pfSense® software

REDES, FIREWALL Y SEGURIDAD

Arquitectura, administración y laboratorios prácticos

Publicación técnica independiente





Oscar de la Cuesta
palentino.es

Primera edición · octubre de 2026

Créditos, licencia de uso y marcas

© 2026 Oscar de la Cuesta Campillo. Algunos derechos reservados.

Primera edición: octubre de 2026 · palentino.es

Licencia de la obra. Los materiales editoriales originales de este libro se ofrecen bajo Creative Commons Reconocimiento-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0). La licencia permite copiar y compartir la obra, íntegra o en parte, sin fines comerciales, sin difundir adaptaciones y con atribución. Consultar las condiciones oficiales de CC BY-NC-ND 4.0.

Lectura, citas y ejemplos. Se permite buscar, seleccionar y copiar texto, así como citar fragmentos de acuerdo con la licencia y con los límites y excepciones legales. Como autorización adicional, los comandos y configuraciones breves de los laboratorios pueden copiarse, ejecutarse y adaptarse en sistemas propios o autorizados, también en entornos profesionales. El resto de la obra se rige por la licencia indicada.

Independencia editorial. Esta publicación es técnica e independiente: no es documentación oficial ni está afiliada, patrocinada o respaldada por Netgate o Electric Sheep Fencing LLC. Las marcas se utilizan únicamente para identificar las tecnologías estudiadas, sin sugerir certificación ni autorización de sus titulares.

Marcas y programas. pfSense® es una marca registrada de Electric Sheep Fencing LLC y Netgate® es una marca registrada de Rubicon Communications LLC. Los restantes nombres y marcas son de sus titulares. La licencia Creative Commons no alcanza a marcas, programas o materiales ajenos a los derechos editoriales del autor.

Originalidad y referencias. Los textos, ejemplos, esquemas y laboratorios de la obra se presentan como elaboración editorial propia, salvo indicación expresa. La documentación oficial y los estándares se citan como fuentes de contraste; sus derechos permanecen con sus titulares.

Condiciones de difusión. Se permite compartir gratuitamente la obra original no modificada, completa o por partes, respetando las condiciones de atribución y NoComercial de CC BY-NC-ND 4.0. No se permite explotarla comercialmente ni distribuir traducciones o versiones adaptadas sin autorización. Para usos fuera de la licencia: palentino.es. Se mantienen las excepciones legales aplicables.

Aviso técnico. Las instrucciones pueden afectar a la conectividad, la seguridad y la disponibilidad. Antes de intervenir en producción, compruebe versiones y compatibilidad, realice copias de seguridad y disponga de acceso de recuperación. Cada persona debe validar los cambios en su propio entorno.

Estado técnico de referencia. Revisión cerrada el 8 de octubre de 2026, tomando como referencia pfSense CE 2.9.0 y pfSense Plus 26.07. Deben verificarse funciones, licencias y versiones vigentes en sus fuentes oficiales antes de aplicar procedimientos.

Referencia temporal
Los procedimientos sensibles a versión deben contrastarse con la instalación y documentación vigentes.

A Bea

por acompañarme en cada proyecto, por tu paciencia, tu apoyo y por estar siempre.
Este libro también es un poco tuyo.

Prólogo

Administrar un firewall es fácil mientras todo funciona. La dificultad aparece cuando una regla aparentemente correcta no se evalúa, una VPN negocia pero no transporta tráfico, una segunda WAN cambia el camino de retorno o una máquina virtual depende del mismo firewall que debería protegerla. En esos momentos los menús dejan de ser suficientes y solo queda el modelo mental que el administrador haya construido.

Este libro nace precisamente para construir ese modelo. pfSense ofrece una interfaz capaz de simplificar tareas complejas, pero detrás continúan existiendo Ethernet, IPv4 e IPv6, tablas de rutas, estados, traducciones, DNS, certificados, colas, procesos, controladores y decisiones de diseño. La intención de estas páginas es hacer visible esa capa y enseñar a relacionarla con lo que el operador observa en la WebGUI.

He escrito este libro con una idea sencilla: que una persona pueda cerrar la WebGUI y seguir entendiendo qué está ocurriendo en la red. He preferido detenerme en el recorrido de los paquetes, en las decisiones que hay detrás de cada regla y en los fallos que obligan a razonar, porque ahí es donde de verdad se aprende. No busco que el lector copie mis configuraciones, sino que llegue a construir y defender las suyas con criterio.

Por eso el recorrido no empieza con una colección de recetas. Empieza por la historia y la arquitectura, continúa con hardware e interfaces, construye el direccionamiento y el routing, entra después en PF y NAT y, a partir de ahí, añade servicios, VPN, seguridad, redundancia, monitorización y virtualización. Los laboratorios del final no son ejercicios independientes: son la consecuencia natural de todo lo aprendido antes.

La metodología se repite deliberadamente. Primero comprender; después construir; a continuación comprobar; luego romper de forma controlada; por último diagnosticar y llevar el resultado a producción. Esa secuencia obliga a responder algo más importante que «qué opción marco»: obliga a explicar qué decisión de red representa esa opción y qué evidencia demostraría que funciona.

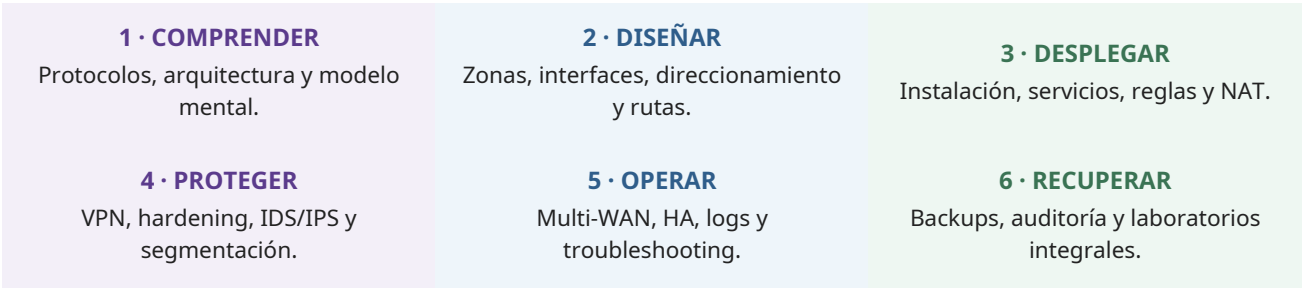
También se ha buscado que la obra siga siendo útil cuando cambie una pantalla. pfSense es un producto vivo y sus versiones evolucionan. Las rutas de menú pueden moverse, los paquetes pueden ganar o perder funciones y una recomendación puede necesitar matices nuevos. En cambio, conceptos como ruta de ida y vuelta, estado, ámbito de broadcast, traducción, identidad criptográfica o punto único de fallo tienen una vida mucho más larga.

El libro puede leerse de principio a fin, pero también pretende servir como obra de consulta. Un administrador puede volver al capítulo de estados durante un incidente, revisar la parte de Multi-WAN antes de añadir un segundo operador, consultar el laboratorio de alta disponibilidad antes de una ventana de mantenimiento o utilizar los anexos como lista de comprobación. La estructura intenta que cada regreso al libro aporte contexto, no solo instrucciones.

Finalmente, esta es una obra independiente. Se apoya en documentación primaria, estándares y pruebas reproducibles para verificar hechos, pero la explicación, los ejemplos y la secuencia pedagógica son propios. El objetivo no es sustituir documentación oficial ni soporte profesional. Es ofrecer algo distinto: criterio técnico para entender por qué una red se comporta como se comporta.

Oscar de la Cuesta

Figura 1. Recorrido de aprendizaje del libro



Sobre el autor



Oscar de la Cuesta Campillo

Soy Ingeniero Informático y Técnico Superior en Telecomunicaciones. Estoy colegiado con el n.º 406 en el Ilustre Colegio Profesional de Ingenieros en Informática de Castilla y León (CPIICyL).

Durante más de 27 años de experiencia profesional he participado en proyectos de muy diversa naturaleza, desarrollados en sectores como la consultoría, el metal, la aeronáutica y la industria agroalimentaria. Esta trayectoria me ha permitido adaptarme a entornos y necesidades muy diferentes, manteniendo siempre el foco en el cumplimiento de los objetivos, los plazos establecidos y la calidad de los resultados.

A lo largo de estos años he trabajado en ámbitos relacionados con la administración de sistemas, bases de datos, programación, consultoría, Internet, arquitectura web y formación. También he impartido formación en técnicas de seguridad informática y protección de datos en la Universidad de Salamanca, y en redes, SEO y optimización web dentro del Máster de Marketing Digital de la Universidad Europea Miguel de Cervantes.

Entre los reconocimientos recibidos figuran el Primer Premio Internet 2005 por Trazagest, otorgado por la Junta de Castilla y León, y el Primer Premio Internet 2004 por un portal multimedia de la provincia de Soria. Desde palentino.es y ctomanager.com comparto proyectos, experiencias y contenidos tecnológicos con una orientación eminentemente práctica.

Web: palentino.es · ctomanager.com

Actividad profesional y publicaciones

Gestiono y evoluciono tecnología, infraestructura, seguridad, sistemas, comunicaciones, automatización y continuidad, conectando la operativa IT con las necesidades reales del negocio. Busco convertir problemas técnicos complejos en soluciones sencillas, seguras, documentadas y sostenibles.

Soy también autor de otras publicaciones técnicas de informática, entre ellas trabajos sobre Windows Server, Proxmox y otros ámbitos de administración de sistemas e infraestructura.

Índice general

Parte I — Historia, fundamentos y ecosistema 19
Capítulo 1. De una idea compacta a una plataforma de red 21
Capítulo 2. Qué es pfSense cuando dejamos de verlo como una pantalla 25
Capítulo 3. FreeBSD y PF: el suelo técnico sobre el que caminamos 28
Capítulo 4. Netgate, CE, Plus y el papel del hardware 31
Capítulo 5. El viaje de un paquete: el mapa mental para todo el libro 34

Parte II — Hardware, interfaces y diseño previo a la instalación 39
Capítulo 6. Dimensionar antes de comprar 41
Capítulo 7. Anatomía del hardware de un firewall 45
Capítulo 8. Interfaces: de un puerto físico a una zona de seguridad 51
Capítulo 9. Appliance, hardware genérico o máquina virtual 55
Capítulo 10. Diseñar la red antes de instalar 58
Capítulo 11. Plan de instalación: convertir el diseño en decisiones 61

Parte III — Instalación, primer arranque y configuración base 67
Capítulo 12. Preparar la instalación sin improvisar 69
Capítulo 13. Del arranque al sistema instalado 72
Capítulo 14. Primer arranque: interfaces y consola 74
Capítulo 15. Primer acceso a la WebGUI: configuración mínima segura 77
Capítulo 16. Servicios base: DNS, DHCP, actualización y administración 80
Capítulo 17. La primera copia de seguridad y la puesta en servicio 83
Capítulo 18. Diagnóstico del primer día 87

Parte IV — Direccionamiento, IPv4/IPv6, interfaces lógicas y routing 90
Capítulo 19. Direcciones, prefijos y decisiones de encaminamiento 92
Capítulo 20. IPv4 y subnetting aplicado al firewall 94
Capítulo 21. IPv6 sin pensar como si fuera IPv4 97
Capítulo 22. Interfaces físicas, virtuales y lógicas 100
Capítulo 23. Gateways, tabla de rutas y rutas estáticas 102
Capítulo 24. VLAN: segmentar capa 2 sin multiplicar switches 104
Capítulo 25. LAGG, bridges, MTU y límites físicos 107
Capítulo 26. Laboratorio: construir una pyme segmentada desde la tabla de rutas 109

Parte V — PF, reglas, estados y NAT 115
Capítulo 27. PF y el modelo de firewall con estado 117
Capítulo 28. Anatomía de una regla de firewall 119
Capítulo 29. Orden de reglas, grupos y Floating Rules 121
Capítulo 30. Aliases: convertir reglas en una política legible 123
Capítulo 31. La tabla de estados: memoria operativa del firewall 125
Capítulo 32. NAT: cambiar identidades sin confundirlo con seguridad 127
Capítulo 33. Port Forward y publicación controlada de servicios 129
Capítulo 34. 1:1 NAT y Outbound NAT 131
Capítulo 35. Laboratorio integral: publicar, traducir y diagnosticar 133

Parte VI — DHCP, DNS, NTP y servicios de infraestructura 141
Capítulo 36. DHCP: mucho más que entregar una dirección IP 143
Capítulo 37. Kea DHCP en pfSense: diseño y operación 146
Capítulo 38. DHCP Relay: cuando el servidor está en otra red 148
Capítulo 39. IPv6: SLAAC, DHCPv6 y Router Advertisements 149
Capítulo 40. DNS Resolver y DNS Forwarder: dos modelos distintos 151
Capítulo 41. Diseñar DNS interno sin crear una caja negra 153
Capítulo 42. NTP y Dynamic DNS: tiempo e identidad externa 155
Capítulo 43. Otros servicios de red y control de acceso 157
Capítulo 44. Laboratorio: servicios de infraestructura para una pyme segmentada 159
Capítulo 45. Troubleshooting de servicios: convertir síntomas en pruebas 162

Parte VII — VPN, criptografía y acceso seguro 166
Capítulo 46. Qué resuelve una VPN 168
Capítulo 47. Criptografía y PKI para administradores de red 170
Capítulo 48. Elegir tecnología: WireGuard, OpenVPN o IPsec 172
Capítulo 49. WireGuard: simple en la superficie, preciso en el routing 174
Capítulo 50. OpenVPN: identidad, políticas y flexibilidad 176
Capítulo 51. IPsec: IKE, SA, políticas y VTI 178
Capítulo 52. Acceso remoto: identidades, RADIUS, LDAP y MFA 180
Capítulo 53. Site-to-site: routing, DNS y redes solapadas 182
Capítulo 54. Rendimiento, Multi-WAN, alta disponibilidad y operación 184
Capítulo 55. Troubleshooting y laboratorio integral 186

Parte VIII — Seguridad avanzada, IDS/IPS y hardening 191
Capítulo 56. Seguridad antes de los paquetes: modelo de amenaza y defensa en profundidad 193
Capítulo 57. Hardening del propio firewall 195
Capítulo 58. IDS/IPS: observar no es lo mismo que bloquear 197
Capítulo 59. Suricata: IDS/IPS multihilo y operación en línea 199
Capítulo 60. Snort: firmas, reputación y evolución hacia Snort 3 201
Capítulo 61. Afinar IDS/IPS: del ruido a una señal útil 202
Capítulo 62. pfBlockerNG, DNSBL, GeoIP y reputación 204
Capítulo 63. Segmentación avanzada, egress filtering y control lateral 206
Capítulo 64. Seguridad operativa: actualizaciones, parches, logs y copias 208
Capítulo 65. Laboratorio integral de hardening y respuesta a incidentes 210

Parte IX — Multi-WAN y alta disponibilidad 216
Capítulo 66. Disponibilidad: diseñar antes de duplicar 219
Capítulo 67. Gateway monitoring: medir el camino real 221
Capítulo 68. Gateway Groups: failover, balanceo y tiers 223
Capítulo 69. Policy routing: decidir por dónde sale cada tráfico 225
Capítulo 70. Multi-WAN con DNS, NAT, VPN y servicios 227
Capítulo 71. CARP: redundancia de direcciones 228
Capítulo 72. pfsync: conservar la tabla de estados 229
Capítulo 73. XMLRPC: mantener dos configuraciones coherentes 230
Capítulo 74. Diseñar un clúster HA completo 231
Capítulo 75. Pruebas de fallo, operación y troubleshooting 233

Parte X — Monitorización y troubleshooting avanzado 237
Capítulo 76. Observabilidad: medir antes de intervenir 239
Capítulo 77. Logs: reconstruir lo que ocurrió 241
Capítulo 78. Estados, pfTop y pfInfo: ver qué está haciendo PF 243
Capítulo 79. Packet capture y tcpdump: observar el paquete real 245
Capítulo 80. Routing, vecinos y pruebas activas 247
Capítulo 81. CLI y pfctl: entrar debajo de la WebGUI sin romper el sistema 249
Capítulo 82. Rendimiento: buscar el cuello de botella correcto 251
Capítulo 83. Tres métodos de troubleshooting que deben convertirse en hábito 253
Capítulo 84. Casos de diagnóstico reproducibles 255
Capítulo 85. Laboratorio integral: investigar sin adivinar 257

Parte XI — Virtualización y despliegue avanzado 261
Capítulo 86. ¿Debe el firewall ser una máquina virtual? 263
Capítulo 87. La cadena virtual: del cable a vtnet0 265
Capítulo 88. Proxmox VE: pfSense sobre KVM 266
Capítulo 89. PCI passthrough y SR-IOV 268
Capítulo 90. VMware vSphere / ESXi 269
Capítulo 91. Microsoft Hyper-V 270
Capítulo 92. Rendimiento y detalles que solo aparecen en virtualización 271
Capítulo 93. El hipervisor se convierte en parte del perímetro 273
Capítulo 94. Alta disponibilidad, migración y recuperación 274
Capítulo 95. Laboratorios y arquitecturas de referencia 276

Parte XII — Laboratorios integrales, recuperación y anexos de referencia 280
Capítulo 96. Método común: de requisito a evidencia 282
Capítulo 97. Laboratorio integral: hogar avanzado 284
Capítulo 98. Laboratorio integral: pyme segmentada 286
Capítulo 99. Laboratorio integral: DMZ y publicación controlada 288
Capítulo 100. Laboratorio integral: empresa multisede 290
Capítulo 101. Laboratorio de continuidad: HA + Multi-WAN + fallo real 292
Capítulo 102. Recuperación: de config.xml a una reconstrucción completa 294
Capítulo 103. Auditoría técnica de pfSense 296
Capítulo 104. Operación: cambios, actualizaciones y documentación viva 298
Capítulo 105. Anexos rápidos de referencia 300

Bibliografía y referencias técnicas consolidadas 304

Recursos de consulta: Diagnóstico rápido · Índice analítico · Notas de edición y erratas

Antes de empezar

Este libro nace con una intención muy concreta: que el lector no se limite a saber dónde hacer clic en pfSense, sino que sea capaz de explicar qué está ocurriendo en la red antes, durante y después de cada decisión de configuración. El objetivo no es memorizar pantallas. Es construir criterio técnico.

pfSense puede utilizarse como un sencillo firewall doméstico, como router de una pequeña empresa, como concentrador VPN, como pieza de segmentación entre VLAN, como nodo de alta disponibilidad o como plataforma virtualizada. La interfaz gráfica facilita muchas tareas, pero también puede ocultar conceptos esenciales: estados, rutas, traducciones de direcciones, tablas, gateways, interfaces lógicas, servicios y dependencias. Este libro intentará hacer visible esa capa que normalmente queda detrás de la WebGUI.

Por ello, cada bloque combina tres niveles: fundamento, aplicación y diagnóstico. Primero se explica el concepto; después se construye una configuración; finalmente se analiza qué ocurre cuando algo falla. Esta secuencia se mantendrá a lo largo de toda la obra.

◆ **Idea central**
Configurar sin entender produce redes frágiles. Entender sin practicar produce conocimiento difícil de aplicar. El libro está diseñado para unir ambas cosas: modelo mental + laboratorio + diagnóstico.

Un libro independiente, no una reproducción de documentación oficial

La obra está escrita desde cero y utiliza una estructura propia. La documentación de pfSense, FreeBSD, estándares de Internet y fuentes técnicas de fabricantes se emplea únicamente para comprobar hechos, sintaxis, compatibilidades, comportamientos y conceptos. No se adopta como guion, ni se traduce capítulo por capítulo, ni se reproducen sus tablas, diagramas o textos como sustituto de una explicación propia.

Esto permite que el libro siga una progresión didáctica distinta: partir de modelos mentales sencillos, aumentar gradualmente la complejidad y regresar continuamente a escenarios reales. Cuando sea útil se citarán las fuentes que permitan al lector ampliar información o comprobar una especificación, pero la explicación, los ejemplos, los diagramas y los laboratorios son parte de una obra independiente.

✓ Criterio de independencia
En todos los capítulos prevalecerá la originalidad: redacción propia, orden propio, ejemplos propios, topologías propias y diagramas propios. Las fuentes oficiales sirven para verificar; no para imitar.

Aviso de independencia y marcas

Esta publicación es una obra técnica independiente. Utiliza la marca pfSense® software únicamente para identificar la tecnología estudiada y no pretende presentarse como documentación oficial, material certificado ni publicación patrocinada por Netgate.

Las atribuciones de marca, condiciones de reutilización de ejemplos y criterios de fuentes se detallan en la página de créditos. Los datos sensibles a versión se fechan y deben contrastarse cuando el lector trabaje con una versión posterior.

1. Qué pretende conseguir este libro

La meta final es que un lector pueda pasar de una red básica a una arquitectura profesional sin sentir que cada función de pfSense es una isla independiente. Firewall, routing, NAT, DNS, DHCP, VLAN, VPN, alta disponibilidad y monitorización forman un sistema. Cuando se comprenden las relaciones entre ellos, las configuraciones dejan de parecer recetas y empiezan a tener sentido.

1.1 De “funciona” a “sé por qué funciona”

Una red puede funcionar aparentemente bien y, sin embargo, estar mal diseñada. Puede depender de una regla demasiado amplia, de un NAT innecesario, de un DNS mal resuelto o de un gateway cuyo comportamiento solo se descubre cuando falla el enlace principal. Por eso no nos conformaremos con alcanzar conectividad.

- Saber qué interfaz recibe un paquete y qué interfaz debería utilizar para salir.
- Distinguir filtrado, routing y NAT como procesos diferentes aunque participen en la misma comunicación.
- Entender por qué una regla aparentemente correcta puede no evaluarse como esperamos.
- Relacionar DNS, DHCP, gateways y rutas con el comportamiento observado por un usuario.
- Diagnosticar por capas antes de modificar configuraciones al azar.
- Diseñar pensando en mantenimiento, seguridad, recuperación y crecimiento.

1.2 Aprender a leer una red

Una de las habilidades centrales será aprender a “leer” una topología. Antes de abrir pfSense, el lector debería poder señalar zonas de confianza, fronteras, rutas probables, puntos únicos de fallo y lugares donde tendría sentido registrar o inspeccionar tráfico. Esa lectura previa reduce errores y hace que la interfaz gráfica se convierta en una herramienta, no en el punto de partida del razonamiento.

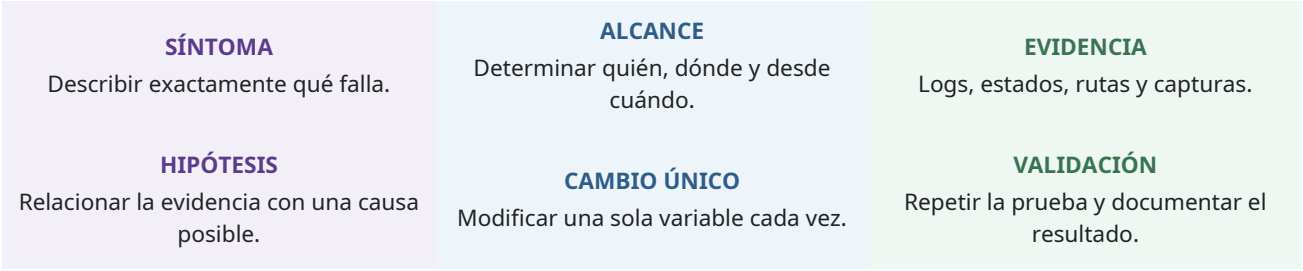
? Pregunta que repetiremos

¿Qué camino debería seguir este paquete, qué decisiones encontrará por el camino y qué evidencia puedo recoger si no llega a destino?

1.3 Adquirir una metodología de diagnóstico

En los capítulos de troubleshooting no se enseñará una colección de trucos aislados. Se aplicará un método repetible: formular el síntoma, delimitar el alcance, observar interfaces, comprobar direccionamiento, rutas y estados, validar resolución de nombres, capturar tráfico cuando sea necesario y modificar una sola variable cada vez. Esta disciplina es mucho más valiosa que memorizar soluciones concretas.

Figura 2. Método de diagnóstico utilizado a lo largo de la obra



2. A quién va dirigido

El libro está pensado para lectores con perfiles diferentes. No exige ser especialista en FreeBSD ni administrador de redes senior, pero sí presupone curiosidad técnica y disposición para practicar. Los conceptos de red fundamentales se explicarán cuando sean necesarios, evitando tanto la simplificación excesiva como la jerga sin contexto.

Perfil	Qué encontrará	Ruta recomendada
Principiante en redes	Fundamentos, terminología, modelos visuales y laboratorios guiados.	Introducción → Parte I → instalación → firewall/NAT → servicios.
Técnico de sistemas	Diseño, integración con servidores, VLAN, VPN, virtualización y diagnóstico.	Partes I-II → redes/routing → VPN → virtualización → troubleshooting.
Administrador de red	Profundidad en reglas, estados, routing, multi-WAN, HA y observabilidad.	Firewall → routing → alta disponibilidad → diagnóstico → laboratorios avanzados.
Profesional de seguridad	Segmentación, exposición de servicios, IDS/IPS, VPN, hardening y análisis de tráfico.	Arquitectura → firewall → seguridad → VPN → capturas y auditoría.
Usuario de Proxmox/VMware/Hyper-V	Diseño virtual, interfaces, bridges, passthrough y escenarios de laboratorio.	Hardware/arquitectura → virtualización → VLAN → HA → laboratorios.

3. Cómo está construido el aprendizaje

3.1 Las tres capas de cada tema

La organización de los capítulos seguirá una pauta deliberada. No todos los temas necesitarán exactamente el mismo número de páginas, pero sí intentaremos mantener la misma lógica pedagógica.

1. Comprender: definición, contexto, componentes y modelo mental.
2. Construir: configuración paso a paso dentro de una topología concreta.
3. Comprobar: pruebas funcionales y evidencias que demuestran que la configuración hace lo esperado.
4. Romper de forma controlada: errores frecuentes o escenarios deliberadamente incorrectos.
5. Diagnosticar: herramientas y razonamiento para localizar la causa.
6. Llevar a producción: consideraciones de seguridad, mantenimiento, respaldo y documentación.

