo público obtenga respuestas antes de solicitar la asistencia que ya esté contratada. Consultar el recurso tampoco implica que todas las instalaciones dispongan del mismo nivel de servicio.

La validación puede requerir identificar la instalación mediante el Netgate Device ID y comprobar la elegibilidad de la versión. Este identificador debe proporcionarse por el canal privado correspondiente. Las condiciones concretas se consultan en la oferta y documentación vigentes; no deben darse por supuestas a partir del texto Paid Support. [10]

Un objetivo de respuesta inicial indica cuándo se espera comenzar la atención según las condiciones del servicio. No constituye una promesa de que cualquier incidente quedará resuelto en ese mismo plazo.

105.10. Elegir el recurso adecuado

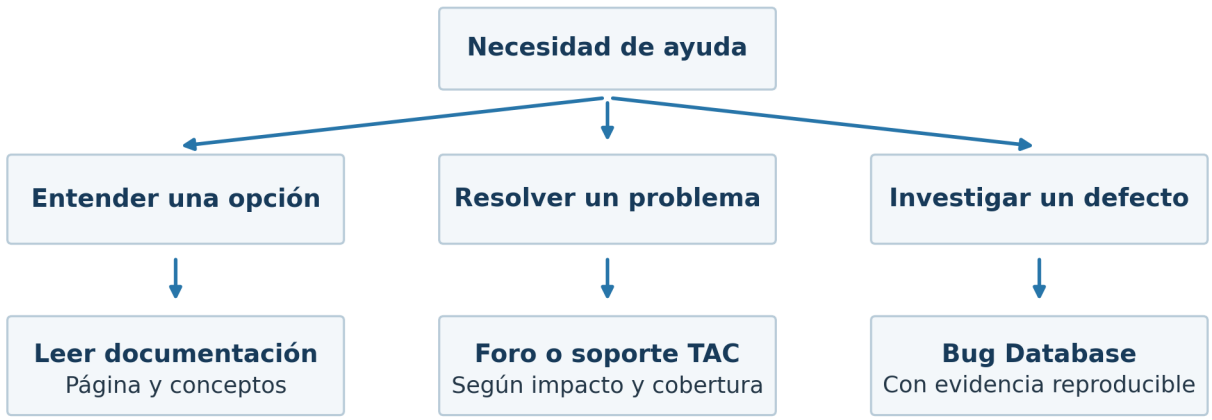


Figura 105.1. Selección del canal según se necesite comprender una función, resolver una incidencia o investigar un defecto.

Situación	Primer recurso útil	Paso posterior
No se entiende un campo de la GUI.	About this Page.	Documentation para ampliar el contexto.
Se quiere diseñar una función completa.	Documentation o pfSense Book.	Relacionar requisitos, configuración y validación.

Situación	Primer recurso útil	Paso posterior
Se necesita comprender el sistema operativo.	FreeBSD Handbook.	Verificar su aplicación específica a pfSense.
Hay una duda de configuración sin causa clara.	Documentación y User Forum.	Aportar pruebas concretas y un esquema mínimo.
Se sospecha un defecto ya conocido.	Bug Database.	Comparar versiones y requisitos del caso.
Hay una interrupción con soporte disponible.	Paid Support y canal TAC contratado.	Comunicar impacto y evidencias por vía privada.

Una incidencia puede recorrer varios de estos recursos. Por ejemplo, una consulta al foro puede ayudar a aislar un defecto reproducible, mientras que un caso TAC puede necesitar consultar una incidencia ya existente. El canal se elige por la necesidad y el impacto, no por el orden del desplegable.

105.11. Preparar una consulta técnica

La información debe permitir reconstruir el problema sin obligar a adivinar la topología ni el objetivo. Presentar primero el síntoma y después el contexto necesario. Las hipótesis deben distinguirse de los resultados observados.

Información	Qué conviene describir
Producto y versión	Edición instalada y versión exacta; paquete y versión si interviene uno.
Entorno	Equipo físico o virtual y componentes pertinentes para el problema.
Objetivo	Comunicación o función que debería realizarse.
Síntoma	Qué falla, desde cuándo y con qué frecuencia.
Alcance	Usuarios o servicios afectados e impacto operativo.
Pruebas	Origen, destino lógico, método, hora con zona horaria y resultado.
Cambios recientes	Actualización o cambio relevante y su relación temporal con el síntoma.
Evidencia	Extractos de registros y esquema mínimo revisados antes de compartirlos.

Evitar conclusiones como «el firewall bloquea todo» si únicamente se ha observado que una aplicación no conecta. Una descripción más útil sería «el puerto TCP responde desde pfSense, pero la misma prueba falla desde el cliente». Esa diferencia orienta la investigación hacia el contexto del cliente y su recorrido.

105.12. Evidencias y confidencialidad

Una captura, un registro, un archivo de configuración o una captura de paquetes puede contener información que no es necesaria para resolver la consulta. Antes de compartirla, revisar direcciones, nombres de equipos, dominios, usuarios, identificadores, rutas, detalles de VPN y cualquier credencial o clave.