3.2 Las cajas didácticas

A lo largo del libro aparecerán bloques recurrentes. No son adornos: permiten separar rápidamente teoría, advertencias y práctica.

Caja	Función
Qué ocurre realmente	Explica el proceso interno que la interfaz oculta o simplifica.
En producción	Traslada el concepto a un entorno real: mantenimiento, redundancia, soporte, seguridad y operación.
Error frecuente	Describe fallos habituales y, sobre todo, por qué parecen razonables cuando se cometen.
Laboratorio	Propone una práctica reproducible con objetivo, topología, pasos, validación y limpieza.
Comprobación	Indica qué evidencia debe observarse para considerar que el resultado es correcto.
Seguridad	Marca decisiones con impacto directo sobre exposición, privilegios, cifrado o superficie de ataque.
Idea clave	Resume el concepto que merece permanecer en la memoria incluso si se olvidan los pasos exactos.

3.3 Capturas, diagramas y comandos

Las capturas de pantalla se utilizarán cuando aporten orientación visual, no para llenar páginas. Siempre que un concepto pueda explicarse mejor con una topología, un flujo o un esquema de capas, se priorizará un diagrama propio. Los comandos aparecerán acompañados de una explicación de propósito, contexto y resultado esperado.

En los procedimientos sensibles a versión, la pantalla exacta puede cambiar. Por eso la explicación intentará apoyarse en conceptos persistentes: interfaz de entrada, dirección de origen, destino, gateway, estado, alias, regla, servicio, certificado o fase de negociación. De esta forma, el lector podrá adaptarse mejor a futuras revisiones del producto.

4. El laboratorio base del libro

Para evitar ejemplos inconexos, gran parte del libro utilizará una topología base que irá creciendo. No será una obligación reproducirla exactamente: su función es dar continuidad a los ejemplos y permitir que un laboratorio se apoye en el anterior.

▣ Topología conceptual
Internet/ISP → WAN de pfSense → núcleo de seguridad → LAN de administración + VLAN usuarios + VLAN servidores + VLAN invitados/IoT. Más adelante añadiremos una segunda sede, VPN, segundo enlace WAN y un nodo de alta disponibilidad.

4.1 Direccionamiento de laboratorio

Los rangos que aparezcan en ejemplos se elegirán para ser fácilmente reconocibles como redes de laboratorio. Cuando se utilicen direcciones privadas, se indicará su función dentro de la topología. En ejemplos públicos se evitará sugerir direcciones reales de terceros como si pertenecieran al escenario.

Zona	Ejemplo	Función	Confianza inicial
LAN-MGMT	192.168.10.0/24	Administración de infraestructura	Alta
VLAN-USERS	192.168.20.0/24	Puestos de usuario	Media
VLAN-SERVERS	192.168.30.0/24	Servicios internos	Controlada
VLAN-GUEST	192.168.40.0/24	Invitados / dispositivos no confiables	Baja
TRANSIT/VPN	redes específicas por laboratorio	Enlaces entre sedes o túneles	Depende del escenario

4.2 Laboratorio físico y laboratorio virtual

El libro contemplará ambos enfoques. Un equipo físico permite trabajar con interfaces y cableado reales; un entorno virtual acelera pruebas, snapshots, escenarios multi-sede y recuperación. La virtualización no se tratará como una simple forma de “instalar pfSense”, sino como un diseño que introduce su propia capa de switching, bridges, VLAN, drivers y riesgos de conectividad.

Cuando un laboratorio pueda hacerse tanto en hardware como en Proxmox, VMware o Hyper-V, se indicarán las diferencias relevantes. No se asumirá que virtualizar elimina la necesidad de comprender la red física: solo desplaza parte de ella al hipervisor.

5. Convenciones utilizadas en el libro

5.1 Nombres y ejemplos

- WAN, LAN, OPT, VLAN y nombres de interfaces se escribirán de forma consistente dentro de cada escenario.
- Los nombres de hosts y dominios de ejemplo serán ficticios y reconocibles como tales.
- Las credenciales mostradas serán de laboratorio y nunca se presentarán como contraseñas recomendadas.
- Las direcciones IP, puertos y redes se acompañarán de contexto para evitar recetas ambiguas.
- Cuando una función dependa de una edición o versión determinada, se marcará de forma explícita.

5.2 Comandos y configuración

Los comandos de consola se diferenciarán visualmente del texto. Antes de ejecutar una orden potencialmente destructiva se explicará qué modifica y cómo volver atrás. En tareas administrativas se priorizarán procedimientos reproducibles y reversibles.

! Regla de laboratorio

Antes de cambiar firewall, routing, VPN o interfaces en un equipo remoto, debe existir un camino de recuperación: consola, acceso fuera de banda, snapshot válido o presencia física. El libro recordará esta regla cuando sea relevante.



5.3 “Permitir” no significa “seguro”

Una regla que permite tráfico solo resuelve una parte del problema. También importan el origen, el destino, el servicio, el sentido de la comunicación, la exposición, la autenticación y la capacidad de detectar abusos. Por eso no presento “any to any” como una solución segura en escenarios de producción.

6. Rutas de lectura

El libro puede leerse de principio a fin, pero no todos los lectores tienen la misma necesidad. Estas rutas permiten llegar antes a un objetivo sin perder los fundamentos imprescindibles.

6.1 Ruta de iniciación

Introducción → historia y fundamentos → hardware e interfaces → instalación → direccionamiento → reglas básicas → NAT → DHCP/DNS → backup y diagnóstico elemental.

6.2 Ruta de administración empresarial

Fundamentos → diseño → VLAN → routing → aliases y políticas → VPN → multi-WAN → monitorización → alta disponibilidad → backups → laboratorios de sede central y delegación.

6.3 Ruta de seguridad

Modelo de estados → política de mínimo privilegio → segmentación → exposición controlada → VPN → IDS/IPS → hardening → logs → captura de paquetes → respuesta ante incidentes de red.

6.4 Ruta de virtualización

Arquitectura → interfaces → bridges y VLAN → instalación virtual → VirtIO/VMXNET3 según plataforma → passthrough cuando proceda → HA del hipervisor frente a HA del firewall → laboratorios multi-sede.

7. Mapa general de la obra

La obra se organiza en doce partes que avanzan desde los fundamentos y el diseño hasta la operación, la alta disponibilidad, la virtualización, el diagnóstico y los laboratorios integrales. El recorrido está pensado para que cada bloque se apoye en los anteriores sin convertir los capítulos en recetas aisladas.

Parte	Objetivo
Parte I — Historia, fundamentos y ecosistema	Origen, FreeBSD, PF, papel de Netgate, ediciones y primer modelo mental del flujo de tráfico.
Parte II — Hardware, interfaces y diseño previo a la instalación	Dimensionamiento, appliances y hardware genérico, CPU, RAM, almacenamiento, NIC, interfaces y diseño previo.
Parte III — Instalación, primer arranque y configuración base	Instalación física y virtual, consola, WAN/LAN, WebGUI, servicios mínimos, actualización, backup y diagnóstico inicial.
Parte IV — Direccionamiento, IPv4/IPv6, interfaces lógicas y routing	Subredes, IPv4/IPv6, gateways, rutas estáticas, VLAN, LAGG, bridges, MTU y segmentación.
Parte V — PF, reglas, estados y NAT	Firewall stateful, aliases, floating rules, tabla de estados, Port Forward, 1:1 y Outbound NAT.
Parte VI — DHCP, DNS, NTP y servicios de infraestructura	Kea DHCP, relay, SLAAC/DHCPv6/RA, Unbound, DNS, NTP, Dynamic DNS y servicios auxiliares.
Parte VII — VPN, criptografía y acceso seguro	PKI, WireGuard, OpenVPN, IPsec, RADIUS/MFA, acceso remoto, site-to-site y troubleshooting.
Parte VIII — Seguridad avanzada, IDS/IPS y hardening	Hardening, Suricata, Snort, pfBlockerNG, DNSBL, reputación, egress filtering, segmentación y respuesta.
Parte IX — Multi-WAN y alta disponibilidad	Gateway monitoring, grupos y policy routing, CARP, pfsync, XMLRPC, failover, balanceo y pruebas de fallo.
Parte X — Monitorización y troubleshooting avanzado	Logs, estados, pfTop/pfInfo, packet capture, tcpdump, pfctl, rutas, DNS, rendimiento y diagnóstico por capas.
Parte XI — Virtualización y despliegue avanzado	Proxmox, VMware, Hyper-V, VirtIO, VLAN-aware, passthrough, seguridad del hipervisor, HA y recuperación.
Parte XII — Laboratorios integrales, recuperación y anexos de referencia	Escenarios completos, recuperación, auditoría, operación, checklists, runbooks y referencia rápida.

8. Fuentes y verificación técnica

Un libro original no significa un libro aislado de las fuentes. Al contrario: cuanto más técnica es una afirmación, más importante es comprobarla. La diferencia está entre utilizar documentación para verificar y utilizarla como sustituto de la escritura propia.

8.1 Jerarquía de fuentes

1. Documentación y notas oficiales de pfSense/Netgate para comportamiento, compatibilidad y funciones concretas del producto.
2. Documentación oficial de FreeBSD para el sistema base, red, kernel, interfaces y herramientas relacionadas.
3. RFC y documentos IETF cuando se expliquen protocolos de Internet, direccionamiento, routing, DNS, DHCP, IPsec u otros estándares.
4. Documentación de proyectos específicos cuando un paquete o servicio externo tenga comportamiento propio.
5. Laboratorios reproducibles y pruebas controladas para validar procedimientos y observar resultados.

Las fuentes secundarias pueden aportar contexto y experiencias, pero no sustituirán a una especificación o documentación primaria cuando exista una duda técnica importante.

8.2 Cómo abordar los cambios de versión

La interfaz de un producto vivo evoluciona. Cuando cambie una pantalla, el libro intentará conservar utilidad describiendo el objetivo y el flujo lógico además de la ruta de menús. Si una función desaparece, cambia de edición o modifica su comportamiento, se actualizará el capítulo correspondiente sin rehacer artificialmente toda la explicación.

> ↻ **Principio de longevidad**
> Las pantallas envejecen antes que los conceptos. Por eso cada procedimiento debe enseñar el “por qué” además del “dónde”.

9. Qué no pretende ser este libro

- No pretende ser documentación oficial ni reemplazar soporte profesional.
- No pretende enumerar cada opción de cada pantalla sin contexto.
- No pretende presentar una única arquitectura como válida para todas las organizaciones.
- No pretende convertir recomendaciones de laboratorio en reglas universales de producción.
- No pretende ocultar complejidad cuando comprenderla sea importante para seguridad o disponibilidad.
- No pretende copiar la organización de otros manuales: el recorrido responde a una lógica de aprendizaje propia.

10. Comenzar el recorrido

Con esta introducción quedan fijados los criterios de lectura del libro. A partir de aquí comienza la Parte I: antes de instalar nada, entenderemos de dónde viene pfSense, sobre qué base técnica se apoya y cómo debemos imaginar el recorrido de un paquete a través del sistema. Ese modelo mental será el hilo conductor de toda la obra.

> ◆ **La pregunta guía del libro**
> La pregunta no es solo "¿qué opción debo seleccionar?", sino "¿qué decisión de red estoy expresando al seleccionar esta opción?". Esa diferencia resume el espíritu de toda la obra.

Fuentes de referencia de la obra

- Documentación oficial de pfSense y Netgate (consulta técnica y verificación de funciones).
- Documentación oficial del Proyecto FreeBSD.
- RFC y documentación del IETF para estándares y protocolos.
- Documentación de proyectos y paquetes utilizados en laboratorios.
- Pruebas propias en entornos controlados y topologías reproducibles.

Las referencias concretas de cada tema se incluyen al final de la parte correspondiente. La presencia de una fuente no implica que su estructura, redacción o material gráfico se reproduzca en esta obra.

pfSense® software

REDES, FIREWALL Y SEGURIDAD

Arquitectura, administración y laboratorios prácticos

PARTE I

Historia, fundamentos y ecosistema

Oscar de la Cuesta

palentino.es



Primera edición · octubre de 2026

Independencia, fuentes y criterio de originalidad

Este libro es una obra técnica independiente concebida para enseñar pfSense desde una perspectiva progresiva: primero entender el problema que resuelve, después comprender las piezas que lo forman y, por último, aprender a diseñar, desplegar, proteger y diagnosticar redes reales. No es una traducción de la documentación oficial ni intenta reproducir su estructura.

La documentación de pfSense, FreeBSD y Netgate se utiliza como referencia para verificar hechos, versiones, conceptos y comportamiento técnico. La organización de capítulos, la narrativa, los ejemplos, las analogías, los laboratorios, los esquemas y la selección pedagógica son propios de esta obra. Cuando una afirmación depende de una versión concreta se indica de forma expresa, para evitar convertir una explicación válida hoy en una regla aparentemente eterna.

pfSense® es una marca registrada de Electric Sheep Fencing LLC y Netgate® es una marca registrada de Rubicon Communications LLC. Esta obra es independiente y no está afiliada, patrocinada ni respaldada por dichas entidades. Las marcas se utilizan únicamente para identificar las tecnologías tratadas.

Mi criterio de trabajo

En cada capítulo busco explicar los fundamentos con claridad, contrastar las decisiones técnicas y ofrecer ejemplos prácticos que permitan comprender qué ocurre en la red y actuar con criterio.

Cómo leer esta Parte I

Esta primera parte evita deliberadamente empezar por la instalación. Antes de conectar una WAN y una LAN conviene saber qué es pfSense, de dónde procede, por qué se apoya en FreeBSD, qué papel tiene PF y cómo encaja Netgate en el ecosistema. Esta base evita uno de los problemas más comunes de los manuales de administración: aprender pantallas sin construir un modelo mental.

- Capítulo 1: origen y evolución del proyecto, desde m0n0wall hasta el ecosistema actual.
- Capítulo 2: qué es pfSense y cómo debe pensarse como plataforma, no solo como una interfaz web.
- Capítulo 3: FreeBSD y PF como cimientos técnicos.
- Capítulo 4: Netgate, las ediciones CE y Plus y el papel del hardware dedicado.
- Capítulo 5: el recorrido conceptual de un paquete, que servirá de brújula para el resto del libro.

Capítulo 1. De una idea compacta a una plataforma de red

Para entender pfSense conviene empezar antes de pfSense. Su historia no es la de un producto nacido en una gran empresa con un catálogo cerrado, sino la de una necesidad muy concreta: convertir hardware común en un equipo de red robusto y administrable sin obligar al usuario a construir todo el sistema desde cero.

1.1 Antes de pfSense: cuando un firewall era, sobre todo, una máquina dedicada

A principios de los años 2000 el mercado de seguridad perimetral estaba muy polarizado. En un extremo había routers domésticos con pocas opciones y firmware limitado; en el otro, appliances empresariales costosos, con licencias, soporte y modelos de administración propietarios. Entre ambos extremos existía un espacio atractivo para administradores, pequeñas empresas, proveedores de servicios y entusiastas: utilizar un PC o un equipo embebido como router y firewall avanzado.

Los sistemas BSD resultaban especialmente interesantes para este tipo de trabajos. Su tradición en redes, la calidad de su pila TCP/IP, el modelo de licencias y la disponibilidad de herramientas de filtrado permitían construir dispositivos muy especializados. El problema no era únicamente filtrar paquetes: también había que ofrecer configuración persistente, gestión de interfaces, NAT, VPN, DHCP, DNS, monitorización y una forma razonable de operar todo aquello sin editar decenas de ficheros a mano.

En ese contexto apareció m0n0wall. Su importancia histórica no reside solo en las funciones que ofrecía, sino en el concepto: empaquetar un sistema basado en FreeBSD para comportarse como un appliance de red, con una interfaz web y una configuración centralizada. El objetivo estaba muy condicionado por el hardware embebido disponible en aquella época, donde memoria y almacenamiento eran recursos mucho más escasos que hoy.

Idea clave

La gran innovación conceptual no fue inventar el firewall. Fue reunir componentes de sistema, red y seguridad en una experiencia administrable como un appliance.

1.2 m0n0wall como punto de partida, no como destino

En 2004 el proyecto tomó un camino distinto a partir de m0n0wall. Compartía su herencia, pero el horizonte técnico era más amplio: no se trataba de permanecer condicionado por el perfil de los dispositivos embebidos de entonces, sino de aprovechar también PC y servidores capaces de asumir más interfaces, servicios y carga de trabajo. Ese cambio de escala, más que el simple hecho de crear un fork, ayuda a explicar buena parte de la evolución posterior de pfSense.

A partir de ahí las decisiones comenzaron a separarse. Una plataforma destinada a entornos muy distintos necesita combinar interfaces, routing, VPN, extensiones, monitorización y operación de

una forma que no depende de un único tipo de equipo. Al aumentar los recursos disponibles, también aumentó el espacio para construir escenarios que iban mucho más allá del appliance compacto del que procedía la idea original.

La cronología sirve aquí sólo como ancla: el proyecto comenzó en 2004 y la versión 1.0 llegó el 13 de octubre de 2006. Lo verdaderamente útil para el resto del libro es entender lo ocurrido entre ambos hitos: una base heredada fue adquiriendo decisiones propias hasta convertirse en una plataforma con objetivos, ritmo de desarrollo y alcance diferentes.

1.3 El nombre: “hacer comprensible PF”

El nombre pfSense está ligado a PF, el sistema de filtrado de paquetes que constituye una pieza central de la plataforma. La antigua frase asociada al proyecto, “making sense of PF”, resume bien la filosofía: tomar una tecnología potente de filtrado y convertirla en algo que pueda administrarse de forma coherente, visible y repetible.

Conviene detenerse aquí porque ayuda a evitar un error conceptual. pfSense no es simplemente “PF con una web”. La plataforma integra el sistema operativo, mecanismos de red, servicios, almacenamiento de configuración, automatización, paquetes y una interfaz que coordina todos esos elementos. PF es fundamental, pero el producto final es mucho más amplio que el filtro de paquetes aislado.

Esta distinción será constante en el libro. Cuando configuremos una regla desde la WebGUI, intentaremos entender qué representación lógica existe detrás; cuando usemos NAT, estudiaremos cómo se relaciona con estados y rutas; cuando diagnostiquemos una VPN, separaremos la capa criptográfica de la política de firewall. Aprender pfSense de esta manera reduce la dependencia de memorizar menús.

1.4 2006: la versión 1.0 y el comienzo de una etapa estable

La publicación de pfSense 1.0 en octubre de 2006 marcó el paso de proyecto en construcción a plataforma que podía desplegarse con una referencia de versión clara. En los años siguientes llegaron versiones 1.2.x y, posteriormente, la rama 2.x. Cada salto fue incorporando cambios en componentes, hardware compatible, interfaz y capacidades.

La relevancia de esta evolución no debe medirse solo por números de versión. Los firewalls viven en uno de los puntos más sensibles de una red. Una actualización puede afectar conectividad, VPN, traducciones NAT, compatibilidad de tarjetas de red o reglas de filtrado. Por eso, en una plataforma de este tipo, madurez significa también procesos de actualización, capacidad de restauración, documentación y mecanismos para diagnosticar fallos.

A lo largo del libro veremos que “actualizar” no debe confundirse con “hacer clic en Update”. En entornos profesionales hay que conocer la versión de configuración, las dependencias de paquetes, la base FreeBSD utilizada, los cambios de comportamiento y el plan de reversión. Esta cultura operativa es parte de la madurez que fue adquiriendo el ecosistema.

1.5 Netgate entra en escena

Netgate, nombre comercial de Rubicon Communications, fue fundada en 2004. La propia compañía sitúa sus primeros productos en firewalls y puntos de acceso, inicialmente con m0n0wall y más tarde con pfSense. Su relación con el proyecto evolucionó desde el apoyo temprano hasta asumir su patrocinio en 2012.

Desde ese momento la historia de pfSense y Netgate quedó fuertemente conectada. Netgate pasó a aportar infraestructura, desarrollo, pruebas, distribución, documentación, soporte y una línea de appliances. Esto transformó el proyecto en un ecosistema donde conviven una comunidad amplia, una edición comunitaria, ofertas comerciales, hardware y servicios de soporte.

Para un lector técnico es importante separar tres planos: el software, la empresa y la marca. El software puede tener unas condiciones de licencia; la documentación, otras; la marca y los logotipos, otras diferentes. Esta obra trata los tres ámbitos con claridad para que el lector entienda la tecnología sin confundir “proyecto abierto” con “todo lo relacionado con el nombre puede reutilizarse de cualquier forma”.

1.6 2021: Community Edition y pfSense Plus

A partir de 2021 ya no basta con utilizar la palabra pfSense como si describiera una única línea de producto. La aparición de pfSense Plus y la denominación Community Edition hicieron necesario distinguir edición, versión y disponibilidad de funciones cada vez que se documenta una característica. Las dos líneas comparten una historia y numerosos conceptos, pero no deben darse por idénticas en calendario, soporte o capacidades.

pfSense CE continúa siendo la referencia comunitaria y puede ejecutarse en hardware compatible propio. pfSense Plus es la línea comercial mantenida por Netgate y está especialmente vinculada a sus appliances y ofertas. En determinados momentos pueden diferir en versión de FreeBSD, ritmo de publicación y funciones disponibles.

A octubre de 2026, la tabla oficial de versiones sitúa pfSense CE 2.9.0 como versión soportada, publicada el 20 de agosto de 2026, y pfSense Plus 26.07 como versión soportada, publicada el 13 de agosto de 2026. La rama Plus 26.10 figura todavía como futura en la documentación consultada. Estos datos son deliberadamente fechados: sirven para saber desde qué punto histórico se escribe el libro, no para convertir una versión concreta en parte permanente de la teoría.

1.7 Una cronología útil

Año	Hito	Por qué importa
2004	pfSense nace como fork de m0n0wall.	Se abre el camino hacia una plataforma más amplia para PC y servidores.
2006	Publicación de pfSense 1.0.	El proyecto alcanza una referencia estable de versión.
2012	Netgate asume el patrocinio del proyecto.	Se profesionalizan recursos de desarrollo, pruebas, distribución y soporte.

Año	Hito	Por qué importa
2018	Netgate lanza TNSR.	El ecosistema de la empresa se amplía hacia otro enfoque de red de alto rendimiento.
2021	Aparece pfSense Plus y se consolida el nombre Community Edition.	Desde entonces hay que distinguir las dos líneas al documentar funciones y versiones.
2026	CE 2.9.0 y Plus 26.07 aparecen como versiones soportadas en la documentación consultada.	Este libro parte de un estado técnico contemporáneo, pero explica principios que sobreviven a las versiones.

En producción
La historia sirve para administrar mejor: explica por qué aparecen dos ediciones, por qué FreeBSD sigue siendo central y por qué determinadas decisiones de interfaz esconden componentes con décadas de evolución.

1.8 Qué debemos conservar de la historia

De esta cronología conviene conservar cinco ideas. Primera: pfSense no surgió como una distribución generalista, sino como un sistema de red especializado. Segunda: su herencia de m0n0wall explica la orientación a appliance y la gestión centralizada. Tercera: FreeBSD no es un detalle de implementación; condiciona drivers, red, herramientas y actualizaciones. Cuarta: Netgate es hoy una parte esencial del ecosistema, pero proyecto, producto, empresa y marca no son conceptos intercambiables. Quinta: CE y Plus obligan a documentar siempre sobre qué edición y versión se está hablando.

Con esa base podemos abandonar la cronología y pasar a la pregunta que realmente interesa a un administrador: ¿qué es pfSense cuando lo observamos como sistema?

Capítulo 2. Qué es pfSense cuando dejamos de verlo como una pantalla

Un firewall no es el menú “Firewall”. Un router no es la página “Routing”. pfSense es una plataforma donde varias funciones de red comparten sistema operativo, interfaces, tabla de rutas, reglas, estados, servicios y configuración.

2.1 Una distribución especializada de FreeBSD

Para entender pfSense conviene pensar menos en una simple distribución y más en un sistema de red especializado. FreeBSD aporta el núcleo, los controladores, la pila de red y las herramientas de sistema; pfSense añade la lógica de configuración y coordinación que convierte esas piezas en un firewall, un router y una plataforma de servicios administrable como una unidad. La WebGUI simplifica la operación, pero debajo siguen existiendo interfaces, procesos, rutas, sockets y mecanismos reales del sistema operativo.

Esto tiene consecuencias prácticas. Si una interfaz no es reconocida por FreeBSD, pfSense no puede inventar un controlador. Si la tabla de rutas contiene un camino inesperado, una regla de firewall correcta puede no producir el resultado esperado. Si un servicio no escucha en la dirección adecuada, abrir un puerto no lo hará aparecer. La interfaz web coordina, pero no sustituye las leyes básicas de TCP/IP.

2.2 Cinco funciones que conviven en el mismo equipo

Aunque en despliegues pequeños se hable de “el firewall”, un sistema pfSense puede desempeñar simultáneamente varias funciones. Entenderlas por separado ayuda a diagnosticar después sus interacciones.

- Firewall con seguimiento de estado: decide qué tráfico se permite y mantiene contexto de las conexiones.
- Router: reenvía paquetes entre redes y elige rutas y gateways.
- Traductor de direcciones: aplica NAT de origen, destino, 1:1 y redirecciones de puertos según el diseño.
- Concentrador VPN: puede terminar túneles de acceso remoto o entre sedes mediante varias tecnologías.
- Plataforma de servicios: DHCP, resolución DNS, NTP, monitorización, paquetes adicionales y otras funciones auxiliares.

En un diseño profesional no siempre conviene activar todas las funciones en todos los equipos. La posibilidad técnica no implica que la arquitectura deba concentrarlo todo. El libro distinguirá entre “pfSense puede hacerlo” y “es recomendable hacerlo aquí”.

2.3 El modelo por capas

Para razonar sobre pfSense utilizaremos un modelo de capas propio. No pretende sustituir al modelo OSI; es un mapa mental de administración que permite saber dónde buscar cuando algo falla.

Capa conceptual	Qué representa
1. Hardware	CPU, memoria, almacenamiento, NIC, puertos físicos, aceleración y plataforma.
2. FreeBSD	Kernel, drivers, pila de red, interfaces, procesos y utilidades base.
3. Motor de red y seguridad	PF, estados, NAT, routing, colas y mecanismos del sistema.
4. Servicios	DNS, DHCP, VPN, NTP, monitorización y paquetes instalados.
5. Orquestación pfSense	Configuración central, generación de reglas, scripts y lógica que mantiene coherencia.
6. WebGUI y consola	Superficies de administración desde las que el operador consulta y modifica el sistema.

Qué ocurre realmente

Cuando guardamos un cambio en la WebGUI no "se ejecuta una página web". La interfaz modifica la configuración que pfSense utiliza para regenerar o recargar componentes del sistema. Comprender qué componente se ha tocado es la diferencia entre administrar y simplemente hacer clic.

2.4 Stateful: el firewall recuerda

pfSense utiliza un enfoque de firewall con seguimiento de estado. Esto significa que no evalúa cada paquete como si fuera un acontecimiento aislado. Cuando una conexión permitida genera un estado válido, los paquetes posteriores relacionados con esa comunicación pueden procesarse utilizando esa información de contexto.

La tabla de estados es, por tanto, una pieza fundamental. Explica por qué una modificación de reglas no siempre afecta inmediatamente a conexiones ya establecidas, por qué algunos diagnósticos requieren limpiar estados y por qué el rendimiento de un firewall depende también del número de conexiones concurrentes y de cómo se gestionan.

Más adelante dedico un capítulo entero a estados, timeouts y comportamiento de PF. Por ahora basta con retener una regla mental: una política de firewall no es solo una lista de "permitir" y "bloquear"; es una máquina que clasifica tráfico y mantiene memoria operacional de las conversaciones que ha aceptado.

2.5 La configuración como activo

En un appliance de red, el valor no está solo en el binario instalado. Está en la configuración: interfaces, VLAN, reglas, objetos, certificados, usuarios, VPN, gateways y decisiones acumuladas. Perder el hardware es un incidente; perder una configuración no documentada puede convertirse en una reconstrucción completa de la red.

pfSense centraliza gran parte de su configuración en un fichero XML y proporciona mecanismos de copia y restauración. Esto permite tratar la configuración como un activo que debe respaldarse, versionarse de forma controlada y protegerse. En capítulos posteriores veremos estrategias para backups previos a cambios, recuperación y migraciones.

2.6 Lo que pfSense no es

Definir por exclusión evita expectativas incorrectas. pfSense no es un switch gestionable de capa 2, aunque pueda trabajar con bridges y VLAN. No es un punto de acceso Wi-Fi universal, aunque FreeBSD soporte determinados adaptadores inalámbricos. No es un EDR para endpoints. No sustituye una estrategia de seguridad. Tampoco convierte una red mal segmentada en segura por el mero hecho de instalarlo.

Su fortaleza aparece cuando se integra en un diseño coherente: interfaces bien delimitadas, direccionamiento claro, segmentación, reglas mínimas necesarias, servicios controlados, monitorización y procedimientos de cambio. En ese contexto pfSense puede convertirse en el punto donde política, conectividad y observabilidad se encuentran.

2.7 Escenarios donde encaja

- Hogar avanzado o laboratorio con varias redes, VPN y control de salida.
- Pyme con segmentación por departamentos, invitados, servidores e IoT.
- Sede corporativa con múltiples WAN, VPN entre centros y alta disponibilidad.
- Entorno virtualizado donde el firewall se ejecuta como máquina virtual con interfaces o VLAN dedicadas.
- Laboratorio de formación para aprender routing, NAT, VPN, reglas con estado y diagnóstico de tráfico.
- Nube o infraestructura híbrida cuando el modelo de despliegue y las imágenes disponibles lo permiten.

La misma interfaz puede aparecer en todos estos escenarios, pero los criterios de diseño no son los mismos. Por eso el libro no enseñará una única “configuración correcta”; enseñará a justificar configuraciones en función de requisitos y riesgos.

Capítulo 3. FreeBSD y PF: el suelo técnico sobre el que caminamos

Quien administra pfSense no necesita convertirse en administrador de FreeBSD, pero comprender la base evita diagnosticar a ciegas. El objetivo de este capítulo es conocer lo suficiente para interpretar interfaces, rutas, procesos, drivers y filtrado.

3.1 Por qué importa saber que no es Linux

En muchos centros de datos Linux es tan dominante que se utiliza la palabra como sinónimo informal de “sistema tipo Unix”. Con pfSense ese atajo conduce a errores. FreeBSD comparte numerosos conceptos con Linux, pero no es una distribución Linux: tiene su propio kernel, organización del sistema, herramientas, controladores, ciclo de desarrollo y decisiones de red.

Esto se nota especialmente en compatibilidad de hardware, nombres de interfaces, comandos de diagnóstico y disponibilidad de drivers. Una tarjeta Ethernet puede funcionar perfectamente en Windows o Linux y no estar igualmente soportada en la versión de FreeBSD utilizada por una versión concreta de pfSense. Antes de comprar hardware, el soporte del sistema importa más que el logotipo de la caja.

3.2 FreeBSD como plataforma de red

FreeBSD posee una larga tradición en redes y servidores. pfSense aprovecha esa base y la adapta a un propósito específico. El kernel gestiona interfaces, interrupciones, memoria, sockets y encaminamiento; los controladores hablan con el hardware; las utilidades permiten observar el sistema; y pfSense añade la capa de configuración que transforma esas piezas en un appliance.

La documentación oficial de pfSense explica que la elección histórica de FreeBSD estuvo influida por el origen en m0n0wall, la familiaridad del equipo, la disponibilidad de drivers y consideraciones de rendimiento de red. Estas razones pertenecen al contexto de 2004 y no deben interpretarse como una competición simple de “un sistema es siempre mejor que otro”. La decisión importante es que pfSense construyó su identidad técnica alrededor de FreeBSD y esa herencia continúa condicionando el producto.

3.3 PF: política, estados y traducción

PF es el componente de filtrado de paquetes alrededor del cual gira una parte esencial de pfSense. Un administrador interactúa con reglas de interfaz, floating rules, alias, NAT y estados; pfSense traduce esas decisiones a la lógica que necesita el motor subyacente.

En términos conceptuales, PF responde preguntas como: ¿puede este flujo entrar?, ¿debe traducirse una dirección?, ¿existe ya un estado que autoriza el tráfico?, ¿qué interfaz y dirección están implicadas?, ¿hay una regla especial que deba aplicarse antes que otras? La respuesta real depende de la configuración completa, no de una regla aislada vista en pantalla.

Por eso evito explicaciones simplistas como “la regla de arriba gana”. En pfSense existen categorías de reglas y momentos de procesamiento diferentes. El orden se analiza en los capítulos de firewall y NAT mediante trazas y ejemplos reproducibles.

3.4 Tabla de rutas: el mapa que existe antes del firewall

Una de las ideas más importantes de todo el libro es que filtrar y enrutar son tareas diferentes. El firewall puede permitir una comunicación que el sistema no sabe cómo entregar; también puede existir una ruta perfecta para un tráfico que una regla bloquea. Cuando una conexión falla hay que preguntar al menos dos cosas: “¿se permite?” y “¿existe un camino?”

La tabla de rutas describe destinos y siguientes saltos. Los gateways, rutas estáticas, redes directamente conectadas y algunas VPN modifican ese mapa. Más adelante estudiaremos policy routing, donde una regla puede influir en el gateway utilizado. Pero el principio base permanece: el firewall no reemplaza el routing.

3.5 Interfaces lógicas frente a puertos físicos

Otro concepto esencial es separar puerto físico de interfaz lógica. Un conector RJ45 puede transportar varias VLAN etiquetadas; una interfaz VLAN puede existir sin tener un conector exclusivo; una VM puede presentar interfaces virtuales; un LAGG puede agrupar varios enlaces; un bridge puede unir dominios de capa 2. En pfSense los nombres WAN y LAN son asignaciones funcionales, no tipos físicos especiales de puerto.

Esta abstracción será muy importante en Proxmox, VMware y entornos con switches gestionables. El mismo diseño lógico puede implementarse con cuatro NIC físicas o con una única NIC trunk y varias VLAN. El dibujo de red debe mostrar ambas cosas: qué redes existen y por qué enlaces físicos o virtuales viajan.

3.6 Servicios y procesos

DHCP, DNS, VPN y monitorización se implementan mediante servicios y procesos que escuchan en direcciones y puertos concretos. La WebGUI ofrece una forma homogénea de configurarlos, pero cada servicio conserva su propia lógica. Por eso, cuando una función falla, conviene dividir el problema: ¿el proceso está activo?, ¿escucha donde debe?, ¿hay ruta?, ¿el firewall permite llegar?, ¿la respuesta regresa por el camino correcto?

Esta forma de diagnóstico por capas es más lenta los primeros días y mucho más rápida a largo plazo. El objetivo del libro es que el lector termine pensando de esta manera de forma natural.

3.7 Herramientas que más adelante utilizaremos

Aunque la mayor parte de la administración puede hacerse desde la interfaz web, un profesional debe reconocer algunas herramientas de consola. No las estudiaremos aún en profundidad, pero conviene saber qué papel tendrán.

Herramienta	Uso conceptual
pfctl	Consultar reglas, estados, tablas y comportamiento de PF.

Herramienta	Uso conceptual
tcpdump	Observar paquetes en una interfaz y responder qué tráfico entra o sale realmente.
netstat / sockstat	Examinar rutas, conexiones y procesos que escuchan.
ifconfig	Consultar y entender interfaces del sistema.
ping / traceroute	Comprobar alcance IP y camino aproximado.
dig / drill	Investigar resolución DNS y separar un problema de nombres de uno de conectividad.

Error frecuente

Intentar arreglar desde las reglas de firewall un problema que en realidad es de DNS, routing, interfaz o servicio. La herramienta correcta depende de la capa donde esté el fallo.

Capítulo 4. Netgate, CE, Plus y el papel del hardware

pfSense puede estudiarse como software, pero el ecosistema actual incluye empresa, soporte, ediciones diferentes y appliances. Separar estos conceptos permite evaluar opciones sin convertir el capítulo en un catálogo comercial.

4.1 Netgate como actor del ecosistema

Netgate se presenta como una compañía de redes seguras orientada a appliances y software. Fue fundada en 2004 y asumió el patrocinio del proyecto pfSense en 2012. Desde entonces su papel abarca desarrollo, pruebas, distribución, documentación, soporte y diseño de hardware, además de otros productos como TNSR.

Para el lector esto significa que una parte considerable de la evolución de pfSense está vinculada a las decisiones de Netgate, especialmente en pfSense Plus y en los appliances oficiales. Sin embargo, el objetivo de este libro no es adoptar una perspectiva de fabricante, sino utilizar esa información para comprender compatibilidad, soporte, ciclos de actualización y opciones de despliegue.

4.2 Community Edition y Plus: cómo pensar la diferencia

La comparación entre CE y Plus cambia con el tiempo y no debe reducirse a una tabla eterna de funciones. Conviene utilizar criterios más estables: modelo de distribución, relación con hardware oficial, soporte, cadencia de versiones, características exclusivas y dependencia de las decisiones comerciales del fabricante.

Cuando una función del libro exista en ambas ediciones, se explicará de forma común. Cuando haya diferencias relevantes se marcarán explícitamente. Así evito duplicar capítulos y ayudo a evitar que se apliquen instrucciones de una edición a otra sin comprobar compatibilidad.

Convención de lectura
En los capítulos prácticos se indicará “CE”, “Plus” o “ambas” cuando la diferencia sea importante. Si una pantalla o función puede variar por versión, se explicará el concepto primero y la interfaz después.

4.3 El appliance oficial frente al hardware propio

Una de las fortalezas históricas de pfSense es que puede desplegarse en hardware compatible propio. Esto abre muchas posibilidades: reutilizar un servidor, instalarlo en un mini-PC, ejecutarlo como máquina virtual o construir una plataforma con NIC específicas. A cambio, el administrador asume la responsabilidad de validar compatibilidad, rendimiento y calidad del conjunto.

Un appliance oficial reduce parte de esa incertidumbre porque hardware, software y soporte se ofrecen como una solución integrada. Pero no elimina la necesidad de dimensionar. Dos equipos con puertos de igual velocidad pueden comportarse de forma muy diferente cuando intervienen

paquetes por segundo, VPN, IDS/IPS, múltiples interfaces, número de estados o almacenamiento para logs.

Por eso el capítulo de hardware no utilizará únicamente “Gb/s” como métrica. Estudiaremos CPU, arquitectura, número y calidad de NIC, colas, aceleración criptográfica, RAM, almacenamiento, disipación, redundancia y patrón de tráfico. El ancho de banda anunciado por un proveedor de Internet es solo una de las variables.

4.4 Por qué las NIC importan tanto

La tarjeta de red es una de las piezas más críticas de un firewall. Todo paquete que atraviesa el equipo entra por una interfaz y, salvo tráfico dirigido al propio firewall, normalmente sale por otra. Drivers deficientes, offloading problemático, colas mal utilizadas o hardware de baja calidad pueden generar síntomas que parecen errores de reglas o de ISP.

En hardware propio recomiendo elegir controladores bien soportados por FreeBSD y no confiar solo en el argumento de que “el chipset funciona en Linux”.
También estudiaremos cuándo tiene sentido 2.5/5/10 GbE, SFP/SFP+, interfaces dedicadas y trunks VLAN.

4.5 CPU, cifrado y trabajo por paquete

El rendimiento de un firewall depende de cuánto trabajo realiza con cada paquete. En routing simple la carga puede ser relativamente baja; al añadir cifrado VPN, inspección IDS/IPS, shaping o paquetes adicionales aumenta el procesamiento. También importa el tamaño de los paquetes: mover 1 Gbit/s con paquetes grandes no exige el mismo número de decisiones por segundo que mover el mismo caudal con paquetes pequeños.

Esta idea explica por qué las pruebas de rendimiento deben leerse con contexto. Un número máximo de throughput no responde por sí solo a preguntas como “¿qué ocurrirá con IPsec?”, “¿cuántos usuarios concurrentes?”, “¿con Suricata activo?” o “¿cuál es la latencia bajo carga?”. En el bloque de rendimiento construiremos una metodología de pruebas reproducible.

4.6 Hardware físico y virtualización

pfSense también puede ejecutarse como máquina virtual. Esto aporta snapshots del hipervisor, movilidad, consolidación y flexibilidad, pero introduce una capa adicional que debe diseñarse correctamente. Un bridge virtual mal configurado, una VLAN entregada al puerto equivocado o una ruta de gestión dependiente del propio firewall pueden convertir un cambio menor en pérdida total de acceso.

En el capítulo de Proxmox incluyo un laboratorio para separar red de gestión, WAN, LAN y trunks, comparando virtio con passthrough cuando proceda. El objetivo no será demostrar que “virtual es mejor” o “físico es mejor”, sino aprender a elegir según riesgo, rendimiento, recuperación y operación.

4.7 TNSR no es “pfSense rápido”

Netgate también desarrolla TNSR, un producto distinto orientado a redes de alto rendimiento y basado en una arquitectura diferente. Es importante mencionarlo porque aparece en el mismo ecosistema empresarial, pero no debe confundirse con una edición avanzada de pfSense. Que dos productos compartan fabricante no significa que compartan arquitectura o modelo de administración.

En este libro TNSR aparecerá solo como contexto cuando ayude a comprender decisiones de mercado o límites de alcance. El objeto de estudio sigue siendo pfSense.

Capítulo 5. El viaje de un paquete: el mapa mental para todo el libro

Antes de aprender menús, vamos a seguir un paquete imaginario. Esta secuencia no pretende describir todos los detalles internos de PF; pretende ofrecer un mapa que luego refinaremos con reglas, estados, NAT, routing y captura de tráfico.

5.1 Escenario base

Imaginemos un PC con dirección 192.168.10.50/24 en una red LAN. Su gateway es 192.168.10.1, una interfaz de pfSense. El usuario abre una página HTTPS en Internet. Para simplificar, suponemos que el nombre ya se ha resuelto a una dirección IP y que la WAN del firewall tiene conectividad con el proveedor.

Escenario

PC 192.168.10.50 → switch → LAN de pfSense 192.168.10.1 → firewall / estados / NAT / routing → WAN → ISP → servidor HTTPS

5.2 Paso 1: el equipo decide si el destino es local

El PC compara la IP destino con su propia red. Como el servidor está fuera de 192.168.10.0/24, no intenta enviárselo directamente. Construye una trama dirigida a la MAC de su gateway. Si no conoce esa MAC, utiliza ARP para averiguarla. Ya aparece la primera lección: antes de pfSense pueden fallar cosas. Un problema de VLAN, switch o ARP puede impedir que el paquete llegue siquiera al firewall.

5.3 Paso 2: el paquete entra por una interfaz

La interfaz LAN recibe el tráfico. Para el sistema no es una idea abstracta: hay un dispositivo lógico asociado a un driver, con direcciones y estado. Si el enlace está caído, la VLAN no coincide o el tráfico llega por otra interfaz, la política que esperábamos aplicar puede no ser la que intervenga.

5.4 Paso 3: reglas y estado

El tráfico debe cumplir la política de firewall correspondiente. Si una regla permite iniciar esa comunicación, PF puede crear un estado. Ese estado contiene información que permite reconocer los paquetes posteriores pertenecientes a la conversación. La tabla de estados se convierte así en una memoria temporal del firewall.

Cuando estudiemos reglas veremos dirección, protocolo, origen, destino, puertos, opciones avanzadas, gateways y logging. Por ahora basta con una pregunta: “¿esta nueva conversación puede nacer?”. Si la respuesta es no, el viaje termina aquí.

5.5 Paso 4: NAT cuando es necesario

En la salida típica a Internet desde una red privada, la dirección 192.168.10.50 no puede utilizarse directamente como origen global. pfSense aplica una traducción de origen según la política de outbound NAT. El servidor remoto verá una dirección correspondiente a la salida del firewall, no la IP privada del PC.

El firewall debe recordar cómo deshacer esa traducción cuando llegue la respuesta. Por eso NAT y estados están estrechamente relacionados. Este mecanismo suele funcionar de manera transparente, pero se vuelve crítico en conexiones entrantes, multi-WAN, VPN y diseños con redes solapadas.

5.6 Paso 5: routing y gateway

Después de decidir que el tráfico puede pasar y cómo debe traducirse, el sistema necesita una ruta hacia el destino. En el caso simple utiliza la ruta por defecto hacia el gateway del ISP. En escenarios más complejos una regla puede seleccionar otro gateway, una VPN puede aportar una ruta, o el destino puede estar detrás de una interfaz interna.

Este es el punto donde muchos diagnósticos se confunden. Una regla “allow” no crea automáticamente una ruta. Del mismo modo, una ruta válida no autoriza por sí misma el tráfico. Política y camino deben coincidir.

5.7 Paso 6: salida por WAN y viaje de retorno

El paquete sale por la WAN y continúa por el proveedor hasta el servidor. La respuesta recorre Internet en sentido inverso y alcanza la dirección pública utilizada. pfSense identifica el estado existente, revierte la traducción necesaria y entrega el tráfico al host original.

Si todo funciona, el usuario solo ve que la página carga. El administrador, en cambio, debe ser capaz de descomponer el proceso: resolución de nombres, capa 2, entrada por interfaz, política, estado, NAT, ruta, salida, retorno y entrega. Esta será nuestra metodología de diagnóstico.

5.8 El mismo viaje, convertido en preguntas

1. ¿El cliente tiene IP, máscara, gateway y DNS correctos?
2. ¿Llega el paquete a la interfaz esperada de pfSense?
3. ¿Existe una regla que permita iniciar la conversación?
4. ¿Se crea o existe el estado correspondiente?
5. ¿Hay una traducción NAT y es la adecuada?
6. ¿Qué ruta y gateway se eligen?
7. ¿El paquete sale realmente por la interfaz de salida?
8. ¿La respuesta vuelve al firewall?
9. ¿La respuesta coincide con el estado y se entrega al cliente?
10. Si se usa un nombre, ¿el problema es realmente de DNS y no de conectividad?

5.9 Una primera práctica sin tocar pfSense

Antes de instalar nada, dibuja una red sencilla con un firewall, una LAN, una WAN y un servidor en Internet. Marca dónde habría una dirección privada, dónde aparecería NAT, qué dispositivo funciona como gateway y en qué punto se tomaría una decisión de firewall. Después añade una VLAN de invitados. El objetivo no es configurar; es aprender a separar conceptos.

Laboratorio mental 1

Si un cliente puede hacer ping a 8.8.8.8 pero no abrir www.example.com, no empieces cambiando reglas. La conectividad IP ya está demostrando algo importante; investiga primero la resolución DNS. Esta forma de descartar capas será una constante del libro.

5.10 Cierre de la Parte I

Ya tenemos el vocabulario mínimo para empezar a construir. Sabemos de dónde viene pfSense, por qué FreeBSD importa, qué lugar ocupa PF, cómo encaja Netgate, por qué existen CE y Plus y qué recorrido conceptual realiza un paquete. La siguiente parte comenzará con hardware, diseño de interfaces y preparación de una instalación real.

A partir de aquí el libro será cada vez más práctico, pero mantendremos esta regla: cada pantalla debe responder a una idea técnica. Si sabemos qué queremos que ocurra con un paquete, la interfaz deja de ser un conjunto de casillas y se convierte en una herramienta para expresar una política de red.

Glosario esencial de la Parte I

Término	Definición de trabajo
Appliance	Equipo concebido para realizar una función especializada y administrarse como una unidad.
CE	Community Edition, línea comunitaria de pfSense.
Estado	Registro temporal que permite al firewall reconocer tráfico perteneciente a una comunicación.
FreeBSD	Sistema operativo de la familia BSD sobre el que se construye pfSense.
Gateway	Siguiente salto utilizado para alcanzar redes no directamente conectadas.
NAT	Traducción de direcciones y, según el caso, puertos entre espacios de direccionamiento.
Netgate	Empresa estrechamente vinculada al desarrollo, distribución, soporte y hardware de pfSense.
PF	Packet Filter, tecnología de filtrado que constituye una pieza central de pfSense.
pfSense Plus	Línea comercial de pfSense mantenida por Netgate.
Routing	Proceso de seleccionar el camino que debe seguir un paquete para alcanzar su destino.
Stateful firewall	Firewall que mantiene contexto de las comunicaciones mediante estados.
VLAN	Red lógica de capa 2 identificada mediante etiquetado 802.1Q u otros mecanismos de segmentación.
WebGUI	Interfaz web de administración de pfSense.

Fuentes técnicas consultadas para contraste

Las siguientes fuentes se han utilizado para verificar fechas, terminología, versiones y contexto técnico. El contenido de esta Parte I está redactado y estructurado de forma original y no reproduce el orden de estas fuentes.

1. Netgate Documentation — “Introduction / Project Inception”, docs.netgate.com/pfsense/en/latest/general/index.html (consulta: 8 de octubre de 2026).

2. Netgate Documentation — “Why FreeBSD?”, docs.netgate.com/pfsense/en/latest/general/why-freebsd.html (consulta: 8 de octubre de 2026).

3. Netgate Documentation — “What does pfSense stand for/mean?”, docs.netgate.com/pfsense/en/latest/general/what-is-pfsense.html (consulta: 8 de octubre de 2026).

4. Netgate Documentation — “What is pfSense Plus Software?”, docs.netgate.com/pfsense/en/latest/general/plus.html (consulta: 8 de octubre de 2026).

5. Netgate Documentation — “Versions of pfSense software and FreeBSD”, docs.netgate.com/pfsense/en/latest/releases/versions.html (consulta: 8 de octubre de 2026).

6. Netgate — “About Us / Our Story”, netgate.com/about-us (consulta: 8 de octubre de 2026).

7. Netgate — “pfSense Software’s Sweet 16”, 13 de octubre de 2022, netgate.com/blog/pfsense-softwares-sweet-16.

8. FreeBSD Documentation Portal — FreeBSD Architecture Handbook, docs.freebsd.org/en/books/arch-handbook/ (consulta: 8 de octubre de 2026).

pfSense® software

REDES, FIREWALL Y SEGURIDAD

Arquitectura, administración y laboratorios prácticos

PARTE II

Hardware, interfaces y diseño previo a la instalación

Oscar de la Cuesta

palentino.es



Primera edición · octubre de 2026

Punto de partida de esta parte

La Parte I construyó el vocabulario y el modelo mental: pfSense como plataforma de red sobre FreeBSD, PF como motor de filtrado y el recorrido conceptual de un paquete. Esta Parte II cambia la pregunta. Ya no preguntamos solo qué hace el firewall, sino qué máquina, qué interfaces y qué topología necesita para hacerlo de forma estable, mantenible y segura.

El objetivo no es convertir la compra de hardware en una tabla de especificaciones. Un firewall se dimensiona por carga, funciones, interfaces, paquetes por segundo, cifrado, número de estados, crecimiento, tolerancia a fallos y facilidad de recuperación. La misma conexión de 1 Gb/s puede exigir equipos muy distintos según el tráfico sea una copia grande, miles de conexiones pequeñas, inspección IDS/IPS o túneles VPN cifrados.

La documentación oficial de pfSense, FreeBSD y las fichas comerciales de Netgate se han utilizado únicamente para contrastar compatibilidad, requisitos y hechos que pueden cambiar. La estructura, los ejemplos, las conclusiones, las tablas y la explicación son propios de este libro.

Regla de diseño de esta Parte II
Primero se diseña la red y se define la carga. Después se elige el hardware. Comprar un equipo y forzar la arquitectura a sus puertos disponibles invierte el orden correcto del problema.