Para consultas públicas, utilizar un esquema reducido y datos ficticios coherentes. Mantener los mismos nombres sustitutivos en todas las evidencias permite seguir el problema sin revelar la instalación. Ocultar únicamente una contraseña no anonimiza el conjunto de un diagnóstico.

Un canal privado de soporte tampoco elimina la necesidad de seleccionar la información. Entregar lo solicitado y pertinente para el caso, utilizando el mecanismo indicado por el servicio. Conservar la evidencia original de forma interna para poder correlacionarla con los datos revisados que se comparten.

Posibles vulnerabilidades. Si se sospecha un problema de seguridad del producto, seguir las instrucciones de Security Information de Netgate para comunicarlo al equipo de seguridad. El aviso técnico tiene un canal específico; los detalles sensibles no deben comenzar como una publicación pública de diagnóstico. [11]

105.13. Dos ejemplos de uso del menú

Duda sobre una traza con asteriscos

Un administrador observa asteriscos en Traceroute, aunque una aplicación sigue funcionando. El primer paso es About this Page para comprender el significado de las sondas y sus respuestas. Documentation permite ampliar las diferencias entre métodos y los límites de interpretación.

Si todavía necesita ayuda, puede plantear en User Forum una consulta con el origen de la prueba, la familia IP, el método, el límite de saltos y una salida anonimizada. El objetivo es aclarar el comportamiento; la presencia de asteriscos no basta para abrir un informe de defecto.

Comportamiento repetible en una función

Una opción de la interfaz produce siempre un resultado distinto del documentado. Se comprueba primero la versión y se reduce el caso a las condiciones necesarias. Después se busca una incidencia existente y se contrasta el diagnóstico mediante los canales de ayuda apropiados.

Si se confirma un defecto reproducible, el informe debe seguir la guía del proyecto y describir los hechos comprobados. La guía vigente de Netgate rechaza informes generados mediante IA o sistemas similares. El remitente debe revisar esos requisitos y redactar el informe a partir de sus observaciones verificadas. [7]

105.14. Cuando no se abre un recurso de ayuda

Los recursos de Help son páginas web que normalmente abre el navegador del equipo administrador. Por tanto, su acceso depende también de la resolución DNS, la conectividad, el proxy y la confianza de certificados de ese equipo. Que la GUI local sea accesible no garantiza que el navegador pueda llegar a un sitio externo.

1. Comprobar qué recurso se intenta abrir y revisar la dirección mostrada en el navegador.
2. Distinguir un error de DNS, de conexión, de certificado o de autorización del propio sitio.
3. Probar el portal oficial correspondiente desde el mismo equipo administrador.
4. Si el recurso requiere una cuenta o cobertura, utilizar el acceso previsto para ese servicio.
5. Si la página se ha trasladado, buscar el tema desde el índice oficial y actualizar el marcador local.

El acceso web desde el equipo administrador y una prueba generada por pfSense tienen orígenes distintos. Comprobar DNS, conectividad, navegador y proxy del puesto antes de modificar reglas para resolver el acceso a la ayuda.

105.15. Glosario técnico

Término	Definición aplicada
Ayuda contextual	Referencia relacionada con la página o función que se está consultando.
Documentación	Contenido técnico que describe conceptos, opciones y procedimientos.
Bug o defecto	Problema del software que debe distinguirse de una configuración incorrecta.
Incidencia operativa	Problema de funcionamiento que necesita diagnóstico y resolución.
Redmine	Plataforma utilizada por el proyecto para registrar y seguir incidencias.
TAC	Centro de asistencia técnica de Netgate.
Reproducción	Conjunto de condiciones y pasos con los que se observa de nuevo un problema.
Regresión	Fallo en un comportamiento que funcionaba en una versión o situación anterior.
NDI	Netgate Device ID utilizado para identificar una instalación en procesos de servicio.

105.16. Referencias oficiales

Los enlaces siguientes permiten consultar los recursos principales y sus instrucciones. El destino final de un acceso del menú puede variar por las redirecciones vigentes.

[1] Netgate Finding Information and Getting Help
https://docs.netgate.com/pfsense/en/latest/general/help.html

[2] Proyecto pfSense Definición pública del menú Help
https://github.com/pfsense/pfsense/blob/master/src/usr/local/www/head.inc

[3] Netgate The pfSense Documentation
https://docs.netgate.com/pfsense/en/latest/

[4] Proyecto FreeBSD FreeBSD Handbook
https://docs.freebsd.org/en/books/handbook/

[5] Netgate Using Software from FreeBSD
https://docs.netgate.com/pfsense/en/latest/recipes/freebsd-pkg-repo.html

[6] Proyecto pfSense Redmine issue tracker
https://redmine.pfsense.org/

[7] Netgate Reporting Issues with pfSense Software
https://docs.netgate.com/pfsense/en/latest/development/bug-reports.html

[8] Netgate User Forum
https://forum.netgate.com/

[9] Netgate Global Support
https://www.netgate.com/support

[10] Netgate How to Sign Up for a TAC Subscription
https://docs.netgate.com/pfsense/en/latest/solutions/reference/tac-signup.html

[11] Netgate Security Information
https://www.netgate.com/security