Qué aprenderemos en esta parte

- Dimensionar CPU, memoria, almacenamiento y interfaces a partir de escenarios reales.
- Distinguir rendimiento en bits por segundo de rendimiento en paquetes por segundo.
- Elegir NIC y entender por qué el driver y el chipset importan tanto como la velocidad impresa en el puerto.
- Interpretar nombres de interfaces como em, igb, igc, ix o vtnet sin memorizarlos como si fueran marcas comerciales.
- Decidir entre appliance dedicado, hardware genérico y máquina virtual.
- Diseñar WAN, LAN, redes de gestión, servidores, IoT, invitados y DMZ antes de instalar.
- Preparar VLAN, trunks, switches administrables y crecimiento futuro sin depender de una única topología.
- Llegar a la instalación con un documento de arquitectura y una lista de comprobación, no con decisiones improvisadas.

Capítulo 6. Dimensionar antes de comprar

La pregunta “¿qué ordenador necesito para pfSense?” parece sencilla, pero suele estar mal formulada. El firewall no consume recursos por existir; los consume al procesar tráfico y ejecutar funciones. Por eso la pregunta útil es: “¿qué tendrá que procesar esta máquina, con qué margen y durante cuánto tiempo?”.

6.1 El mínimo técnico no es el objetivo de diseño

La documentación actual establece para hardware genérico una base mínima de CPU amd64 de 64 bits, 1 GB de RAM, al menos 8 GB de almacenamiento y una o más interfaces de red compatibles. Esos valores indican que el sistema puede instalarse y arrancar; no describen un dimensionamiento sensato para cualquier entorno.

Un laboratorio doméstico que enruta unos pocos cientos de megabits y una empresa con varias VLAN, cientos de usuarios, túneles IPsec, Suricata y múltiples WAN pueden ejecutar el mismo software, pero no tienen la misma carga. El error consiste en convertir un “mínimo de arranque” en una recomendación de producción.

Idea clave
Un firewall no se dimensiona por el número de menús que utilizaremos, sino por el trabajo que hará por paquete, por flujo y por servicio. Las funciones activadas multiplican la carga de formas diferentes.

6.2 Cinco variables para dimensionar

Variable	Pregunta que debemos responder	Qué componente presiona más
Caudal	¿Cuántos Mbit/s o Gbit/s deben atravesar el firewall?	CPU, bus, NIC
PPS	¿Cuántos paquetes por segundo aparecen en los picos?	CPU, NIC, colas, kernel
Estados	¿Cuántas conexiones simultáneas debe mantener PF?	RAM y estructuras del kernel
Cifrado	¿Qué volumen de VPN, TLS o IPsec debe procesarse?	CPU y aceleración criptográfica
Servicios	¿Habrá IDS/IPS, DNSBL, proxy, monitorización o paquetes adicionales?	CPU, RAM y almacenamiento

Estas variables deben estudiarse juntas. Dos redes con 1 Gb/s de acceso a Internet pueden comportarse de forma opuesta: una puede transferir archivos grandes en pocas sesiones; otra puede generar decenas de miles de conexiones cortas con paquetes pequeños. En la segunda, los paquetes por segundo y la creación de estados pueden ser más exigentes aunque el caudal total sea menor.

6.3 Mbps, Gbps y PPS no cuentan la misma historia

El ancho de banda expresa volumen de bits por unidad de tiempo. Los paquetes por segundo expresan cuántas unidades debe recibir, clasificar, filtrar, enrutar, traducir y transmitir el sistema. Cada paquete implica trabajo fijo: interrupciones o colas, búsqueda de rutas, evaluación de estados y reglas, posibles transformaciones y entrega a una interfaz de salida.

Por eso los paquetes pequeños son una prueba especialmente dura. A igual caudal, cuanto menor es el paquete, mayor es el número de paquetes por segundo y mayor es el trabajo administrativo del firewall. Esta es una de las razones por las que un resultado de iperf con tramas grandes no debe interpretarse como garantía universal de rendimiento.

Qué ocurre realmente
Si un equipo mueve 1 Gb/s con paquetes grandes, no significa automáticamente que sostenga 1 Gb/s con tráfico formado por paquetes pequeños, miles de flujos y servicios de inspección. El puerto de 1 GbE es solo una de las piezas del camino.

6.4 CPU: frecuencia, núcleos e instrucciones

La CPU participa en prácticamente todo el recorrido de un paquete. No basta con contar núcleos. La frecuencia por núcleo, la arquitectura, la caché, el rendimiento por ciclo y las instrucciones disponibles pueden ser decisivos. Algunos trabajos se paralelizan bien; otros dependen en mayor medida de uno o pocos hilos.

Para routing y filtrado simples, una CPU moderna modesta puede mover gran cantidad de tráfico. Al añadir VPN, IDS/IPS, múltiples colas, reglas complejas o paquetes adicionales, el margen desaparece con rapidez. Es preferible diseñar con reserva suficiente para que un pico, una actualización o un nuevo servicio no conviertan el firewall en cuello de botella.

En cifrado, las extensiones de la CPU importan especialmente. Las instrucciones AES-NI están presentes en muchos procesadores modernos y aceleran determinados algoritmos. En pfSense Plus existen además mecanismos de aceleración que pueden aprovechar otros conjuntos SIMD y, en determinados equipos, dispositivos QAT. El principio práctico es sencillo: si la VPN es crítica, hay que dimensionar para el cifrado elegido, no solo para el ancho de banda de la WAN.

6.5 RAM: estados, servicios y ZFS

La memoria no debe dimensionarse únicamente pensando en el sistema base. PF mantiene estados, los servicios conservan cachés y tablas, y paquetes como Suricata o Snort pueden necesitar cantidades significativas de memoria según reglas y configuración. Un entorno con miles de estados y varios servicios debe tener margen para crecer sin entrar en presión de memoria.

En instalaciones con ZFS, parte de la RAM puede utilizarse como ARC, la caché adaptativa del sistema de archivos. Ver poca memoria "libre" no significa necesariamente que exista un problema: FreeBSD intenta aprovechar RAM para caché y puede liberarla cuando otros procesos la necesitan. La señal preocupante no es un porcentaje de memoria libre aislado, sino fallos de asignación, swap sostenido, procesos terminados o presión real durante picos.

Error frecuente
Interpretar "RAM libre baja" como avería y aplicar tunables sin comprender el motivo. En sistemas BSD, memoria empleada en caché puede ser memoria útil, no memoria perdida.

6.6 Almacenamiento: más importante por fiabilidad que por capacidad

Un firewall típico no necesita grandes terabytes. Lo importante es que el medio sea fiable, tenga vida útil adecuada y permita recuperar el sistema con rapidez. Logs, paquetes, actualizaciones, bases de datos auxiliares y escrituras periódicas convierten un almacenamiento de mala calidad en un punto de fallo evitable.

Un SSD de calidad suele ser preferible a memorias USB o medios flash de consumo para una instalación permanente. Si el equipo admite varios discos y la continuidad lo justifica, ZFS puede utilizar espejos. Pero la redundancia de discos no sustituye al backup de configuración: protege frente al fallo de una unidad, no frente a una mala regla, una corrupción lógica, un error administrativo o la pérdida completa del equipo.

6.7 NIC: la pieza subestimada

La interfaz de red no es un mero conector. Incluye chipset, firmware, colas, buffers, capacidades de offload y un driver dentro de FreeBSD. Una NIC con buen soporte puede descargar trabajo de la CPU y comportarse de forma predecible bajo carga. Una implementación deficiente puede introducir pérdidas, bloqueos, errores con VLAN o un consumo de CPU desproporcionado.

La documentación de pfSense recomienda generalmente NIC Intel para hardware genérico por la calidad de sus drivers en FreeBSD y desaconseja los adaptadores Ethernet USB para un firewall de producción. Esto no significa que cualquier otra marca sea inutilizable; significa que la compatibilidad y la calidad deben verificarse por chipset y driver, no por el logotipo de la caja.

6.8 Tabla de dimensionamiento por escenario

Escenario	Prioridad	Margen recomendado de diseño
Laboratorio / aprendizaje	Compatibilidad y flexibilidad	2+ NIC o VLAN; recursos suficientes para snapshots si es virtual; no optimizar al límite.
Hogar avanzado	Bajo consumo, estabilidad, VPN ocasional	Reservar capacidad para reglas, DNS y una VPN sin saturar CPU.
Pyme	Fiabilidad, varias VLAN, VPN, monitorización	CPU moderna, RAM holgada, NIC de calidad, almacenamiento fiable y fuente estable.
Sede con VPN intensa	Cifrado y latencia	Priorizar CPU con aceleración criptográfica y medir el algoritmo real.
IDS/IPS	CPU, RAM, NIC	Dimensionar reglas, tráfico inspeccionado y crecimiento; evitar mínimos.
Multi-Gigabit	PPS, buses, NIC, CPU	Verificar 2.5/5/10 GbE extremo a extremo y medir con mezcla real de tráfico.

6.9 Capacidad de crecimiento

Un firewall bien dimensionado debe poder absorber el crecimiento razonable de la red. Si hoy existen tres VLAN y se prevé añadir voz, cámaras, IoT o una segunda sede, esa evolución debe influir en puertos, memoria, CPU y estrategia de switching. El objetivo no es sobredimensionar sin límite, sino evitar que una ampliación previsible obligue a sustituir el equipo completo.

En producción
Documenta el pico normal y el pico extraordinario. Un firewall que trabaja al 80-90 % de CPU en condiciones habituales no tiene reserva para un ataque, una copia masiva, una nueva VPN o una tarea de mantenimiento.

Capítulo 7. Anatomía del hardware de un firewall

Para administrar bien un firewall conviene poder mirarlo como un sistema físico. Los menús ocultan los detalles, pero los fallos no: una NIC con problemas, un SSD agotado, una fuente inestable o una temperatura excesiva pueden producir síntomas que parecen “de pfSense” y en realidad nacen mucho más abajo.

7.1 Del puerto RJ45 al kernel

Cuando un frame Ethernet entra por un puerto, no aparece mágicamente en PF. La señal física llega al transceptor, el controlador de red la recibe, utiliza buffers y colas, notifica al sistema y el driver de FreeBSD entrega los datos a la pila de red. A partir de ahí intervienen VLAN, routing, filtrado, estados, NAT y los servicios configurados.

Este recorrido explica por qué un fallo de driver puede parecer una regla incorrecta, por qué una cola saturada puede manifestarse como pérdida de paquetes y por qué el tipo de interfaz virtual elegido en un hipervisor puede cambiar notablemente el rendimiento.

7.2 Los bloques físicos que debemos reconocer

Bloque	Función	Qué observar
CPU / SoC	Ejecuta kernel, PF, routing, cifrado y servicios	Arquitectura, frecuencia, núcleos, AES/SIMD, temperatura
RAM	Estados, procesos, buffers, cachés	Capacidad, presión, margen para paquetes y ZFS
NIC	Entrada/salida de frames	Chipset, driver, colas, offload, VLAN, velocidad
Almacenamiento	Sistema, configuración, logs, paquetes	Fiabilidad, SMART, capacidad, redundancia si aplica
Bus / PCIe	Comunica CPU con NIC y almacenamiento	Ancho de banda y reparto de líneas en equipos multi-Gigabit
Consola	Acceso cuando la red falla	VGA, serie, USB-serie, IPMI/BMC según plataforma
Fuente	Alimenta todo el equipo	Calidad, redundancia, UPS, consumo
Refrigeración	Mantiene estabilidad térmica	Flujo de aire, polvo, ventiladores, temperatura ambiente

7.3 Consola: el salvavidas que se olvida hasta que hace falta

Si una regla bloquea el acceso a la WebGUI, se asigna una interfaz equivocada o la LAN pierde su dirección, la administración por red puede desaparecer. La consola local o serie permite recuperar el control sin depender de la propia configuración que estamos reparando. En entornos remotos, disponer de IPMI/BMC o de una consola fuera de banda puede reducir enormemente el tiempo de recuperación.

Seguridad y operación
La consola de administración también es una superficie de seguridad. Un puerto serie accesible, una interfaz BMC expuesta o credenciales por defecto pueden convertirse en una ruta alternativa hacia el equipo.

7.4 ARM, amd64 y la diferencia entre compatibilidad y disponibilidad

Para hardware genérico, pfSense se orienta a sistemas amd64 de 64 bits. Existen appliances Netgate basados en ARM compatibles con pfSense Plus, pero eso no significa que cualquier placa ARM pueda ejecutar pfSense. El soporte depende de plataforma, bootloader, kernel, drivers y distribución de imágenes, no solo de que la CPU pertenezca a una familia conocida.

Esta es una distinción útil para evitar el clásico razonamiento “si FreeBSD funciona en esta placa, pfSense también debería funcionar”. La compatibilidad del sistema operativo base no garantiza que exista una imagen de pfSense diseñada y soportada para esa plataforma concreta.

7.5 Appliances Netgate como referencia de categorías

Netgate comercializa appliances con pfSense Plus que abarcan desde equipos compactos de borde hasta plataformas de rack. Aquí no se presentan como catálogo ni como guía de compra, sino como referencia para comprender que una misma plataforma puede desplegarse en escalas muy diferentes.

Familia observada (oct. 2026)	Lectura didáctica	Entorno típico que representa
1100 / 2100	Appliance compacto, bajo consumo, pocos puertos	Hogar avanzado, microempresa, oficina pequeña
4200	Escalón intermedio con mayor margen	Pyme, sucursal, redes segmentadas
6100	Más interfaces y capacidad	Pyme exigente, sede, multi-WAN / VPN
8200	Plataforma de rack de mayor capacidad	Sede principal, servicios intensivos
8300	Gama alta / datacenter y agregación	Entornos con caudal, interfaces y servicios elevados

La disponibilidad comercial cambia y no debe formar parte rígida del diseño. Un lector que consulte este libro años después debe conservar el método: clasificar el entorno por carga y necesidades, y después buscar el appliance o hardware que encaje en esa clase.

7.5.1. Familias Netgate y evolución reciente

A octubre de 2026, la gama pfSense Plus de Netgate se organiza desde equipos compactos de sobremesa hasta appliances de rack. El interés didáctico no está en memorizar precios o cifras de rendimiento —cambian con el tiempo—, sino en observar cómo varían formato, arquitectura, conectividad, almacenamiento y redundancia conforme aumenta la criticidad del entorno.

Appliances Netgate

Seis escalones de hardware para pfSense Plus

Comparativa didáctica · Arquitectura, conectividad y formato · Octubre de 2026

Netgate 1100

Entrada · ARM



CPU ARM Cortex-A53 · 2 × 1,2 GHz
RAM / disco 1 GB DDR4 · 10,6 GB eMMC
Puertos 3 × 1 GbE, switch integrado
Perfil Hogar y oficina pequeña

Netgate 2100 MAX

Sucursal · ARM



CPU ARM Cortex-A53 · 2 × 1,2 GHz
RAM / disco 4 GB DDR4 · SSD SATA 128 GB (MAX)
Puertos 1 × 1 GbE combo + 4 × 1 GbE LAN
Perfil Oficina, sucursal pequeña

Netgate 4200

Sobremesa · pyme



CPU Intel Atom C1110 · 4 × 2,1 GHz
RAM / disco 4 GB LPDDR5 · SSD NVMe 128 GB
Puertos 4 × 2,5 GbE independientes
Perfil Pyme y segmentación de redes

Netgate 6100

Sobremesa · multi-gigabit



CPU Intel Atom C3558 · 4 × 2,2 GHz
RAM / disco 8 GB DDR4 · eMMC/SSD según versión
Puertos 2 × 10G SFP+ · 2 × 1G combo · 4 × 2,5G
Perfil Sedes exigentes, VPN y multi-WAN

Netgate 8200

Rack 1U · alto caudal



CPU Intel Atom C3758R · 8 × 2,4 GHz
RAM / disco 16 GB DDR4 · SSD NVMe 128 GB
Puertos 2 × 10G SFP+ · 2 × 1G combo · 4 × 2,5G
Perfil Sede central · rack · ventilación activa

Netgate 8300 MAX

Rack 1U · gama alta



CPU Intel Xeon D-1733NT · 8 × 2,0 GHz
RAM / disco 32 GB ECC DDR4 · SSD NVMe 512 GB
Puertos 4 × 10G SFP+ · 4 × 1G SFP · 3 × 2,5G
Perfil Datacenter · PSU extraíbles (2 MAX)

Cómo interpretar la figura

Los puertos no equivalen al caudal real: valorar carga, VPN, IDS/IPS, número de estados y redundancia.
1100: tres puertos con switch. 2100: cuatro LAN conmutadas y WAN independiente (combo RJ45/SFP).

Ilustraciones originales orientativas: apariencia y posición de conectores no son planos ni fotos oficiales.
Especificaciones contrastadas en fichas de Netgate (cada tarjeta enlaza a su fuente). La disponibilidad cambia.

Familia	Formato orientativo	Lectura técnica
1100	Compacto / entrada	Referencia para hogar, laboratorio y pequeña oficina con necesidades moderadas.
2100	Compacto / sucursal	Más margen de memoria y conectividad para sede pequeña y servicios adicionales.
4200	Sobremesa / pyme	Escalón intermedio para redes con más caudal, VPN y segmentación.
6100	Sobremesa de altas prestaciones	Mayor densidad y opciones de red para sedes exigentes y enlaces rápidos.
8200	Rack	Orientado a centro de datos, sede central y escenarios donde formato y capacidad de expansión importan.
8300	Rack de gama alta	Escala superior, pensada para cargas empresariales y mayor exigencia de interfaces y rendimiento.

La evolución de producto también ayuda a leer la historia del hardware: la documentación de ciclo de vida de Netgate sitúa, entre otros relevos, al 4200 como sustituto del 4100, al 6100 como sucesor de familias como 5100 y 7100 DT, al 8200 como relevo del 7100 1U y al 8300 como sustituto de las plataformas 1537/1541. El mensaje útil es que el hardware cambia más deprisa que los criterios de dimensionamiento; por eso este libro prioriza arquitectura y carga frente a modelos concretos.

7.6 Hardware genérico: libertad a cambio de responsabilidad

Un equipo x86-64 estándar ofrece gran libertad: podemos elegir chasis, CPU, RAM, SSD, NIC, fuente y formato. Esa libertad puede reducir costes o permitir configuraciones muy específicas, pero traslada al administrador la responsabilidad de validar drivers, BIOS/UEFI, consumo, temperaturas, actualizaciones de firmware y comportamiento bajo carga.

En un entorno profesional, el precio de compra no es el único coste. También cuentan las horas de diagnóstico, disponibilidad de repuestos, garantía, tiempo para reinstalar, documentación y soporte. Un mini-PC barato puede ser excelente en un laboratorio y una mala elección para una sede donde una hora de caída cuesta más que la diferencia de precio con un appliance validado.

7.7 Fuente, UPS y continuidad

El firewall se sitúa en una posición crítica: si se apaga, la red puede quedar aislada incluso aunque switches, servidores y almacenamiento sigan funcionando. Por ello debe formar parte del diseño eléctrico de la infraestructura. Una UPS adecuada, protección contra sobretensiones y una política de apagado controlado son componentes de red tanto como una VLAN.

En equipos de rack, las fuentes redundantes permiten sobrevivir al fallo de una PSU o a la pérdida de una línea eléctrica si cada fuente está conectada a un circuito o PDU distinto. En equipos compactos, la redundancia puede trasladarse a la estrategia de disponer de un segundo firewall preparado o de un repuesto compatible.

7.8 Temperatura, polvo y mantenimiento físico

Los firewalls suelen instalarse y olvidarse en armarios de comunicaciones. Esa estabilidad aparente puede ocultar ventiladores saturados de polvo, temperaturas crecientes y fuentes envejecidas. El mantenimiento preventivo debe incluir inspección, limpieza, revisión de SMART, temperatura y estado de ventiladores cuando el hardware lo permita.

En producción
Una caída térmica o eléctrica no se diagnostica mirando solo las reglas. Mantén inventario del modelo, números de serie, tipo de fuente, almacenamiento, NIC y método de consola. Esa ficha puede ser decisiva cuando el equipo no arranca.

Capítulo 8. Interfaces: de un puerto físico a una zona de seguridad

Una interfaz no es simplemente “el agujero donde conecto un cable”. En pfSense, las interfaces son puntos de entrada y salida a los que asignamos identidad lógica, direccionamiento y política. Entender esa separación evita confundir un puerto físico con el papel que desempeña.

8.1 Puerto, NIC, interfaz y rol lógico

Término	Ejemplo	Qué significa
Puerto físico	RJ45 2.5 GbE nº 1	Conector visible en el equipo
NIC / controlador	Intel i226, controlador integrado	Hardware que transmite y recibe
Interfaz del sistema	igc0, igb1, em0, ix0	Nombre que FreeBSD asigna al driver/dispositivo
Interfaz virtual	vtnet0, VLAN sobre igc1, LAGG	Interfaz creada por virtualización o lógica de red
Rol pfSense	WAN, LAN, SERVIDORES, INVITADOS	Nombre funcional que el administrador asigna

Es perfectamente posible que el puerto etiquetado físicamente como “LAN” no termine siendo LAN después de una reinstalación o un cambio de hardware. Lo que importa es la correspondencia documentada entre conector, interfaz del sistema y rol lógico.

8.2 Por qué aparecen nombres como em0, igb0, igc0 o ix0

FreeBSD nombra muchas interfaces a partir del driver que controla el dispositivo. Por eso dos tarjetas Ethernet de la misma velocidad pueden aparecer con prefijos diferentes. El número final suele distinguir instancias del mismo driver. No conviene memorizar una lista cerrada: hay que aprender a asociar el nombre con su driver y con la MAC física.

En entornos virtuales aparecen otros nombres, como vtnet para dispositivos VirtIO. El nombre revela una parte importante de la ruta: una vtnet no es un puerto PCIe físico controlado directamente por pfSense, sino una interfaz paravirtualizada suministrada por el hipervisor.

Laboratorio mental
Imagina que el instalador muestra igc0, igc1, igc2 e igc3. Antes de asignar WAN y LAN, ¿cómo sabrías qué conector físico corresponde a cada uno? La respuesta profesional no es “probar al azar”: usar MAC, link up/down, etiquetas del chasis y documentación.

8.3 WAN, LAN y OPT no describen tecnologías

WAN y LAN son roles convencionales. Una interfaz WAN puede utilizar Ethernet, PPPoE, una VLAN entregada por el operador o incluso una interfaz virtual. Una LAN puede ser una red de usuarios, una red de gestión o un trunk que transporte varias VLAN. Las interfaces OPT son simplemente interfaces adicionales que podemos renombrar con significado: SERVIDORES, VOZ, CCTV o DMZ.

La práctica recomendable es utilizar nombres funcionales. “OPT3” obliga a recordar qué contiene; “IOT” o “GESTION” comunica intención y reduce errores. La nomenclatura es una herramienta de seguridad porque disminuye la probabilidad de aplicar reglas a la zona equivocada.

8.4 Una NIC para todo: cuándo tiene sentido y qué implica

Es posible construir un laboratorio con una sola NIC física usando VLAN para separar WAN y redes internas, siempre que el switch y el diseño soporten 802.1Q. Esta arquitectura, a veces llamada de forma informal “router-on-a-stick”, reduce hardware pero concentra tráfico y dependencia en un único enlace físico.

Para producción, dos o más interfaces físicas simplifican separación y diagnóstico, aunque no existe una regla universal. Un trunk de 10 GbE con múltiples VLAN puede ser superior a cuatro puertos de 1 GbE si la arquitectura del switch y la redundancia están bien diseñadas. El número de conectores no equivale por sí mismo a calidad de diseño.

8.5 VLAN: varias redes lógicas sobre el mismo enlace

802.1Q añade una etiqueta a las tramas Ethernet para indicar a qué VLAN pertenecen. En un enlace trunk, varias VLAN viajan por la misma interfaz física manteniendo dominios de broadcast separados. pfSense crea interfaces VLAN sobre una interfaz padre y después esas interfaces pueden recibir nombres, direcciones y reglas independientes.

Esto permite separar usuarios, servidores, invitados, voz, cámaras o IoT sin dedicar una NIC física a cada red. Sin embargo, la separación lógica depende de que switch, firewall y configuración de puertos estén coordinados. Un trunk mal configurado puede dejar una VLAN inaccesible o, peor, mezclar tráfico donde no debería.

Qué ocurre realmente
La VLAN no “vive dentro de pfSense”. Es una convención de etiquetado que debe entender cada dispositivo del camino que transporta esa trama etiquetada. Un extremo que espera tráfico sin etiqueta y otro que lo envía etiquetado no están hablando el mismo idioma.

8.6 Access, trunk y VLAN nativa

Un puerto access pertenece normalmente a una VLAN y entrega al dispositivo final tramas sin etiqueta. Un trunk transporta varias VLAN etiquetadas entre equipos que entienden 802.1Q, como firewall y switch gestionable. La idea de VLAN nativa o tráfico sin etiqueta en un trunk debe manejarse con disciplina para evitar ambigüedades y errores de seguridad.

Para diseños nuevos es aconsejable documentar explícitamente qué VLAN se permite en cada trunk y no asumir que “todas” deben atravesar todos los enlaces. La reducción del dominio de VLAN también limita el impacto de errores de configuración.

8.7 LAGG: agregación y redundancia

LAGG permite combinar varias interfaces físicas en una interfaz lógica mediante protocolos o modos de agregación, como LACP cuando el switch lo soporta. Su principal valor suele ser la redundancia y la distribución de múltiples flujos, no convertir mágicamente una única conexión TCP en una conexión del doble de velocidad.

La agregación debe diseñarse junto con el switch. Si un extremo cree que dos enlaces forman un LAG y el otro los trata como puertos independientes, pueden aparecer bucles, pérdidas o comportamiento impredecible. Además, el algoritmo de hash determina cómo se distribuyen los flujos entre miembros.

8.8 Bridge: unir segmentos no siempre es la mejor solución

Un bridge permite conectar interfaces a nivel 2, haciendo que compartan un dominio Ethernet. Puede ser útil en escenarios concretos, pero no debe emplearse para evitar aprender routing. El routing crea fronteras claras y permite aplicar políticas entre redes; un bridge extiende el mismo dominio y puede ampliar broadcast, dependencia de spanning tree y complejidad de diagnóstico.

Cuando la intención es segmentar por seguridad, crear subredes y enrutar entre ellas suele ser más explícito que puentear. El bridge debe aparecer porque responde a un requisito técnico, no porque “faltan puertos en el switch”.

8.9 Offloading: cuando el hardware hace parte del trabajo

Las NIC modernas pueden calcular checksums, segmentar paquetes grandes o agrupar recepción para reducir trabajo de CPU. Estas funciones suelen mejorar rendimiento, pero algunas combinaciones de driver, hardware o virtualización pueden producir comportamientos problemáticos. En pfSense existen opciones para desactivar checksum offload y otras formas de offloading cuando el entorno lo requiere.

En capturas de paquetes es normal observar checksums aparentemente incorrectos en determinadas circunstancias porque la captura puede realizarse antes de que la NIC calcule el checksum de salida. Este detalle evita diagnosticar como corrupción un comportamiento esperado de la ruta de captura.

Error frecuente
Cambiar opciones de offloading “porque lo recomienda un foro” sin comprobar síntomas, driver y plataforma. Un ajuste útil en una VM concreta puede perjudicar o no aportar nada en hardware físico.

8.10 Wi-Fi: separar el firewall del punto de acceso

Aunque FreeBSD admite determinados adaptadores inalámbricos, la práctica más robusta para redes modernas suele ser que pfSense enrute y filtre, mientras puntos de acceso dedicados gestionan la radio. Esto permite elegir AP con estándares Wi-Fi actuales, roaming, gestión centralizada y múltiples SSID/VLAN sin condicionar el firewall a las limitaciones del driver inalámbrico.

Desde el punto de vista del firewall, el Wi-Fi se convierte en redes: corporativa, invitados, IoT, etc. Esa separación conceptual es valiosa porque la política se diseña por zona de confianza, no por el hecho de que el cliente use ondas de radio.

Capítulo 9. Appliance, hardware genérico o máquina virtual

No existe una plataforma universalmente superior. La decisión correcta depende de qué se quiera optimizar: simplicidad, coste, soporte, flexibilidad, consolidación, rendimiento, aislamiento o recuperación. Lo importante es entender qué riesgos se introducen con cada elección.

9.1 Appliance dedicado

Un appliance integra hardware y software con un objetivo concreto. Su ventaja principal es reducir variables: puertos conocidos, plataforma validada, consumo predecible y, en modelos comerciales, soporte del fabricante. También simplifica inventario y sustitución cuando la organización estandariza un modelo.

La contrapartida es menor libertad para ampliar CPU, RAM o NIC, y un coste de adquisición que puede ser superior al de componentes genéricos. Sin embargo, comparar solo precios de piezas ignora horas de validación, repuestos, soporte y riesgo operativo.

9.2 Hardware genérico o white-box

Un sistema construido a medida permite elegir exactamente los componentes. Es una opción excelente para aprendizaje, laboratorios y muchos entornos profesionales si se selecciona hardware bien soportado. También puede facilitar 10 GbE, múltiples ranuras PCIe, almacenamiento redundante o una CPU concreta.

La disciplina aquí es documentar chipset y driver antes de comprar. “Tiene cuatro puertos Intel” es mejor información que “tiene cuatro puertos”, pero aún conviene conocer el controlador exacto y la experiencia de FreeBSD con esa revisión. Lo mismo se aplica a controladoras de almacenamiento, sensores y consolas.

9.3 Máquina virtual

Virtualizar pfSense puede aportar snapshots, backup del disco virtual, migración, clonación de laboratorio y aprovechamiento de infraestructura existente. También crea una dependencia nueva: si el hipervisor, su almacenamiento o su switching virtual fallan, el firewall puede fallar junto con otras cargas.

La virtualización es especialmente potente cuando el equipo entiende claramente el dominio de fallo. Un pfSense virtual que proporciona acceso a Internet al mismo hipervisor que necesita Internet para ser administrado puede crear una situación circular si no existe consola o red de gestión alternativa.

Idea clave
Virtualizar un firewall no elimina hardware; añade una capa de software entre el firewall y el hardware. Esa capa ofrece ventajas, pero también debe diseñarse, monitorizarse y recuperarse.

9.4 NIC emulada, paravirtualizada o passthrough

Modelo	Cómo funciona	Ventajas	Riesgos / coste
Emulada	El hipervisor imita una NIC conocida	Compatibilidad amplia	Más sobrecarga; menos eficiente
Paravirtualizada (VirtIO)	Guest e hipervisor cooperan mediante driver optimizado	Buen rendimiento y flexibilidad	Depende del stack virtual y ajustes de offload
PCI passthrough	La VM controla directamente una NIC física	Aislamiento y ruta más directa	Pierde flexibilidad de migración; requiere IOMMU y diseño PCIe

pfSense incorpora drivers VirtIO en el kernel. En plataformas como Proxmox, la documentación actual insiste en comprobar el checksum offloading para interfaces vtnet, porque determinadas combinaciones pueden impedir o degradar el tráfico. Esto muestra por qué una VM no debe tratarse como una “caja negra” equivalente a un appliance físico.

9.5 Proxmox como ejemplo de arquitectura virtual

Un diseño típico utiliza dos bridges virtuales: uno conectado a la NIC o VLAN de WAN y otro conectado a la LAN o trunk interno. pfSense recibe dos interfaces VirtIO y actúa como router entre ambos mundos. En diseños más avanzados, el trunk puede transportar varias VLAN hacia un único vtnet interno.

La decisión crítica es qué tráfico debe atravesar el firewall y qué tráfico puede circular dentro del hipervisor. Si dos VM están en el mismo bridge y la misma subred, pueden comunicarse a nivel 2 sin pasar por pfSense. Para imponer política entre ellas deben pertenecer a redes diferentes o utilizar mecanismos adicionales de filtrado.

9.6 El problema del “huevo y la gallina”

Si pfSense virtual proporciona DHCP, DNS, routing e Internet a la red desde el mismo host que lo ejecuta, una caída del host elimina simultáneamente el firewall y los servicios que necesitamos para acceder al host. Esto no hace inválido el diseño, pero obliga a disponer de consola local, IPMI, una interfaz de gestión independiente o procedimientos de recuperación fuera de banda.

En producción
Antes de virtualizar el firewall, simula mentalmente tres fallos: hipervisor apagado, datastore no disponible y bridge mal configurado. Si en cualquiera de ellos no sabes cómo volver a entrar al host, falta una ruta de recuperación.

9.7 Cuándo elegir cada modelo

Si priorizas…	Opción que suele encajar mejor	Motivo
Simplicidad y soporte	Appliance dedicado	Menos variables de hardware y ruta de soporte clara
Personalización y coste	Hardware genérico validado	Control de CPU, NIC, chasis y ampliaciones
Laboratorio y automatización	Máquina virtual	Snapshots, clonación y topologías rápidas
Consolidación de sede pequeña	VM con gestión fuera de banda	Reduce equipos manteniendo recuperabilidad
Aislamiento físico fuerte	Appliance o passthrough dedicado	Menos dependencia del switching virtual
Alta disponibilidad	Dos nodos equivalentes	El diseño importa más que el formato físico

Capítulo 10. Diseñar la red antes de instalar

El instalador pide WAN y LAN muy pronto. Eso puede dar la impresión de que primero instalamos y después diseñamos. Para una red seria debe ocurrir lo contrario: antes de arrancar el instalador deberíamos poder dibujar las zonas, los enlaces, el direccionamiento y las dependencias principales.

10.1 Empezar por zonas de confianza

Una buena segmentación comienza preguntando qué dispositivos tienen un nivel de confianza parecido y qué comunicaciones necesitan. Los nombres de las VLAN vienen después. Usuarios, servidores, administración, invitados, IoT, voz o CCTV no son simplemente grupos organizativos: son superficies de riesgo y patrones de tráfico diferentes.

Un invitado necesita normalmente Internet pero no acceder a servidores internos. Una cámara puede necesitar hablar con el NVR y quizá con NTP, pero no iniciar conexiones hacia equipos de usuario. Una red de gestión debería ser accesible desde pocos dispositivos administrativos. Convertir estas frases en reglas será mucho más sencillo si la topología refleja la intención.

10.2 Una topología base para el libro

Zona	Subred de ejemplo	VLAN	Objetivo
GESTION	10.20.10.0/24	10	Administración de firewall, switches, AP e hipervisores
USUARIOS	10.20.20.0/24	20	Equipos corporativos
SERVIDORES	10.20.30.0/24	30	Servicios internos
IOT	10.20.40.0/24	40	Dispositivos de confianza reducida
INVITADOS	10.20.50.0/24	50	Acceso a Internet aislado
DMZ	10.20.60.0/24	60	Servicios expuestos o de frontera
VOZ	10.20.70.0/24	70	Telefonía IP

Estas direcciones son didácticas, no una recomendación universal. Lo importante es la regularidad: numeración coherente, espacio para crecimiento y relación clara entre VLAN y subred cuando eso ayude a la operación. El diseño definitivo debe evitar solapamientos con sedes, VPN y redes de terceros que sepamos que habrá que conectar.

10.3 El error de usar 192.168.1.0/24 para todo

Las redes privadas más comunes aparecen también en routers domésticos, hoteles, tethering y oficinas pequeñas. Si una VPN conecta dos lugares que utilizan exactamente la misma subred, el routing se vuelve ambiguo. Por eso, cuando se diseña una organización con futuras sedes o teletrabajo, conviene elegir un plan de direccionamiento que reduzca la probabilidad de solapamiento.

No existe un bloque privado “mágicamente correcto”. Lo profesional es reservar rangos, documentar su asignación y mantener capacidad de sumarización cuando sea útil. IPv6 añade otra dimensión que trataremos en profundidad más adelante, pero la disciplina de planificación sigue siendo la misma.

10.4 Dónde termina la LAN y empieza el switching

pfSense no sustituye a un switch de acceso. El firewall debe concentrarse en routing y política entre redes; el switch conecta dispositivos dentro de cada dominio de capa 2 y transporta trunks entre elementos de infraestructura. Usar puertos del firewall como si fueran un pequeño switch puede ser válido en casos concretos, pero no debe confundirse con una arquitectura de switching escalable.

En redes con varias VLAN, un switch gestionable se convierte en pieza central. Sus puertos access asignan dispositivos a una VLAN; los trunks transportan varias VLAN hacia pfSense, puntos de acceso, hipervisores u otros switches. El firewall ve interfaces lógicas y decide qué puede cruzar de una red a otra.

10.5 Red de gestión

Separar la administración de infraestructura tiene dos ventajas: reduce exposición y facilita imponer una política distinta. La WebGUI de pfSense, SSH de switches, controladores Wi-Fi, IPMI y paneles de hipervisores no tienen por qué ser accesibles desde cualquier PC de usuario.

Una red de gestión no es segura únicamente por existir. Debe tener reglas restrictivas, autenticación robusta y, cuando sea posible, acceso desde estaciones administrativas concretas o mediante un salto controlado. También hay que pensar cómo entrar si el firewall principal falla: la gestión fuera de banda pertenece a un plano distinto.

10.6 DMZ: no es “la red de servidores”

Una DMZ es una zona diseñada para reducir el impacto de servicios que deben ser alcanzables desde redes menos confiables. No todos los servidores internos deben estar en ella. Un ERP, un servidor de ficheros o un controlador de dominio no se convierten en “más seguros” por llamarlos DMZ si las reglas permiten todo hacia la LAN.

La DMZ funciona cuando existe una política explícita entre Internet, DMZ y redes internas. El servicio publicado debe recibir únicamente los puertos necesarios; sus conexiones hacia dentro deben limitarse a dependencias concretas. La segmentación no sustituye al hardening del servidor, pero restringe el movimiento lateral.

10.7 IoT, CCTV e invitados: segmentar por riesgo

Dispositivos embebidos, cámaras, televisores, impresoras y equipos de invitados suelen tener ciclos de actualización y niveles de confianza distintos a un puesto corporativo. Colocarlos en redes separadas permite aplicar políticas de salida, bloquear acceso lateral y observar su comportamiento con mayor claridad.

La segmentación no debe convertirse en una colección infinita de VLAN sin propósito. Cada nueva zona aumenta reglas, documentación y diagnóstico. Se crea cuando existe una diferencia de confianza, servicio, administración o requisito que justifica esa frontera.

10.8 Multi-WAN: diseñar antes de añadir el segundo proveedor

Tener dos conexiones de Internet no garantiza continuidad. Hay que decidir qué significa “fallo”, cómo se monitoriza cada gateway, qué tráfico debe cambiar de proveedor, qué ocurre con las sesiones existentes, cómo se comportan las VPN y si existen servicios publicados que dependan de una dirección pública concreta.

El segundo enlace puede utilizarse para failover, balanceo o políticas selectivas. Estas funciones se estudiarán después; en esta fase basta con reservar interfaces, alimentación, equipos del operador y caminos físicos de forma que ambos enlaces no compartan todos los puntos de fallo.

10.9 DNS y DHCP forman parte de la arquitectura

DHCP decide cómo reciben configuración los clientes; DNS influye en casi toda experiencia de usuario. Antes de instalar conviene definir si pfSense proporcionará esos servicios, si existen servidores corporativos, qué redes necesitan DHCP relay, qué dominios internos habrá y qué resolvers serán autoritativos o recursivos.

Una red “sin Internet” puede tener routing perfecto y estar sufriendo únicamente un fallo de DNS. Por eso el diseño debe diferenciar conectividad IP, resolución de nombres y entrega de parámetros. Más adelante utilizaremos esa separación como método de diagnóstico.

10.10 Dibujar flujos, no solo cajas

Un diagrama de red útil no debe limitarse a iconos. Debe permitir responder quién inicia una conexión, hacia dónde, por qué puerto, a través de qué interfaz y con qué dependencia. Una flecha “USUARIOS → SERVIDORES: HTTPS 443” aporta más información de seguridad que dos rectángulos unidos por una línea.

Laboratorio
Toma las siete zonas del ejemplo y escribe diez flujos permitidos. Después escribe diez flujos que deberían estar prohibidos. Si no puedes justificar cada decisión con una necesidad de negocio o técnica, todavía no tienes una política: tienes intuiciones.

Capítulo 11. Plan de instalación: convertir el diseño en decisiones

Antes de insertar un USB o crear una VM, necesitamos transformar la arquitectura en una hoja de instalación. Ese documento será la referencia para asignar interfaces y evitar que decisiones tomadas bajo presión se conviertan en deuda técnica.

11.1 Hoja de interfaces

Rol	Interfaz / puerto	Tipo	VLAN	Dirección prevista	Conecta con
WAN1	igc0 / puerto 1	Física	—	DHCP o estática ISP	ONT/router operador
TRUNK-LAN	igc1 / puerto 2	Física trunk	10,20,30,40,50,60,70	Sin IP directa idealmente	Switch principal
WAN2	igc2 / puerto 3	Física	—	Según ISP2	Segundo operador
GESTION-OOB	BMC/IPMI o puerto separado	Fuera de banda	—	Red de administración	Switch/puerto OOB

En una instalación física, esta tabla debe acompañarse con MAC, etiqueta del chasis y, si es posible, fotografía o diagrama de puertos. En una VM, debe incluir bridge virtual, VLAN awareness, modelo de NIC y MAC asignada. La meta es que otra persona pueda reconstruir la correspondencia sin preguntarnos “¿cuál era la WAN?”.

11.2 Hoja de direccionamiento

Zona	CIDR	Gateway pfSense	DHCP	Rango reservado	Notas
GESTION	10.20.10.0/24	10.20.10.1	Opcional	10.20.10.2-49	Infraestructura fija
USUARIOS	10.20.20.0/24	10.20.20.1	Sí	10.20.20.2-49	Clientes corporativos
SERVIDORES	10.20.30.0/24	10.20.30.1	No / reservas	10.20.30.2-199	IPs documentadas
IOT	10.20.40.0/24	10.20.40.1	Sí	10.20.40.2-49	Salida restringida
INVITADOS	10.20.50.0/24	10.20.50.1	Sí	—	Sin acceso interno
DMZ	10.20.60.0/24	10.20.60.1	Normalmente no	10.20.60.2-199	Servicios publicados

11.3 Hoja de dependencias

Además de IP, hay que registrar dependencias: DNS internos, NTP, autenticación, RADIUS/LDAP, syslog, monitorización, backup de configuración, correo de alertas, certificados y VPN. Cuando el firewall se sustituye, son estas relaciones las que suelen causar sorpresas.

- ¿Qué sistemas dependen de la dirección LAN actual del firewall?
- ¿Qué rutas estáticas existen en routers, servidores o switches de capa 3?
- ¿Qué port-forward publica servicios hacia Internet?
- ¿Qué VPN remotas esperan una IP pública o FQDN concreto?
- ¿Qué dispositivos tienen DNS o gateway configurado manualmente?
- ¿Qué sistemas envían logs, métricas o backups a través del firewall?
- ¿Qué certificados, claves o credenciales hay que preservar?

11.4 Lista de compra técnica

La lista de compra no debe limitarse al firewall. Incluye cables, módulos SFP/SFP+, transceptores, switch gestionable, UPS, adaptador de consola, almacenamiento de repuesto, etiquetas y, si el riesgo lo justifica, un segundo equipo. Una arquitectura puede fallar el día de la instalación por un transceptor incompatible o un cable que no soporta la velocidad prevista.

11.5 Checklist de compatibilidad antes de comprar

- CPU amd64 soportada para hardware genérico y margen suficiente para la carga prevista.
- NIC identificadas por chipset y driver FreeBSD, no únicamente por velocidad comercial.
- Puertos suficientes o estrategia VLAN/trunk definida.
- Almacenamiento fiable y procedimiento de backup independiente del disco.
- Método de consola recuperable sin red: VGA, serie, IPMI/BMC o consola del hipervisor.
- Switch con 802.1Q si habrá VLAN y LACP si se proyecta agregación.
- Capacidad de UPS y alimentación para firewall, switch y equipos de operador.
- Plan para reemplazo: repuesto, segundo nodo o procedimiento de reinstalación probado.
- En virtualización: CPU/RAM reservables, bridges, VLAN, VirtIO/passthrough y gestión fuera de banda.
- Documentación de MAC, puertos, VLAN, direcciones, credenciales de emergencia y dependencias.

11.6 Laboratorio de decisión: tres diseños para la misma pyme

Supongamos una empresa de 70 usuarios, fibra de 1 Gb/s, 20 teléfonos IP, 30 cámaras, Wi-Fi corporativa e invitados, una pequeña DMZ, acceso remoto por VPN y previsión de una segunda sede. El objetivo es comparar arquitecturas, no buscar un único equipo “correcto”.

Diseño A — Appliance dedicado + switch gestionable

El firewall dispone de WAN, trunk LAN y un puerto adicional reservado. Todas las redes internas viajan etiquetadas hacia un switch gestionable. El appliance se conecta a una UPS y su consola queda accesible. Es una arquitectura clara y con dominio de fallo separado del clúster de virtualización.

Ventaja principal: simplicidad operacional. Inconveniente: hardware dedicado y menor elasticidad que una VM. Es especialmente razonable cuando el equipo de sistemas quiere que la conectividad sobreviva a mantenimientos del hipervisor.

Diseño B — pfSense virtual en Proxmox

Dos NIC físicas del host se dedican a conectividad de firewall o se integran cuidadosamente en bridges. pfSense usa VirtIO y un trunk virtual hacia las VLAN internas. La red de gestión del host queda diseñada de modo que pueda accederse incluso si la VM de firewall está detenida.

Ventaja: snapshots, backup y consolidación. Riesgo: el host se convierte en un punto de fallo más amplio. La solución no es “no virtualizar”, sino disponer de rutas de gestión y recuperación independientes.

Diseño C — Dos firewalls para alta disponibilidad

Dos nodos equivalentes conectan con los switches y operadores necesarios. Más adelante configuraremos CARP, pfsync y sincronización. En esta fase hay que reservar interfaces, direccionamiento y conexiones para que el segundo nodo no sea un accesorio improvisado.

Ventaja: mantenimiento y fallo de nodo con menor interrupción. Coste: más puertos, más direccionamiento, mayor disciplina y necesidad de evitar puntos únicos de fallo en switches, alimentación y operadores.

11.7 Cómo elegir entre los tres

Pregunta	Si la respuesta es sí…	Consecuencia de diseño
¿La conectividad debe seguir durante mantenimiento del hipervisor?	Favorece appliance separado o clúster muy bien diseñado	Separar dominio de fallo
¿Existe personal que administra Proxmox con soltura?	La VM gana atractivo	La complejidad virtual es asumible
¿Una hora sin red tiene alto impacto?	Considerar HA y repuestos	Invertir en redundancia y procedimientos
¿Habrá 10 GbE interno?	Revisar NIC, PCIe y switching	No dimensionar solo por WAN
¿IDS/IPS y VPN serán intensivos?	Aumentar CPU/RAM y medir	El software adicional puede dominar el sizing
¿No existe consola fuera de banda?	Evitar dependencias circulares	Diseñar recuperación antes de desplegar

11.8 Prueba previa a producción

Una vez elegido el hardware, la validación debe reproducir los aspectos críticos del entorno: throughput, múltiples VLAN, VPN, failover, reinicio, restauración de configuración, desconexión de enlaces y acceso por consola. La prueba útil no consiste solo en comprobar que la WebGUI abre.

1. Actualizar firmware/BIOS cuando proceda y documentar la versión.
2. Verificar que todas las NIC aparecen y mantener un mapa MAC ↔️ puerto.
3. Comprobar link a las velocidades esperadas y errores de interfaz.
4. Crear las VLAN de laboratorio y confirmar etiquetas en switch y firewall.
5. Medir rendimiento base sin paquetes adicionales.
6. Activar VPN o IDS/IPS previstos y repetir la medición.
7. Reiniciar el sistema y comprobar que vuelve sin intervención manual.
8. Restaurar una copia de configuración en un entorno seguro.
9. Probar acceso por consola cuando la interfaz LAN está deliberadamente mal configurada.
10. Registrar resultados y dejar un margen explícito entre carga medida y capacidad máxima.

Criterio de aceptación
No declares "válido" un firewall porque alcance la velocidad contratada una vez. Declárlo válido cuando soporte la carga prevista con margen, se recupere de fallos ensayados y otra persona pueda entender su cableado y configuración.

Cierre de la Parte II

A estas alturas todavía no hemos pulsado "Install", y ésa es precisamente la intención. Ya sabemos qué tiene que hacer la máquina, cómo estimar su carga, por qué la NIC y el driver importan, qué diferencia existe entre puerto físico y rol lógico, cómo encajan VLAN y trunks, qué cambia al virtualizar y cómo dibujar una red antes de configurarla.

La Parte III convertirá este diseño en una instalación reproducible. Prepararemos medios, examinaremos BIOS/UEFI, instalaremos sobre ZFS, asignaremos interfaces, realizaremos el primer acceso seguro y construiremos una configuración base que pueda restaurarse. A partir de ese momento cada capítulo podrá apoyarse en una plataforma coherente, en lugar de improvisar sobre una topología distinta.

Glosario esencial de la Parte II

Término	Definición de trabajo
amd64	Nombre utilizado por FreeBSD para la arquitectura x86-64 de 64 bits, tanto Intel como AMD.
PPS	Paquetes por segundo; medida crítica para evaluar carga de procesamiento más allá de los bits por segundo.
NIC	Network Interface Controller/Card; hardware y lógica que conecta el sistema con una red.
Driver	Componente del sistema operativo que controla un dispositivo, como una NIC.
Offloading	Trabajo de red delegado al hardware de la NIC, por ejemplo checksum o segmentación.

Término	Definición de trabajo
AES-NI	Conjunto de instrucciones de CPU que acelera operaciones AES compatibles.
QAT	Tecnología de aceleración de Intel para determinadas cargas criptográficas y de compresión; disponibilidad según plataforma/edición.
ZFS ARC	Caché adaptativa en memoria utilizada por ZFS.
Trunk	Enlace que transporta múltiples VLAN, normalmente mediante etiquetado 802.1Q.
Access	Puerto de switch asociado normalmente a una única VLAN para un equipo final.
LAGG	Interfaz lógica que agrupa varios enlaces físicos para redundancia y/o distribución de tráfico.
VirtIO	Familia de dispositivos paravirtualizados para máquinas virtuales.
Passthrough	Asignación directa de un dispositivo físico PCI/PCIe a una máquina virtual.
IOMMU	Mecanismo de hardware que permite aislar y mapear acceso DMA, necesario habitualmente para passthrough seguro.
OOB	Out-of-band management; canal de administración independiente de la red de datos principal.
DMZ	Zona de seguridad separada para sistemas con exposición o requisitos distintos a la red interna.

Fuentes técnicas consultadas para contraste

Estas fuentes se han utilizado para verificar requisitos, compatibilidad, terminología y comportamiento técnico. La redacción y organización de esta Parte II son originales y no siguen la estructura de la documentación citada.

1. Netgate Documentation — “Minimum Hardware Requirements”, docs.netgate.com/pfsense/en/latest/hardware/minimum-requirements.html (consulta: 8 de octubre de 2026).

2. Netgate Documentation — “Hardware Sizing Guidance”, docs.netgate.com/pfsense/en/latest/hardware/size.html (consulta: 8 de octubre de 2026).

3. Netgate Documentation — “Hardware Selection”, docs.netgate.com/pfsense/en/latest/hardware/selection.html (consulta: 8 de octubre de 2026).

4. Netgate Documentation — “Memory Management” y “ZFS Tuning”, docs.netgate.com/pfsense/en/latest/hardware/ (consulta: 8 de octubre de 2026).

5. Netgate Documentation — “Cryptographic Accelerators”, docs.netgate.com/pfsense/en/latest/hardware/cryptographic-accelerators.html (consulta: 8 de octubre de 2026).

6. Netgate Documentation — “Interface Types and Configuration”, docs.netgate.com/pfsense/en/latest/interfaces/ (consulta: 8 de octubre de 2026).

7. Netgate Documentation — “Virtual LANs (VLANs)”, docs.netgate.com/pfsense/en/latest/vlan/ (consulta: 8 de octubre de 2026).

8. Netgate Documentation — “Networking / Hardware Checksum Offloading”, docs.netgate.com/pfsense/en/latest/config/advanced-networking.html (consulta: 8 de octubre de 2026).

9. Netgate Documentation — “VirtIO Drivers” y “Virtualizing with Proxmox VE”, docs.netgate.com/pfsense/en/latest/virtualization/ y /recipes/virtualize-proxmox-ve.html (consulta: 8 de octubre de 2026).

10. Netgate Store — colección de productos pfSense Plus, shop.netgate.com/collections/pfsense-products (consulta: 8 de octubre de 2026).

11. Netgate — “Product Lifecycle”, netgate.com/support/product-lifecycle (consulta: 8 de octubre de 2026).

12. FreeBSD Documentation Portal — Handbook y documentación de drivers de red, docs.freebsd.org (consulta: 8 de octubre de 2026).

13. IEEE 802.1Q — concepto de virtual bridged LANs y etiquetado VLAN, utilizado como referencia conceptual.

pfSense® software

REDES, FIREWALL Y SEGURIDAD

Arquitectura, administración y laboratorios prácticos

PARTE III

Instalación, primer arranque y configuración base

Oscar de la Cuesta

palentino.es



Primera edición · octubre de 2026

Punto de partida de esta parte

La Parte II terminó antes de encender el firewall: hardware seleccionado, interfaces identificadas, zonas definidas, direccionamiento previsto y dependencias anotadas. Esta Parte III comienza exactamente en ese punto. Ahora convertiremos un diseño sobre papel en un sistema arrancable, administrable y recuperable.

El objetivo no es memorizar una sucesión de pantallas. La instalación es el primer momento en el que aparecen decisiones con consecuencias reales: qué medio utilizar, cómo dar conectividad al instalador, qué interfaz será WAN, qué almacenamiento recibirá el sistema, qué red tendrá la LAN, qué credenciales protegerán la administración y cómo conservar una copia recuperable de la configuración.

A octubre de 2026, el procedimiento oficial de instalación se apoya en Netgate Installer, un instalador conectado que descarga los componentes necesarios durante el proceso. Esto obliga a entender una diferencia importante respecto a generaciones anteriores: el medio de arranque inicia la instalación, pero no contiene necesariamente todo el sistema que terminará instalado.

Criterio de esta parte
La documentación oficial se utiliza para verificar comportamiento, requisitos y valores actuales. Las explicaciones, tablas, escenarios, diagramas y laboratorios siguen el enfoque didáctico propio de este libro.

Qué aprenderemos en esta parte

- Preparar una instalación física o virtual sin depender de improvisaciones durante el arranque.
- Entender qué hace un instalador conectado y qué dependencias introduce.
- Identificar interfaces por MAC, enlace y función, no solo por nombres como igb0 o vtnet1.
- Interpretar la configuración inicial que pfSense crea por defecto y saber cuándo modificarla antes de conectar la red.
- Utilizar la consola como mecanismo de recuperación, no como una pantalla de emergencia desconocida.
- Completar el primer acceso a la WebGUI con una configuración mínima segura.
- Separar los cambios imprescindibles del primer día de las optimizaciones que deben esperar.
- Actualizar con criterio, registrar el estado inicial y crear una primera copia de configuración verificable.
- Realizar una puesta en servicio controlada con pruebas de conectividad, DNS, NAT, hora, administración y recuperación.

Capítulo 12. Preparar la instalación sin improvisar

Instalar un firewall parece una tarea local: insertar un USB, arrancar y responder preguntas. En realidad es una operación de red. Desde el primer minuto intervienen el firmware del equipo, el medio de instalación, los controladores, el enlace físico, el acceso al upstream, el almacenamiento de destino y, en el modelo actual, la conectividad necesaria para descargar los paquetes de instalación.

Por eso la instalación debe comenzar con una pequeña ficha de despliegue. Cinco minutos dedicados a escribir qué puerto es cuál, qué equipo proporciona Internet y qué dirección debe tener la LAN ahorran gran parte de los errores que después se atribuyen al firewall.

12.1. La ficha de despliegue

Dato	Ejemplo	Por qué importa
Equipo objetivo	Mini-PC amd64, 4 NIC Intel, SSD 128 GB	Define arquitectura, consola y controladores esperables.
WAN física	Puerto 1 / MAC …:A1	Evita intercambiar WAN y LAN durante la asignación.
LAN física	Puerto 2 / MAC …:A2	Permite conectar el equipo de administración al lado correcto.
Upstream	Router del operador, DHCP	Determina cómo obtendrá conectividad el instalador.
LAN prevista	10.20.0.1/24	Evita usar una red que choque con el upstream.
DHCP inicial	10.20.0.100–10.20.0.199	Permite administrar sin configurar cada cliente a mano.
DNS/NTP	Inicialmente automáticos; después se revisan	La resolución y la hora condicionan actualizaciones, certificados y logs.
Consola	VGA + teclado / serial / consola VM	Debe existir una ruta de recuperación si la WebGUI queda inaccesible.

Error frecuente
Conectar todas las interfaces a la red antes de haber decidido su función. Un cable mal puesto puede convertir el primer arranque en un problema de DHCP duplicado, subredes solapadas o acceso a la GUI desde el lado equivocado.

12.2. Elegir el medio de instalación

El medio de instalación no debe confundirse con el sistema instalado. Su misión es arrancar un entorno mínimo capaz de reconocer el hardware, establecer red, seleccionar el destino y desplegar pfSense en el almacenamiento interno.

En el momento de redactar esta edición existen imágenes oficiales para amd64 mediante memoria USB, amd64 mediante ISO y una variante AARCH64 destinada a determinados dispositivos ARM. Para un servidor físico convencional suele interesar la memoria USB; para IPMI, una unidad óptica virtual o un hipervisor, la ISO resulta más cómoda.

Escenario	Medio práctico	Observación
PC/servidor físico amd64	Memoria USB	Adecuado cuando se dispone de acceso físico y firmware USB.
Servidor con IPMI/iKVM	ISO montada remotamente	Evita desplazamiento y permite reinstalación fuera de banda.
Proxmox/ESXi/Hyper-V	ISO virtual	La consola del hipervisor sustituye a monitor y teclado.
Appliance ARM compatible	Imagen AARCH64 específica	No debe suponerse que cualquier equipo ARM es compatible.

Seguridad
Descarga el instalador desde la fuente oficial y verifica su integridad mediante SHA-256 antes de escribirlo en un USB o montarlo como ISO. La verificación no mejora el rendimiento: confirma que los bytes recibidos son los esperados.

12.3. Firmware: BIOS, UEFI y orden de arranque

Antes de culpar al instalador, conviene revisar el firmware. Un equipo puede tener el USB perfectamente grabado y, sin embargo, iniciar siempre desde el SSD. En entornos virtualizados puede ocurrir lo mismo cuando la ISO queda por detrás del disco duro en el orden de arranque.

- Comprobar que el medio aparece entre los dispositivos de arranque.
- Revisar el modo UEFI/legacy si el hardware tiene restricciones particulares.
- Documentar cualquier cambio de Secure Boot cuando el hipervisor o la plataforma lo exijan.
- No borrar el almacenamiento antiguo hasta tener confirmado el plan de recuperación.
- Si el equipo admite consola serie, conocer de antemano velocidad y puerto físico.

El objetivo no es crear una receta universal de firmware. Cada placa base y cada hipervisor presenta opciones diferentes. Lo importante es entender qué debe ocurrir: el firmware entrega el control al medio de instalación, el medio carga su kernel y, a partir de ahí, pfSense debe ser capaz de reconocer almacenamiento y red.

12.4. La instalación actual depende de Internet

El instalador actual es un instalador en línea. Eso significa que necesita una ruta funcional hacia Internet para obtener los componentes que instalará. Puede trabajar con una WAN que reciba dirección por DHCP, con direccionamiento estático o con PPPoE. Si la organización utiliza otro mecanismo de acceso más complejo, debe prepararse una vía temporal compatible.

Qué ocurre realmente

El USB o la ISO arranca un entorno de instalación. Ese entorno detecta interfaces, obtiene conectividad y descarga los paquetes. Si no hay DNS, puerta de enlace, enlace físico o autenticación WAN válida, el problema puede manifestarse como 'no instala', aunque el almacenamiento y el medio estén correctos.

12.5. Instalación física frente a instalación virtual

En hardware físico el riesgo principal es confundir puertos o controladores. En una máquina virtual, el riesgo cambia: puede construirse una topología lógicamente incorrecta aunque todos los adaptadores aparezcan como activos. Una vNIC conectada al bridge equivocado funciona técnicamente, pero transporta el tráfico de la red que no corresponde.

Físico	Virtual
Puerto visible, cable real y LED de enlace.	vNIC, bridge/vSwitch y asociación lógica.
El fallo puede estar en cable, transceptor, NIC o switch.	El fallo puede estar en el vSwitch, bridge, VLAN tagging o modelo de adaptador.
Consola VGA/serie/IPMI.	Consola del hipervisor.
Un reinicio afecta solo al firewall.	Un reinicio o fallo del host puede afectar al firewall y a otras VM.

En producción

Si pfSense será el perímetro de una empresa, la decisión de virtualizarlo debe estar tomada antes de instalar. El primer arranque no es el momento de descubrir que la administración del hipervisor depende del mismo firewall que todavía no funciona.

Capítulo 13. Del arranque al sistema instalado

Una instalación bien preparada debe poder explicarse como una cadena de estados. Esa cadena es más útil que recordar pantallas, porque permite localizar dónde se ha detenido el proceso.

Firmware → medio de arranque → kernel del instalador → detección de hardware → conectividad WAN → descarga de componentes → almacenamiento de destino → escritura del sistema → reinicio → detección/asignación de interfaces

13.1. Detectar antes de escribir

La primera comprobación es sencilla: ¿el instalador ve las interfaces y el disco que esperábamos? Si falta una NIC o un dispositivo de almacenamiento, continuar no arreglará nada. Es preferible detenerse y resolver compatibilidad, modo del controlador o configuración del hipervisor.

La detección de interfaces debe contrastarse con la ficha de despliegue. Las direcciones MAC son especialmente útiles porque permanecen ligadas a cada interfaz virtual o física y permiten distinguir dos adaptadores del mismo modelo.

13.2. Construir conectividad temporal

Durante la instalación, WAN no significa todavía 'interfaz protegida por todas las reglas que configuraremos después'. Es, ante todo, el camino por el que el instalador alcanzará los servidores necesarios. Si el upstream asigna por DHCP, el proceso suele ser simple. Si usa una IP fija, deben conocerse dirección, prefijo, gateway y DNS. En PPPoE hacen falta además las credenciales.

Idea clave
El instalador necesita conectividad; el firewall definitivo necesita una política de seguridad. Son dos problemas relacionados, pero no idénticos. No conviene diseñar toda la política definitiva dentro del instalador.

13.3. El papel de la LAN durante la instalación

La LAN permite preparar un lado administrativo local y, en determinados escenarios, facilita diagnóstico. El valor habitual de una instalación nueva es 192.168.1.1/24 con servicio DHCP activo. No debemos aceptar ese valor de forma automática si la WAN o cualquier red adyacente utiliza ya 192.168.1.0/24.

Cuando WAN y LAN pertenecen a la misma subred, el firewall no tiene una frontera de encaminamiento coherente entre ambas. El síntoma puede parecer caprichoso —GUI inaccesible, rutas extrañas, tráfico que toma el lado equivocado—, pero la causa es conceptual: dos interfaces de capa 3 no deben competir por la misma red conectada.

13.4. Almacenamiento: sistema, configuración y recuperación

pfSense no se administra como un FreeBSD genérico en el que cada servicio mantiene una configuración manual repartida por decenas de archivos. La configuración declarativa principal se concentra en un XML y, a partir de ella, el sistema genera archivos y comportamiento operativo. Esta característica cambia cómo debemos pensar el respaldo: preservar config.xml es extraordinariamente valioso.

El instalador debe escribir el sistema en un dispositivo fiable. Un SSD modesto suele ser preferible a una memoria flash de baja calidad, especialmente si el equipo registrará muchos eventos o instalará paquetes que escriban con frecuencia.

Qué ocurre realmente
El sistema base puede reinstalarse; la identidad operativa del firewall está principalmente en su configuración. Por eso una copia reciente de config.xml puede tener más valor para recuperación que una imagen sector a sector del disco.

13.5. Primer reinicio: retirar el medio

Al finalizar la instalación, el equipo debe reiniciar desde el almacenamiento interno. Si el USB o ISO conserva prioridad, volveremos al instalador y parecerá que la instalación no ha persistido. En una VM conviene desmontar la ISO o corregir el orden de arranque; en físico, retirar el USB cuando corresponda.

El reinicio marca un cambio de contexto: ya no estamos en un entorno temporal. Ahora arrancará el sistema que mantendrá estados, reglas, servicios y configuración. A partir de aquí, cualquier modificación debe quedar documentada.

13.6. Tres síntomas que conviene interpretar

Síntoma	Causa probable	Comprobación inicial
No aparece ninguna NIC	Modelo de vNIC o hardware no soportado/detectado	Revisar consola, modelo de adaptador y firmware/hipervisor.
Installer sin Internet	WAN equivocada, DHCP/gateway/DNS/PPPoE	Verificar enlace, MAC, dirección, ruta por defecto y DNS.
Tras reiniciar vuelve el instalador	Medio todavía primero en el arranque	Retirar USB/ISO y revisar boot order.
No aparece el disco destino	Controlador/modo de almacenamiento	Revisar BIOS, controlador virtual y visibilidad del dispositivo.
LAN coincide con upstream	Subred solapada	Cambiar LAN antes de conectar el resto de la red.

Capítulo 14. Primer arranque: interfaces y consola

La consola es la primera interfaz de administración que existe incluso cuando todavía no hay una WebGUI accesible. Saber utilizarla transforma muchos incidentes graves en correcciones de pocos minutos.

En una instalación nueva, pfSense intenta asociar las interfaces detectadas con funciones como WAN y LAN. En hardware conocido puede existir una correspondencia automática; en otros equipos o VM puede pedir una asignación manual.

14.1. No memorizar nombres de interfaz

Nombres como igb0, em1, igc2, ix0, vtnet0, hn0 o vmx0 dependen del controlador y de la plataforma. El administrador debe pensar en identidad y función:

```
Identidad física/virtual → MAC → enlace → red conectada → función lógica
Ejemplo: vtnet0 → 52:54:...:10 → bridge WAN → upstream → WAN
```

En Proxmox con VirtIO es habitual ver nombres vtnet; en Hyper-V se emplean adaptadores identificados de forma distinta; en VMware aparecen otros controladores. El nombre no es la red: solo es el identificador que el sistema operativo asigna al dispositivo.

14.2. La técnica del cable y el enlace

Cuando existen varias NIC idénticas y no hay etiquetas fiables, una forma práctica de identificarlas consiste en observar el estado de enlace mientras se conecta o desconecta un cable. En una VM, el equivalente es comparar la MAC configurada en el hipervisor con la mostrada por pfSense.

Laboratorio mental

Tienes cuatro puertos idénticos. El instalador muestra cuatro MAC. Antes de asignar WAN, fotografía o anota la etiqueta física de cada puerto y su MAC. Después conecta solo el cable upstream. La interfaz que cambia a 'link up' es una candidata inequívoca para WAN.

14.3. Qué crea pfSense por defecto

Tras una instalación nueva, el sistema establece un punto de partida utilizable. En la configuración predeterminada vigente, WAN intenta obtener IPv4 por DHCP y también puede solicitar IPv6; LAN utiliza 192.168.1.1/24; existe DHCP en LAN; el tráfico iniciado desde LAN puede salir; las conexiones entrantes desde WAN se bloquean; se realiza NAT IPv4 hacia WAN; el DNS Resolver está activo; SSH permanece desactivado y la GUI escucha por HTTPS.

Componente	Estado inicial conceptual	Implicación
WAN	Cliente automático	Puede obtener conectividad sin intervención en muchos accesos.
LAN	192.168.1.1/24	Proporciona una red de administración inmediata.

Componente	Estado inicial conceptual	Implicación
DHCP LAN	Activo	Un portátil puede recibir IP automáticamente.
Firewall WAN	Entradas no solicitadas bloqueadas	No equivale a que todo el sistema esté ya endurecido.
LAN → Internet	Permitido + NAT IPv4	Facilita la puesta en marcha.
DNS Resolver	Activo	Los clientes pueden consultar DNS a través del firewall.
WebGUI	HTTPS	Administración cifrada desde el inicio.
SSH	Desactivado	Reduce superficie mientras no sea necesario.

Error frecuente
Confundir 'configuración por defecto razonablemente segura' con 'firewall listo para producción'. Aún faltan credenciales propias, direccionamiento definitivo, DNS/NTP, usuarios, actualizaciones, copia de seguridad y validación.

14.4. La consola como red de seguridad

El menú de consola permite resolver problemas que no requieren una reinstalación: reasignar interfaces, cambiar direcciones IP, recuperar acceso a la GUI, reiniciar servicios, realizar pruebas de conectividad o abrir una shell para diagnóstico avanzado.

No todas las opciones de consola deben convertirse en herramientas rutinarias. La WebGUI mantiene coherencia y validaciones que reducen errores. La consola es especialmente valiosa cuando el problema impide usar la interfaz web.

Situación	Primera herramienta
LAN tiene una IP incorrecta	Consola: reconfigurar interfaz LAN.
Se intercambiaron WAN y LAN	Consola: reasignar interfaces.
GUI no responde pero hay consola	Revisar dirección, servicio y conectividad desde consola.
Se perdió conectividad tras una regla	Consola + revisión/restauración de configuración.
Se necesita verificar un host	Ping/rutas desde el propio firewall.
Cambio masivo normal de configuración	Preferir WebGUI y backup previo.

14.5. El primer equipo de administración

El primer cliente debería conectarse únicamente a la LAN o a un switch aislado que represente la LAN. Lo ideal es evitar que otras redes corporativas se mezclen con este segmento mientras todavía estamos configurando.

1. Conectar el portátil de administración a LAN.
2. Obtener una dirección por DHCP o asignar una dirección estática compatible.
3. Comprobar la puerta de enlace recibida.
4. Hacer ping a la dirección LAN del firewall si procede.
5. Abrir la GUI por HTTPS.
6. Verificar que la sesión se establece contra la dirección esperada y no contra otro equipo.

Capítulo 15. Primer acceso a la WebGUI: configuración mínima segura

Llegar a la WebGUI no significa que la instalación esté terminada. Significa que ya disponemos de una herramienta cómoda para convertir la configuración de emergencia del primer arranque en una configuración administrativa consciente.

La GUI utiliza HTTPS por defecto. En el primer acceso puede aparecer una advertencia del navegador porque el certificado inicial no ha sido emitido por una autoridad en la que el navegador confíe. Eso no debe resolverse desactivando HTTPS; más adelante podremos sustituir el certificado o integrar una PKI.

15.1. Credenciales iniciales y cambio de contraseña

La cuenta administrativa inicial debe dejar de usar credenciales conocidas tan pronto como sea posible. En versiones recientes de pfSense Plus el cambio del password inicial es obligatorio en el primer flujo de configuración. Aunque una edición concreta no lo fuerce, la práctica correcta es la misma: no mantener una contraseña por defecto.

> **Seguridad**
> La contraseña de administración protege la política de red completa. Debe ser única, larga y almacenarse en un gestor de contraseñas. No se debe reutilizar una contraseña de Windows, correo o hipervisor.

15.2. Hostname, dominio y resolución

Asignar un nombre coherente al firewall parece cosmético, pero aparece en logs, copias de seguridad, monitorización, certificados y mensajes de alerta. En una organización con varias sedes, nombres como fw-palencia-01 o edge-madrid-01 contienen información operativa útil sin depender de recordar direcciones IP.

El dominio local debe formar parte de un diseño DNS consciente. No es recomendable inventar nombres que entren en conflicto con dominios públicos reales de terceros. Si la organización controla un dominio, puede usar un subdominio interno bien definido.

Elemento	Ejemplo	Criterio
Hostname	fw-sede01	Breve, estable y reconocible.
Dominio interno	infra.ejemplo.es	Bajo un espacio de nombres controlado.
FQDN	fw-sede01.infra.ejemplo.es	Útil para certificados, DNS y monitorización.
Zona horaria	Europe/Madrid	Los logs deben reflejar el contexto operativo real.

15.3. Hora: un requisito de seguridad, no decoración

Una hora incorrecta rompe la interpretación de logs y puede afectar a TLS, autenticación, certificados, VPN y correlación de eventos. Por eso la zona horaria y NTP deben configurarse desde el comienzo.

Qué ocurre realmente

Cuando una VPN falla por un certificado 'todavía no válido' o 'ya caducado', el problema puede ser el reloj del firewall. La criptografía confía en intervalos temporales; una hora errónea puede invalidar una credencial correcta.

15.4. WAN: confirmar antes de endurecer

La configuración WAN debe reflejar la realidad del proveedor: DHCP, estática o PPPoE, y eventualmente VLAN del operador. Antes de añadir reglas avanzadas, conviene comprobar cuatro cosas: dirección asignada, prefijo, puerta de enlace y resolución DNS.

```
WAN válida = enlace + dirección + ruta por defecto + resolución
No basta con que el LED del puerto esté encendido.
```

15.5. LAN: dejar de depender del valor de fábrica

Si 192.168.1.0/24 no pertenece al plan definitivo, este es el momento de cambiarlo. Tras modificar la LAN, el equipo desde el que administramos puede conservar una concesión DHCP antigua. Será necesario renovar su dirección o reconectar la interfaz.

La LAN de administración no tiene por qué ser la red de usuarios definitiva. En instalaciones más maduras puede reservarse una VLAN de gestión para firewall, switches, AP, hipervisores y controladoras. El primer día, sin embargo, necesitamos una ruta sencilla y controlada para terminar el despliegue.

15.6. No abrir la WebGUI en WAN

Exponer la administración del firewall directamente a Internet para 'poder terminar desde casa' crea una superficie innecesaria en el momento más delicado del despliegue. El acceso remoto debe diseñarse mediante VPN o mecanismos de gestión específicamente protegidos.

En producción

La regla más segura para la administración inicial es simple: WebGUI solo desde redes de gestión autorizadas. Si aún no existe una VPN administrativa, se termina la configuración localmente antes de plantear acceso remoto.

15.7. Usuarios y principio de mínimo privilegio

La cuenta administrativa principal no debería convertirse en la identidad cotidiana de todos los técnicos. A medida que el entorno crece, conviene crear usuarios nominativos, grupos y permisos acordes con las tareas reales.

Esto mejora trazabilidad: un cambio asociado a 'admin' dice poco; un cambio realizado por una identidad individual permite reconstruir quién actuó, cuándo y con qué responsabilidad.

Capítulo 16. Servicios base: DNS, DHCP, actualización y administración

Una vez que WAN y LAN están correctamente definidas, aparece una tentación habitual: instalar inmediatamente paquetes, IDS/IPS, bloqueadores, VPN y decenas de reglas. Conviene resistirla. Primero debemos demostrar que el firewall base funciona de manera predecible.

16.1. DHCP: el primer servicio que ven muchos clientes

DHCP no solo asigna una dirección IP. Entrega al cliente una combinación de parámetros que condiciona su conectividad: máscara/prefijo, puerta de enlace, servidores DNS y duración de la concesión.

Dato DHCP	Función
Dirección IP	Identidad temporal del cliente en la subred.
Máscara/prefijo	Define qué destinos considera locales.
Gateway	Indica dónde enviar tráfico fuera de la subred.
DNS	Indica quién resolverá nombres.
Lease	Determina durante cuánto tiempo mantiene la concesión.

Qué ocurre realmente
Un PC puede tener 'Internet' por IP y, sin embargo, parecer desconectado si DNS falla. Por eso las pruebas iniciales deben separar conectividad IP de resolución de nombres.

16.2. DNS Resolver: separar nombre y transporte

pfSense activa un servicio de resolución DNS que puede atender a los clientes internos. En esta etapa interesa comprobar que el firewall puede resolver nombres y que los clientes pueden consultarlo. Las decisiones avanzadas —DNSSEC, overrides, split DNS, servidores específicos por dominio— se abordarán más adelante.

```
Prueba 1: alcanzar una IP externa
Prueba 2: resolver un nombre
Si 1 funciona y 2 falla → investigar DNS, no NAT.
```

16.3. NTP y zona horaria

Además del propio firewall, puede ser útil que equipos internos utilicen una fuente de tiempo coherente. No debemos confundir la zona horaria —cómo se presenta la hora— con NTP —cómo se sincroniza el reloj—.

En una infraestructura con logs centralizados, SIEM o correlación entre firewalls, servidores y switches, una diferencia de varios minutos puede convertir una investigación de incidentes en un rompecabezas.

16.4. Actualizar antes de complicar

La primera ventana de mantenimiento es un buen momento para comprobar si la rama instalada tiene actualizaciones. Un firewall recién desplegado debería iniciar su vida operativa con una versión soportada y con las correcciones correspondientes, salvo que exista un motivo de compatibilidad documentado para no hacerlo.

Actualizar no es un gesto mecánico. Antes de cualquier cambio de versión debemos conocer el estado actual, leer las notas de la versión, disponer de una copia reciente de configuración y tener acceso a consola por si la WebGUI no vuelve.

En producción
La combinación correcta es: backup → comprobar acceso a consola → revisar cambio → actualizar → validar. Nunca 'actualizar y esperar que todo siga igual'.

16.5. El orden importa

Orden recomendado	Motivo
1. Red básica	Sin direccionamiento y routing válidos no hay base fiable.
2. Hora y DNS	Muchos servicios superiores dependen de ambos.
3. Credenciales/usuarios	Protege la administración antes de ampliar superficie.
4. Actualización	Reduce partir de una base obsoleta.
5. Backup	Captura un estado limpio y recuperable.
6. Servicios avanzados	VPN, IDS/IPS, paquetes, HA y políticas complejas llegan después.

16.6. SSH: activar solo con propósito

SSH está desactivado inicialmente. No hay mérito en activarlo 'por si acaso'. Si una operación, automatización o soporte lo necesita, debe habilitarse con un propósito concreto, preferiblemente limitado a redes de gestión y con autenticación robusta.

Seguridad
Cada servicio administrativo habilitado aumenta superficie de exposición. La pregunta no es '¿puedo activarlo?', sino '¿qué necesidad resuelve y desde qué redes podrá alcanzarse?'.

16.7. Registrar el estado base

Antes de añadir complejidad, conviene guardar una pequeña ficha de estado. Esta ficha será la fotografía lógica del firewall en el momento en que sabemos que el sistema base funciona.

Comprobación	Resultado esperado
Versión instalada	Registrada con fecha.
WAN	IP/prefijo/gateway conocidos.
LAN	IP/prefijo definitivos o provisionales documentados.
DNS	Resolución desde firewall y cliente.
NTP	Hora y zona correctas.
GUI	Acceso HTTPS desde red autorizada.
SSH	Desactivado salvo necesidad documentada.
Backup	Archivo descargado y almacenado fuera del firewall.

16.8. Package Manager: ampliar sin convertir el firewall en un servidor generalista

El sistema de paquetes permite añadir funciones como WireGuard, FRR, Suricata, Snort, pfBlockerNG, FreeRADIUS, HAProxy o herramientas de diagnóstico. Esa extensibilidad es una ventaja, pero cada paquete añade código, dependencias, procesos, configuración y una superficie que también debe mantenerse.

La práctica recomendada es instalar únicamente paquetes del repositorio oficial que respondan a una necesidad concreta, revisar su compatibilidad antes de una actualización y mantener el número de extensiones en el mínimo razonable. Configurar repositorios externos o instalar paquetes ajenos al ecosistema soportado puede dañar la base del sistema y complicar futuras actualizaciones.

Capítulo 17. La primera copia de seguridad y la puesta en servicio

Un firewall no está correctamente instalado hasta que sabemos cómo recuperarlo. La copia de seguridad debe formar parte del proceso de puesta en servicio, no de una lista de tareas para 'más adelante'.

17.1. config.xml como núcleo de recuperación

pfSense almacena su configuración principal en formato XML, en /conf/config.xml. A partir de ese modelo, el sistema genera gran parte de los archivos de ejecución y el comportamiento de servicios. Esto permite reconstruir un equipo nuevo a partir de una copia de configuración en muchos escenarios.

La consecuencia práctica es clara: después de una modificación importante debe existir una copia externa. Guardarla únicamente en el mismo SSD del firewall no es una estrategia de backup.

Idea clave
Una copia no es 'tener el archivo'. Una copia útil debe estar fuera del firewall, identificada, protegida, recuperable y periódicamente probada.

17.2. Copia manual inicial

La interfaz de administración permite descargar la configuración como XML. Para este primer hito de la puesta en servicio interesa una copia completa, no solo de una sección.

1. Confirmar que el firewall se encuentra en un estado estable.
2. Descargar una copia completa de la configuración.
3. Guardar el archivo en un repositorio externo controlado.
4. Registrar versión de pfSense, fecha y motivo del backup.
5. Proteger el archivo porque contiene información sensible de la infraestructura.
6. Crear una segunda copia si el entorno es crítico.

Seguridad
Un config.xml puede contener direcciones, reglas, usuarios, certificados, claves o secretos relacionados con servicios. Debe tratarse como material confidencial, no como un fichero de texto inocuo.

17.3. Historial local y copias remotas

pfSense mantiene un historial de configuraciones que permite retroceder cambios recientes. Es muy útil para errores pequeños, pero sigue residiendo en el propio firewall. No sustituye una copia externa.

El servicio AutoConfigBackup permite almacenar versiones cifradas fuera del dispositivo. Puede ser una capa adicional de recuperación, pero su contraseña de cifrado debe conservarse cuidadosamente: una copia cifrada sin la clave correcta es, en la práctica, una copia inutilizable.

Mecanismo	Ventaja	Límite
Historial local	Reversión rápida de cambios recientes	Depende del propio firewall/almacenamiento.
XML descargado	Independiente, portable y controlable	Requiere disciplina de almacenamiento y custodia.
AutoConfigBackup	Automatiza copias externas cifradas	Depende de clave de cifrado y del servicio remoto.
Restauración durante instalación	Acelera recuperación/reinstalación	Debe prepararse y probarse con anterioridad.

17.4. La prueba de restauración

Un backup que jamás se ha restaurado es una promesa, no una evidencia. En un entorno de laboratorio o una VM aislada puede verificarse periódicamente que la configuración se importa, que las interfaces se reasignan cuando cambia el hardware y que los servicios esperados reaparecen.

No es necesario provocar un desastre en producción. Puede construirse una VM temporal, restaurar la configuración sin conectarla a las mismas redes y observar el proceso. Esto también ayuda a descubrir dependencias invisibles, como paquetes adicionales o nombres de interfaz distintos.

17.5. Checklist de puesta en servicio

Área	Validación
Física/virtual	Puertos/vNIC y bridges documentados; medio de instalación retirado.
WAN	Dirección, gateway y conectividad externa validados.
LAN	Subred correcta, sin solapamientos y con acceso administrativo.
Firewall/NAT	Cliente LAN puede salir; no hay exposición WAN no prevista.
DHCP	Entrega dirección, gateway y DNS correctos.
DNS	Resolución desde firewall y cliente.
Hora	Zona horaria y sincronización correctas.

Área	Validación
Administración	Password propio, usuarios previstos, GUI solo desde redes autorizadas.
Actualización	Estado de versión revisado.
Backup	Copia externa realizada y ubicación registrada.
Consola	Existe un camino conocido para recuperar acceso.

17.6. Laboratorio integral: de cero a firewall base

El siguiente laboratorio reúne lo aprendido sin convertirlo en una receta rígida. El objetivo es poder explicar cada decisión y demostrar el resultado con pruebas.

Escenario

Elemento	Valor del laboratorio
WAN	DHCP desde router de laboratorio 172.16.50.0/24
LAN	10.20.0.1/24
DHCP LAN	10.20.0.100–10.20.0.199
Firewall	VM en Proxmox con dos interfaces VirtIO
Administración	Portátil/VM conectado únicamente al bridge LAN
Objetivo	Instalar, actualizar, asegurar administración y crear backup base

Fase A — Preparación

1. Crear o verificar dos redes virtuales: una para WAN y otra para LAN.
2. Anotar MAC de cada vNIC.
3. Montar la ISO oficial del instalador.
4. Asignar recursos suficientes para el laboratorio.
5. Confirmar que la WAN del laboratorio tiene salida a Internet.
6. Comprobar que la LAN no está conectada accidentalmente a la red corporativa.

Fase B — Instalación

1. Arrancar desde la ISO.
2. Verificar que aparecen disco y dos interfaces.
3. Asociar WAN con la vNIC/bridge upstream utilizando MAC y enlace como referencia.
4. Configurar conectividad requerida por el instalador.
5. Instalar en el disco virtual.
6. Reiniciar y desmontar la ISO.

Fase C — Primer arranque

1. Confirmar asignaciones WAN y LAN desde la consola.
2. Cambiar LAN a 10.20.0.1/24 si aún conserva la red por defecto.
3. Habilitar un rango DHCP de laboratorio.
4. Conectar el equipo de administración al lado LAN.
5. Renovar dirección y verificar que recibe un valor 10.20.0.x.

Fase D — Configuración base

1. Acceder por HTTPS a la dirección LAN.
2. Cambiar la contraseña administrativa.
3. Asignar hostname, dominio operativo y zona horaria.
4. Confirmar WAN, DNS y hora.
5. Revisar actualizaciones disponibles según la rama instalada.
6. Mantener SSH desactivado si no existe una necesidad concreta.

Fase E — Validación

1. Cliente → ping/gateway LAN
2. Firewall → gateway WAN
3. Firewall → IP externa
4. Firewall → resolver nombre
5. Cliente → IP externa
6. Cliente → nombre DNS
7. Navegación HTTP/HTTPS
8. Verificar que no existe administración expuesta en WAN

Fase F — Punto de restauración

1. Descargar config.xml completo.
2. Guardar una copia con fecha y versión.
3. Registrar topología y MAC de las interfaces.
4. Anotar cualquier ajuste específico del hipervisor, como offloading en VirtIO si corresponde.
5. Cerrar el laboratorio con una prueba de reinicio y una nueva validación.

Resultado esperado

Al terminar no tendremos 'pfSense configurado del todo'. Tendremos algo más importante: una base conocida, documentada, actualizable y recuperable sobre la que construir reglas, NAT, VLAN, routing, VPN y servicios avanzados sin mezclar problemas.

Capítulo 18. Diagnóstico del primer día

Los primeros fallos suelen pertenecer a pocas familias. Aprender a clasificarlos evita reinstalar por reflejo.

Problema	Pregunta diagnóstica	Herramienta
No abre WebGUI	¿El cliente está realmente en la LAN y tiene IP compatible?	ipconfig/ip, ping, consola.
No hay Internet	¿WAN tiene IP y gateway?	Status/interfaces, routing, ping desde firewall.
IP funciona, nombre no	¿DNS resuelve desde firewall y cliente?	Diagnostics DNS Lookup / consultas DNS.
Cliente sin IP	¿DHCP está activo y la red es la correcta?	Lease, captura/estado DHCP, IP estática temporal.
Tras cambio de LAN pierdo GUI	¿El cliente conserva concesión anterior?	Renovar DHCP/reconectar.
VM pasa tráfico de forma errática	¿Modelo de vNIC/offloading/bridge es correcto?	Hipervisor + System > Advanced > Networking.
WAN y LAN parecen mezcladas	¿Se asignaron al revés?	MAC, enlace, consola Assign Interfaces.
Actualización falla	¿Hay DNS, ruta, espacio y rama válidos?	Logs, ping/DNS, estado de actualización.

18.1. Diagnosticar por capas

La secuencia más eficaz es ir de lo simple a lo complejo. Una regla de firewall no puede arreglar un cable sin enlace; cambiar DNS no corrige una puerta de enlace inexistente.

Capa física/virtual → interfaz → IP/prefijo → gateway/ruta → firewall/NAT → DNS → aplicación

Método
No cambies tres cosas a la vez. Formula una hipótesis, realiza una prueba que pueda confirmarla o descartarla, cambia una sola variable y vuelve a medir.

18.2. Cuándo NO reinstalar

Una WebGUI inaccesible, una LAN mal direccionada o interfaces intercambiadas rara vez justifican reinstalar. La consola existe precisamente para recuperar esos escenarios. Reinstalar puede borrar la evidencia del fallo y añadir uno nuevo.

- No reinstalar por una IP LAN incorrecta.

- No reinstalar por olvidar qué NIC es WAN.
- No reinstalar por un fallo DNS.
- No reinstalar por una regla que bloquea administración si existe consola y backup.
- Considerar reinstalación cuando el sistema base o el almacenamiento están dañados, o cuando se desea una reconstrucción controlada con restauración de configuración.

Cierre de la Parte III

Esta parte ha convertido el diseño de la Parte II en un firewall base operativo. El valor no está en haber recorrido un instalador, sino en haber establecido una forma de trabajar: preparar, instalar, identificar, asegurar, validar y respaldar.

A partir de aquí el sistema ya puede convertirse en una arquitectura de red real. La Parte IV entrará en direccionamiento, routing, gateways, VLAN, bridges, LAGG, IPv4 e IPv6. Ya no estaremos construyendo simplemente un firewall: estaremos construyendo la topología que atravesará.

Antes de pasar a la Parte IV
Debe existir una topología documentada, acceso de consola, WAN y LAN funcionales, DNS y hora correctos, administración protegida, versión revisada y una copia externa de configuración. Si falta una de estas piezas, conviene resolverla antes de añadir complejidad.

Glosario de la Parte III

Término	Definición en el contexto del libro
Installer	Entorno temporal que prepara y despliega el sistema en el almacenamiento de destino.
WAN	Interfaz o zona orientada al upstream/Internet, no un sinónimo universal de 'puerto 1'.
LAN	Red interna inicial desde la que suele realizarse la administración.
WebGUI	Interfaz web principal de administración de pfSense.
config.xml	Archivo XML que contiene la configuración principal del sistema.
DHCP	Protocolo que entrega parámetros de red a los clientes.
DNS Resolver	Servicio que resuelve nombres para el firewall y/o clientes internos.
NTP	Protocolo utilizado para sincronizar el reloj.

Término	Definición en el contexto del libro
Gateway	Siguiente salto utilizado para alcanzar redes no directamente conectadas.
VirtIO	Dispositivos paravirtualizados habituales en KVM/Proxmox.
Console	Interfaz local/serie/virtual de administración disponible incluso sin WebGUI.
ACB	AutoConfigBackup, servicio de copias de configuración cifradas fuera del dispositivo.

Fuentes técnicas de contraste

Las siguientes fuentes oficiales se han utilizado para verificar valores por defecto, comportamiento del instalador, opciones de recuperación y particularidades de virtualización. Verificación técnica: 8 de octubre de 2026.

- **Netgate Installer:** https://docs.netgate.com/pfsense/en/latest/install/netinstaller.html
- **Download Installation Media:** https://docs.netgate.com/pfsense/en/latest/install/download-installer-image.html
- **Installation Walkthrough:** https://docs.netgate.com/pfsense/en/latest/install/install-walkthrough.html
- **Perform the Installation:** https://docs.netgate.com/pfsense/en/latest/install/install-pfsense.html
- **Assign Interfaces:** https://docs.netgate.com/pfsense/en/latest/install/assign-interfaces.html
- **Configuration / Connecting to the GUI:** https://docs.netgate.com/pfsense/en/latest/config/
- **Setup Wizard:** https://docs.netgate.com/pfsense/en/latest/config/setup-wizard.html
- **Console Menu Basics:** https://docs.netgate.com/pfsense/en/latest/config/console-menu.html
- **XML Configuration File:** https://docs.netgate.com/pfsense/en/latest/config/xml-configuration-file.html
- **Backup and Recovery:** https://docs.netgate.com/pfsense/en/latest/backup/
- **Making Backups in the GUI:** https://docs.netgate.com/pfsense/en/latest/backup/configuration.html
- **Restoring from Backups:** https://docs.netgate.com/pfsense/en/latest/backup/restore.html
- Packages / Package Manager: https://docs.netgate.com/pfsense/en/latest/packages/index.html
- Package Manager: https://docs.netgate.com/pfsense/en/latest/packages/manager.html
- **AutoConfigBackup:** https://docs.netgate.com/pfsense/en/latest/backup/acb.html
- **Virtualizing with Proxmox VE:** https://docs.netgate.com/pfsense/en/latest/recipes/virtualize-proxmox-ve.html
- **Virtualizing with Hyper-V:** https://docs.netgate.com/pfsense/en/latest/recipes/virtualize-hyper-v.html
- **Virtualizing with VMware vSphere / ESXi:** https://docs.netgate.com/pfsense/en/latest/recipes/virtualize-esxi.html

pfSense® software

REDES, FIREWALL Y SEGURIDAD

Arquitectura, administración y laboratorios prácticos

PARTE IV

Direccionamiento, IPv4/IPv6, interfaces lógicas y routing

Oscar de la Cuesta

palentino.es



Primera edición · octubre de 2026

Punto de partida de esta parte

La Parte III dejó un pfSense instalado, accesible, actualizado y con una primera copia de configuración. Esta Parte IV cambia el foco: dejamos de pensar en un dispositivo aislado y comenzamos a construir una red. A partir de ahora cada dirección, prefijo, gateway, VLAN o ruta representa una decisión arquitectónica.

El objetivo de estas páginas no es enseñar a rellenar campos de una interfaz web. El lector debe terminar siendo capaz de mirar una tabla de rutas, una máscara, una VLAN etiquetada o un prefijo IPv6 y anticipar por dónde intentará circular un paquete. Esa capacidad es la base del troubleshooting avanzado que llegará más adelante.

> Criterio de esta parte
> Las fuentes de Netgate se utilizan para comprobar el comportamiento actual de pfSense. Los ejemplos, diagramas lógicos, ejercicios y laboratorios siguen la secuencia didáctica de este libro.

Qué aprenderemos

- Pensar en redes como conjuntos de prefijos y caminos, no como listas de direcciones aisladas.
- Dimensionar IPv4 con CIDR y comprender qué representa realmente una máscara.
- Entender IPv6 sin tratarlo como un IPv4 “más largo”: link-local, global, ULA, RA, DHCPv6 y Prefix Delegation.
- Separar interfaz física, interfaz lógica, red y zona de seguridad.
- Interpretar la tabla de rutas, los gateways y las rutas estáticas.
- Distinguir routing normal de policy routing, dejando preparado el terreno para Multi-WAN y VPN.
- Diseñar VLAN, trunk y puertos access con una nomenclatura consistente.
- Comprender LAGG, bridge, MTU y MSS sin utilizarlos como “botones de rendimiento”.
- Construir un diseño completo de pyme segmentada y demostrar su conectividad por etapas.

Capítulo 19. Direcciones, prefijos y decisiones de encaminamiento

Una dirección IP por sí sola dice muy poco. Para saber qué hará un host con un destino necesitamos conocer también el prefijo de su interfaz, las rutas existentes y, cuando ninguna ruta más específica coincide, el gateway por defecto.

Destino → buscar la ruta más específica → elegir interfaz/siguiente salto → resolver vecino → transmitir

La ruta más específica gana: /32 antes que /24; /24 antes que /16; /16 antes que /0.

19.1. El prefijo responde a una pregunta

El prefijo define qué parte de una dirección identifica la red y, por tanto, qué destinos se consideran directamente alcanzables por esa interfaz. En IPv4 solemos expresarlo como /24, /27 o /30; en IPv6, como /64, /56 o /48. La idea es idéntica aunque los mecanismos de descubrimiento de vecinos sean distintos.

Concepto	Pregunta que responde
Dirección	¿Qué identidad tiene esta interfaz dentro del prefijo?
Prefijo	¿Qué conjunto de direcciones pertenece a esta red?
Gateway	¿A qué router envío destinos que no están directamente conectados?
Ruta	¿Qué prefijo se alcanza por qué interfaz o siguiente salto?
Métrica/prioridad	¿Qué camino prefiero cuando existen alternativas comparables?

Qué ocurre realmente
Cuando un PC envía tráfico a 10.20.30.50/24 desde 10.20.30.10/24, no necesita preguntarle al gateway. Primero determina que el destino está dentro de su red local y busca al vecino directamente. El gateway solo participa cuando la tabla de rutas indica que el destino está fuera del enlace.

19.2. pfSense conoce automáticamente sus redes conectadas

Cuando asignamos 10.20.30.1/24 a una interfaz LAN, el sistema crea una ruta conectada hacia 10.20.30.0/24. No es necesario añadir una ruta estática hacia una red que ya está directamente unida al firewall. Hacerlo suele indicar que el modelo mental de routing todavía no está claro.

LAN = 10.20.30.1/24
→ ruta conectada: 10.20.30.0/24 por LAN

WAN = 198.51.100.10/24
→ ruta conectada: 198.51.100.0/24 por WAN

19.3. El principio de máxima especificidad

Los routers no eligen rutas por intuición ni por el nombre de la interfaz. Comparan el destino con los prefijos de la tabla y escogen la coincidencia más específica. Por eso una ruta 10.20.30.0/24 puede coexistir con 10.0.0.0/8: para un destino 10.20.30.50 se utilizará la /24.

Ruta	Coincide con 10.20.30.50	Preferencia
10.20.30.0/24	Sí	1ª: más específica
10.20.0.0/16	Sí	2ª
10.0.0.0/8	Sí	3ª
0.0.0.0/0	Sí	Último recurso

Error frecuente
Crear rutas estáticas “por si acaso” hacia redes ya conectadas. Una tabla de rutas llena de excepciones innecesarias hace más difícil diagnosticar y puede ocultar un diseño deficiente.

Capítulo 20. IPv4 y subnetting aplicado al firewall

El subnetting se vuelve realmente útil cuando deja de ser un ejercicio académico y se relaciona con decisiones de diseño: cuántos hosts necesito, cuánto quiero aislar, qué tamaño de broadcast domain tolero y cuánto espacio quiero reservar para crecer.

20.1. CIDR como forma de pensar

En IPv4 existen 32 bits. El prefijo indica cuántos pertenecen a la parte de red. Un /24 deja 8 bits para host; un /27 deja 5; un /30 deja 2. No es necesario convertir todas las redes a binario a diario, pero sí comprender qué significa aumentar o reducir el prefijo.

Prefijo	Máscara	Direcciones totales	Uso típico orientativo
/24	255.255.255.0	256	LAN de tamaño medio / laboratorio cómodo
/25	255.255.255.128	128	Dividir un /24 en dos segmentos
/26	255.255.255.192	64	Zona de servidores o usuarios pequeña
/27	255.255.255.224	32	Gestión, voz o grupo reducido
/28	255.255.255.240	16	Segmento muy pequeño
/30	255.255.255.252	4	Enlaces IPv4 punto a punto clásicos
/32	255.255.255.255	1	Una dirección/host específico

En Ethernet IPv4 tradicional no todas las direcciones del bloque se asignan a hosts: la primera identifica la red y la última es broadcast. Sin embargo, reglas especiales como /31 para enlaces punto a punto existen en estándares modernos. En este libro trabajaremos primero con los casos más habituales y luego veremos excepciones cuando aporten valor.

20.2. Cómo calcular sin depender de una calculadora

Para un /27, quedan 5 bits de host: 2^5 = 32 direcciones por subred. El tamaño del bloque en el último octeto es 32, por lo que los comienzos son 0, 32, 64, 96, 128, 160, 192 y 224.

```
192.168.50.64/27
Red:       192.168.50.64
Hosts:     192.168.50.65 - 192.168.50.94
Broadcast: 192.168.50.95
Siguiente: 192.168.50.96/27
```

20.3. Subred no es igual a VLAN

Una subred es un concepto de capa 3. Una VLAN es un mecanismo de capa 2 para crear dominios de broadcast separados sobre infraestructura compartida. En un diseño típico se asigna una subred diferente a cada VLAN, pero son conceptos distintos y conviene mantenerlos separados mentalmente.

Idea clave
"VLAN 20" no significa "192.168.20.0/24". Es una convención frecuente, no una ley técnica. Podemos decidir que VLAN 20 use 10.40.8.0/23 si el plan de direccionamiento lo exige.

20.4. Redes privadas RFC1918 y solapamientos

Los tres grandes bloques privados IPv4 son 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16. Su reutilización permite construir redes internas sin consumir direcciones públicas, pero crea un problema operativo muy frecuente: dos organizaciones, sedes o VPN pueden haber elegido el mismo espacio.

Bloque privado	Rango aproximado	Comentario
10.0.0.0/8	10.0.0.0 – 10.255.255.255	Gran flexibilidad para planes jerárquicos.
172.16.0.0/12	172.16.0.0 – 172.31.255.255	Útil para evitar los 192.168.x.x más comunes.
192.168.0.0/16	192.168.0.0 – 192.168.255.255	Muy utilizado por routers domésticos; más propenso a colisiones en VPN.

En producción
Al diseñar una empresa con futuras VPN, evita llenar todas las sedes con 192.168.1.0/24. Un plan jerárquico —por ejemplo, 10.<sede>.<zona>.0/24— facilita rutas, agregación y troubleshooting.

20.5. Plan jerárquico de ejemplo

Sede/Zona	Red	Gateway pfSense
Sede 1 - Gestión	10.11.10.0/24	10.11.10.1
Sede 1 - Usuarios	10.11.20.0/23	10.11.20.1
Sede 1 - Servidores	10.11.30.0/24	10.11.30.1
Sede 1 - IoT	10.11.40.0/24	10.11.40.1

Sede/Zona	Red	Gateway pfSense
Sede 2 - Gestión	10.12.10.0/24	10.12.10.1
Sede 2 - Usuarios	10.12.20.0/23	10.12.20.1

La ventaja no es estética. Si una futura VPN necesita anunciar todas las redes de Sede 1, un esquema bien reservado puede permitir resumir rutas. La planificación evita que años de crecimiento conviertan el direccionamiento en una colección de excepciones.

Capítulo 21. IPv6 sin pensar como si fuera IPv4

IPv6 no es simplemente “IPv4 con direcciones más largas”. Cambian el tamaño del espacio, el descubrimiento de vecinos, la autoconfiguración y la relación entre direcciones de enlace, globales y prefijos delegados. En pfSense esto se refleja en varias formas de configurar una interfaz: estática, DHCPv6, Track Interface y otros mecanismos específicos.

21.1. 128 bits y prefijos

Una dirección IPv6 tiene 128 bits y normalmente se representa en ocho grupos hexadecimales. Los ceros iniciales pueden omitirse y una secuencia continua de grupos cero puede abreviarse una vez mediante ::.

```
2001:0db8:0000:0010:0000:0000:0000:0042
→ 2001:db8:0:10::42
```

21.2. Tipos de dirección que debemos reconocer

Tipo	Ejemplo conceptual	Uso
Link-local	fe80::/10	Existe en cada enlace; vecino, RA y funciones locales.
Global Unicast	2000::/3	Direcciones globalmente enrutable asignadas por proveedor/organización.
ULA	fc00::/7 (habitualmente fd00::/8)	Espacio local no destinado a Internet público.
Multicast	ff00::/8	Sustituye múltiples usos de broadcast; grupos específicos.
Loopback	::1/128	El propio host.
Unspecified	::/128	Ausencia de dirección / origen durante procesos concretos.

Idea clave
En IPv6 no existe el broadcast IPv4 tradicional. Muchas funciones de descubrimiento se apoyan en multicast e ICMPv6. Bloquear ICMPv6 indiscriminadamente rompe mecanismos esenciales.

21.3. Link-local no significa “dirección defectuosa”

Una interfaz IPv6 puede utilizar una dirección fe80:: aunque también tenga una dirección global. Las link-local son fundamentales en Neighbor Discovery y Router Advertisements. En muchos escenarios, el siguiente salto IPv6 se identifica precisamente mediante una dirección link-local.

21.4. SLAAC, RA y DHCPv6

En IPv6 el router puede anunciar información mediante Router Advertisements. Un cliente puede formar su dirección mediante SLAAC, recibir datos adicionales mediante DHCPv6 o utilizar una combinación de mecanismos. Esto difiere de IPv4, donde DHCP suele entregar también el gateway por defecto.

```
Router Advertisement (RA) → “este prefijo existe y yo soy router”
SLAAC → el host forma una dirección dentro del prefijo
DHCPv6 → puede aportar dirección y/u otros parámetros según el diseño
```

Qué ocurre realmente

La puerta de enlace IPv6 no llega normalmente como una opción DHCPv6 equivalente a la de IPv4. El host aprende routers mediante Router Advertisements. Por eso un DHCPv6 correcto no compensa un RA ausente cuando el diseño lo necesita.

21.5. Prefix Delegation y Track Interface

Muchos ISP no entregan solo una dirección a la WAN. Delegan un prefijo —por ejemplo /56 o /60 — que el firewall puede subdividir y anunciar en sus redes internas. pfSense puede recibir ese prefijo por DHCPv6-PD y hacer que interfaces internas “sigan” a la WAN mediante Track Interface.

```
ISP delega /56 → pfSense WAN recibe/gestiona delegación
        ├─ LAN usuarios: /64
        ├─ VLAN servidores: /64
        ├─ VLAN IoT: /64
        └─ VLAN invitados: /64
```

La longitud exacta que delega cada ISP varía. La información válida debe obtenerse del proveedor porque incluso un mismo operador puede utilizar parámetros distintos según región o tecnología de acceso.

21.6. Por qué /64 es especial en una LAN IPv6

Aunque IPv6 permite muchas longitudes de prefijo, /64 es el tamaño normal de una red de hosts que utiliza SLAAC y Neighbor Discovery. Usar prefijos más pequeños o más grandes sin comprender las consecuencias puede romper expectativas del protocolo y compatibilidad de clientes.

21.7. Dual stack y diagnóstico

Durante muchos años coexistirán IPv4 e IPv6. Eso significa que un cliente puede llegar a un servicio por un protocolo y fallar por el otro. Una prueba de conectividad debe especificar qué familia se está validando.

“Funciona Internet” es ambiguo.
Prueba IPv4 → ruta, DNS A, NAT si existe
Prueba IPv6 → prefijo, RA, ruta, DNS AAAA, firewall; normalmente sin NAT tradicional

Error frecuente

Desactivar IPv6 porque “no lo usamos” sin confirmar qué hace el ISP, el sistema operativo o las aplicaciones. La alternativa profesional es decidir conscientemente si se desplegará IPv6 y, si no, deshabilitarlo de forma coherente en el diseño.

Capítulo 22. Interfaces físicas, virtuales y lógicas

pfSense puede enrutar sobre una NIC física, una VLAN, un LAGG, un bridge, una interfaz de túnel o una interfaz virtual. Para diseñar bien conviene separar tres ideas: el dispositivo que transporta bits, la interfaz lógica que ve el sistema y el rol de seguridad que asignamos a esa interfaz.

NIC/puerto → interfaz FreeBSD → constructo lógico (VLAN/LAGG/bridge/túnel) → asignación pfSense → zona/rol

22.1. Asignar no es crear

Crear una VLAN no la convierte automáticamente en una interfaz con dirección IP, reglas y servicios. Primero existe como interfaz lógica; después se asigna en Interfaces > Assignments; entonces puede habilitarse, nombrarse y recibir IPv4/IPv6.

La misma idea se aplica a un LAGG o un bridge: construir el objeto de capa 2 y asignarlo como interfaz son acciones distintas. Esta separación es útil porque una interfaz lógica puede servir como “padre” de otras sin necesitar una IP propia.

22.2. Nombres que describen función

Nombre pobre	Nombre mejor	Qué aporta
OPT1	SERVERS	Se reconoce en reglas y logs.
OPT2	IOT	Expresa la zona, no el orden de creación.
OPT3	GUEST	Reduce errores humanos.
VLAN20	USERS_V20	Combina función y referencia técnica.

En producción
Los nombres de interfaz aparecen en reglas, DHCP, gráficos y diagnóstico. Renombrar OPT1 antes de crear cincuenta reglas cuesta segundos; hacerlo después de años de operación cuesta atención y riesgo.

22.3. IPv4/IPv6 upstream gateway solo donde corresponde

En una interfaz interna no se configura un upstream gateway como si fuera una WAN. El firewall es el gateway de esa red. Seleccionar un gateway upstream en una interfaz interna altera cómo pfSense la interpreta y puede introducir comportamiento de tipo WAN que no deseamos.

Esto no impide crear un objeto gateway asociado a un router interno para usarlo en rutas estáticas. La diferencia está entre declarar “esta interfaz tiene un upstream” y “existe un router alcanzable desde esta interfaz hacia otras redes”.

22.4. MAC spoofing como excepción, no costumbre

pfSense permite cambiar la MAC presentada por una interfaz. Puede ser útil durante una migración si un upstream retiene la MAC anterior, pero debería tratarse como solución consciente a un requisito concreto. Normalmente es preferible limpiar la tabla ARP o reiniciar el CPE en lugar de perpetuar una identidad falsa sin documentarla.

Capítulo 23. Gateways, tabla de rutas y rutas estáticas

Routing es la decisión de “por dónde”. Firewalling es la decisión de “si está permitido”. Ambas ocurren en el mismo dispositivo, pero resolver una no implica resolver la otra. Una ruta puede existir y el firewall bloquear; una regla puede permitir y no existir ruta válida.

23.1. Qué es un gateway en pfSense

Un gateway representa un router directamente alcanzable a través de una interfaz y permite llegar a prefijos que no están conectados localmente. El caso más conocido es el gateway de Internet, pero también puede existir un router interno, un túnel o un peer que actúe como siguiente salto.

> **Qué ocurre realmente**
> Para usar 10.50.0.254 como gateway desde una interfaz 10.50.0.1/24, el firewall debe poder alcanzar 10.50.0.254 directamente en ese enlace. No se puede elegir como siguiente salto una dirección arbitraria que a su vez requiera otra ruta para ser encontrada.

23.2. La ruta por defecto

0.0.0.0/0 en IPv4 y ::/0 en IPv6 son las rutas menos específicas. Capturan aquello que no coincide con rutas más concretas. IPv4 e IPv6 mantienen gateways por defecto independientes: cambiar uno no cambia el otro.

```
Tabla simplificada:
10.20.0.0/24  → LAN
10.30.0.0/24  → SERVERS
172.16.0.0/16 → gateway ROUTER_INTERNO
0.0.0.0/0     → gateway WAN_GW
```

23.3. Rutas estáticas

Una ruta estática es adecuada cuando una red remota se encuentra detrás de otro router y esa topología no cambia con frecuencia. Primero se define el gateway y después la ruta de destino que utilizará ese siguiente salto.

Destino	Gateway	Lectura humana
10.60.0.0/16	10.50.0.254	Para 10.60.0.0/16, envía a router interno.
192.0.2.80/32	WAN_GW	Un host concreto debe salir por WAN.
2001:db8:2200::/48	GW6_SITE	Ese prefijo IPv6 está detrás del router indicado.

23.4. La vuelta también necesita ruta

Uno de los fallos más frecuentes en redes enrutadas es comprobar solo el camino de ida. Si pfSense sabe llegar a 10.60.1.20 a través de un router interno pero el host remoto no sabe volver a la red origen, la comunicación falla o se vuelve asimétrica.

```
IDA: 10.20.0.50 → pfSense → router interno → 10.60.1.20
VUELTA: 10.60.1.20 → ¿gateway conoce 10.20.0.0/24?
```

Método de diagnóstico

Ante un fallo de routing, dibuja ida y vuelta por separado. Escribe en cada salto qué ruta usaría el dispositivo. Si no puedes justificar un paso de la vuelta, aún no has demostrado conectividad bidireccional.

23.5. Monitorización de gateways

pfSense puede supervisar gateways y utilizar ese estado en escenarios Multi-WAN. El concepto es importante desde ahora: “interfaz arriba” no significa “camino útil”. Un enlace Ethernet puede permanecer activo mientras el router del proveedor o un destino externo es inalcanzable.

Más adelante veremos dpinger, monitor IP, gateway groups y failover. En esta Parte IV basta entender que el estado operativo de un camino no puede reducirse a mirar el LED de la NIC.

23.6. Policy routing: una excepción deliberada al routing normal

Normalmente la tabla de rutas decide el camino. pfSense permite que una regla de firewall seleccione un gateway concreto, lo que se conoce como policy routing. Es una herramienta muy potente para Multi-WAN y VPN, pero introduce una segunda fuente de decisión que debemos recordar durante el diagnóstico.

Advertencia

No uses policy routing para corregir una tabla de rutas mal diseñada. Primero construye rutas coherentes; después utiliza policy routing cuando el requisito sea “este tráfico debe usar un camino distinto al normal”.

Capítulo 24. VLAN: segmentar capa 2 sin multiplicar switches

Una VLAN crea un dominio de broadcast separado dentro de una infraestructura Ethernet compartida. El estándar 802.1Q inserta una etiqueta en las tramas que permite distinguir a qué VLAN pertenecen cuando atraviesan un enlace que transporta varias redes.

24.1. Access y trunk: roles del puerto, no marcas comerciales

Un puerto access entrega normalmente una sola VLAN al dispositivo final sin etiqueta. Un trunk transporta múltiples VLAN etiquetadas entre equipos que entienden 802.1Q, por ejemplo firewall-switch, switch-switch o switch-hipervisor.

```
PC ──[access VLAN 20]── Switch ──[trunk 10,20,30,40]── pfSense
                                  ├─ VLAN10 MGMT
                                  ├─ VLAN20 USERS
                                  ├─ VLAN30 SERVERS
                                  └─ VLAN40 IOT
```

24.2. El router-on-a-stick

Cuando una única interfaz física del firewall recibe un trunk y sobre ella se crean varias VLAN, pfSense puede enrutar entre todas esas redes. Este patrón se conoce comúnmente como router-on-a-stick. Es económico en puertos, pero el enlace físico se convierte en punto de concentración y debe dimensionarse para el tráfico agregado.

> **Idea clave**
> Dos dispositivos en VLAN distintas no se comunican entre sí en capa 2. Para hacerlo necesitan routing. Si pfSense es su gateway, el tráfico inter-VLAN atraviesa el firewall y puede filtrarse con reglas.

24.3. VLAN nativa y tramas sin etiqueta

Los fabricantes utilizan terminología diferente para el tratamiento de tramas sin etiqueta en un trunk. “Native VLAN”, “PVID”, “untagged member” y conceptos similares pueden referirse a aspectos relacionados pero no siempre idénticos. Por eso conviene documentar el comportamiento de cada extremo, no asumir que dos interfaces con el mismo número de VLAN actuarán igual.

Para reducir errores, un diseño de firewall suele ser más fácil de razonar cuando las VLAN de producción importantes viajan explícitamente etiquetadas y la red sin etiqueta se usa solo si existe un motivo claro.

24.4. Crear VLAN en pfSense: el orden conceptual

1. Elegir la interfaz padre que transportará las tramas 802.1Q.
2. Crear la VLAN con su ID/tag y descripción.
3. Asignar esa VLAN como nueva interfaz lógica.
4. Renombrar la interfaz según su función.
5. Configurar IPv4/IPv6 en esa interfaz.
6. Configurar DHCP/RA si corresponde.
7. Crear reglas de firewall para esa zona.
8. Configurar el switch para entregar o transportar esa VLAN.
9. Validar cliente → gateway antes de probar Internet o inter-VLAN.

24.5. VLAN y seguridad

La VLAN aporta separación de capa 2, pero la política de seguridad la determina el firewall y la configuración del switch. Una VLAN IoT que tiene una regla “allow any” hacia todas las redes internas no está realmente aislada en capa 3.

> **Error frecuente**
> Crear diez VLAN y copiar en todas una regla “permitir cualquiera a cualquiera”. La segmentación existe en el diagrama, pero no en la política efectiva.

24.6. Ejemplo de matriz de comunicación

Origen	Destino	Política inicial
MGMT	Firewall, switches, AP, hipervisores	Permitir administración necesaria.
USERS	Internet	Permitir según política corporativa.
USERS	SERVERS	Solo servicios corporativos necesarios.
IOT	USERS	Bloquear por defecto.
IOT	Internet	Permitir servicios mínimos necesarios.
GUEST	Redes RFC1918 internas	Bloquear.
GUEST	Internet	Permitir con controles definidos.

Esta tabla será más útil que memorizar reglas una por una. En la Parte de firewall la convertiremos en una política ordenada y verificable.

24.7. VLAN en Proxmox

En virtualización hay dos lugares donde puede “terminar” la etiqueta: el bridge/vSwitch del hipervisor o la propia VM. En un diseño trunk hacia pfSense, una vNIC puede recibir varias VLAN para que pfSense cree las subinterfaces. En otros diseños, el hipervisor presenta una vNIC distinta por red y oculta el tagging al firewall.

Modelo	Ventaja	Riesgo
Trunk a pfSense	Escalable, menos vNIC, topología parecida a hardware físico	Error de VLAN afecta varias redes; requiere dominar tagging extremo a extremo.
Una vNIC por red	Muy explícito y fácil de visualizar	Más interfaces virtuales y configuración en hipervisor.

Capítulo 25. LAGG, bridges, MTU y límites físicos

Estas funciones suelen aparecer juntas en diseños “avanzados”, pero resuelven problemas diferentes. LAGG agrupa enlaces, bridge une dominios de capa 2 y MTU define el tamaño máximo de paquete/trama que un camino admite sin fragmentación o mecanismos equivalentes.

25.1. LAGG: varios enlaces, una interfaz lógica

FreeBSD y pfSense implementan agregación mediante interfaces lagg. Dependiendo del modo puede buscar redundancia, distribución de flujos o ambas. LACP es el modo empresarial más habitual cuando el switch también lo soporta.

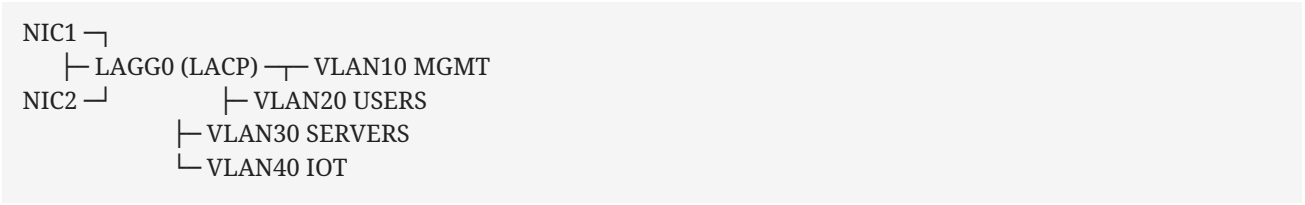
Modo conceptual	Objetivo
LACP	Negociar agregación con switch compatible; distribuir flujos y aportar redundancia.
Failover	Mantener un enlace activo y otro de respaldo.
Load Balance/Round Robin	Distribución según modo; requieren comprender compatibilidad y orden.
None	Agrupación sin protocolo de negociación específico.

Qué ocurre realmente
Un LAGG de 2×1 Gb/s no convierte una única transferencia TCP en 2 Gb/s. La distribución suele hacerse por hash de flujo; un flujo concreto normalmente queda ligado a uno de los miembros. El beneficio aparece al repartir múltiples conversaciones y al aportar redundancia.

LACP entre dos switches físicos distintos solo funciona si esos switches se presentan lógicamente como un único sistema de agregación —por ejemplo, mediante stacking o tecnología equivalente del fabricante. Conectar cada miembro a un switch independiente sin soporte conjunto no crea mágicamente alta disponibilidad.

25.2. VLAN encima de LAGG

Una arquitectura común es crear primero el LAGG y después utilizarlo como padre de varias VLAN. Así se combinan redundancia/capacidad de enlaces con segmentación lógica. Si el LAGG solo transportará VLAN, puede no necesitar una dirección IP propia.



25.3. Bridge: unir interfaces en el mismo dominio de capa 2

Un bridge hace que varias interfaces participen en el mismo dominio Ethernet. Puede ser útil en escenarios transparentes, migraciones o necesidades concretas, pero un firewall no debe convertirse por defecto en sustituto de un switch. Un bridge procesa tráfico en software y añade complejidad de filtrado.

En producción
Si la necesidad es "quiero cuatro puertos LAN iguales", normalmente la solución natural es un switch gestionado, no crear un bridge de cuatro NIC en pfSense. Usa bridge cuando exista un motivo arquitectónico, no para imitar un switch barato.

Cuando el bridge necesita una dirección IP propia, la práctica recomendada es asignar la dirección al bridge y no a uno de sus miembros. Esto evita dependencias del estado de un miembro concreto y mejora compatibilidad con funciones que esperan que la interfaz lógica sea la dueña de la IP.

25.4. MTU: tamaño máximo y camino completo

Ethernet suele trabajar con una MTU IP de 1500 bytes. PPPoE, túneles, VPN o encapsulaciones añaden cabeceras y pueden reducir el tamaño disponible. Si un extremo envía paquetes demasiado grandes para el camino, pueden aparecer fragmentación, pérdida o conexiones que funcionan para tráfico pequeño pero fallan con transferencias grandes.

Aplicación → TCP/UDP → IP → (VPN/PPPoE/VLAN...) → Ethernet
Cada encapsulación añade bytes. El camino útil queda limitado por el tramo más pequeño.

25.5. Path MTU Discovery y MSS clamping

TCP anuncia un MSS que indica cuánto payload TCP puede recibir sin necesidad de fragmentación IP. Cuando una VPN o enlace tiene una MTU inferior, limitar el MSS puede evitar que se formen segmentos demasiado grandes. pfSense dispone de opciones de MSS clamping para escenarios donde PMTUD no funciona correctamente.

Error frecuente
Bajar MTU aleatoriamente hasta que "funcione". Primero identifica el tramo que impone el límite y calcula el overhead. Un ajuste de MTU/MSS sin diagnóstico puede ocultar el problema y reducir eficiencia.

25.6. Síntomas clásicos de MTU

- Ping pequeño funciona, transferencia grande falla o se congela.
- Una web carga parcialmente y determinadas conexiones TLS se atascan.
- VPN conecta pero copiar archivos grandes es inestable.
- Upload mucho peor que download o viceversa según el camino.
- Cambiar temporalmente el tamaño de paquetes modifica el comportamiento.

Capítulo 26. Laboratorio: construir una pyme segmentada desde la tabla de rutas

Este laboratorio no empieza en la GUI. Empieza en una hoja de diseño. La meta es que cada red tenga un propósito, que cada interfaz pueda justificarse y que el lector sea capaz de predecir la ruta antes de probarla.

26.1. Escenario

Empresa de unos 70 usuarios con una sede, un switch gestionado, dos puntos de acceso y pfSense como router/firewall. El proveedor entrega IPv4 por DHCP y un prefijo IPv6 delegado /56. El enlace firewall-switch será un trunk 802.1Q.

Zona	VLAN	IPv4	IPv6 interno	Función
MGMT	10	10.20.10.0/24	/64 derivado del /56	Switches, AP, hipervisor y administración.
USERS	20	10.20.20.0/23	/64	Puestos de trabajo.
SERVERS	30	10.20.30.0/24	/64	Servicios internos.
IOT	40	10.20.40.0/24	/64	Sensores, televisores, dispositivos no confiables.
GUEST	50	10.20.50.0/24	/64	Invitados con salida a Internet.
VOICE	60	10.20.60.0/24	/64	Telefonía IP.

26.2. Paso 1: reservar el direccionamiento

Antes de crear ninguna VLAN se reserva el bloque lógico de la sede. El patrón 10.20.x.0 ayuda a reconocer que todas estas redes pertenecen al mismo emplazamiento. La red de usuarios recibe /23 porque necesita más capacidad; las demás conservan /24 para simplificar operación.

26.3. Paso 2: crear el trunk

La NIC LAN física se conecta al switch mediante un puerto trunk que permite las VLAN 10, 20, 30, 40, 50 y 60. En pfSense esa NIC actúa como padre 802.1Q. No necesita ser por sí misma la LAN de usuarios.

```
pfSense NIC-LAN ── trunk ── Switch
  ├─ VLAN10 → MGMT 10.20.10.1/24
  ├─ VLAN20 → USERS 10.20.20.1/23
  ├─ VLAN30 → SERVERS 10.20.30.1/24
  ├─ VLAN40 → IOT 10.20.40.1/24
  ├─ VLAN50 → GUEST 10.20.50.1/24
  └─ VLAN60 → VOICE 10.20.60.1/24
```

26.4. Paso 3: asignar y nombrar

1. Crear cada VLAN sobre la interfaz padre.
2. Asignar cada VLAN como interfaz.
3. Renombrar inmediatamente: MGMT, USERS, SERVERS, IOT, GUEST, VOICE.
4. Configurar IPv4 del gateway en cada una.
5. Configurar Track Interface o el esquema IPv6 elegido según la delegación del ISP.
6. Activar DHCPv4 donde proceda y definir RA/DHCPv6 según el diseño.
7. No crear todavía reglas amplias “para que funcione todo”.

26.5. Paso 4: observar la tabla de rutas

Después de crear las interfaces, pfSense debe tener rutas conectadas para todas las subredes. Eso significa que el routing entre ellas existe conceptualmente incluso antes de crear reglas de firewall. Las reglas decidirán si ese routing puede utilizarse.

```
10.20.10.0/24 → MGMT
10.20.20.0/23 → USERS
10.20.30.0/24 → SERVERS
10.20.40.0/24 → IOT
10.20.50.0/24 → GUEST
10.20.60.0/24 → VOICE
0.0.0.0/0     → WAN gateway
```

Qué ocurre realmente

La existencia de varias interfaces convierte a pfSense en router entre esas redes. El firewall stateful decide qué conversaciones pueden atravesar ese router. Por eso “crear una VLAN” y “permitir comunicación” son pasos diferentes.

26.6. Paso 5: pruebas por capas

Prueba	Qué demuestra
Cliente recibe DHCP	VLAN/access + DHCP local funcionan.
Cliente hace ping a su gateway	Capa 2 y direccionamiento local funcionan.
pfSense resuelve DNS	Conectividad del firewall y DNS funcionan.

Prueba	Qué demuestra
Cliente alcanza IP externa	Routing + firewall + NAT IPv4 funcionan.
Cliente resuelve nombre	DNS extremo a extremo funciona.
USERS intenta SERVERS	Valida política inter-VLAN, no solo routing.
GUEST intenta MGMT	Debe fallar cuando apliquemos política de aislamiento.
Cliente obtiene IPv6 y llega por IPv6	RA/prefijo/ruta/firewall IPv6 funcionan.

26.7. Añadir un router interno

Para introducir routing estático añadimos un pequeño router de laboratorio conectado a SERVERS con IP 10.20.30.254. Detrás existe la red 10.90.0.0/16. pfSense necesita un gateway interno y una ruta estática hacia ese prefijo.

```
pfSense SERVERS 10.20.30.1/24
      │
      ├── servidor 10.20.30.20
      └── router interno 10.20.30.254 ── 10.90.0.0/16

Ruta pfSense: 10.90.0.0/16 → 10.20.30.254
```

El router interno también necesita conocer las redes 10.20.x.x de retorno, ya sea mediante rutas específicas, una ruta agregada que sea válida o una ruta por defecto hacia pfSense. La ida no basta.

26.8. Matriz de verificación final

Origen	Destino	Resultado esperado con reglas de paso aplicadas
MGMT	Gateway de todas las VLAN	Conectividad de routing; la política fina llegará después.
USERS	Internet IPv4/IPv6	Operativo.
SERVERS	Internet según diseño	Operativo si se permite.
IOT	Red propia/gateway	Operativo; aislamiento se reforzará con reglas.
GUEST	Internet	Operativo; redes internas se bloquearán explícitamente.
pfSense	10.90.0.0/16	Alcanzable mediante ruta estática y retorno correcto.

Resultado del laboratorio

Al terminar, el lector debe poder dibujar la tabla de rutas sin mirar pfSense, explicar por qué cada VLAN tiene su prefijo, identificar qué interfaces son directamente conectadas y justificar cualquier ruta estática. La Parte V añadirá la política: reglas, estados, aliases, floating rules y el funcionamiento real de PF.

26.9. Diagnóstico rápido de direccionamiento y routing

Síntoma	Hipótesis inicial
Cliente no llega ni al gateway	VLAN/access, IP, máscara/prefijo, cable o interfaz.
Llega al gateway pero no a otra VLAN	Regla de firewall o ruta/retorno en topologías con routers adicionales.
Llega por IPv4 pero no IPv6	RA/DHCPv6/prefix delegation/routing o firewall IPv6.
Una red remota solo funciona en un sentido	Ruta de retorno o filtrado asimétrico.
Todo funciona salvo paquetes grandes	MTU/MSS/PMTUD.
Un único flujo no supera 1 Gb/s en LAGG 2×1G	Comportamiento esperado de hashing por flujo.
Después de añadir gateway a LAN aparecen rutas extrañas	Interfaz interna tratada como upstream; revisar diseño.

Cierre de la Parte IV

Esta Parte IV ha construido el esqueleto de red sobre el firewall: direcciones, prefijos, interfaces, VLAN, gateways y rutas. Todavía no hemos desarrollado la política de seguridad en profundidad. Esa separación es intencionada: primero debemos saber por dónde podría circular un paquete; después decidiremos si debe hacerlo.

La Parte V abordará el núcleo de pfSense como firewall: PF, estados, orden de evaluación, aliases, reglas por interfaz, floating rules, NAT y el recorrido completo de una conexión. Allí uniremos routing y seguridad en un único modelo mental.

Antes de continuar

Debes poder responder sin abrir la WebGUI: ¿qué redes están directamente conectadas?, ¿cuál es la ruta por defecto?, ¿qué gateway lleva a cada red remota?, ¿qué VLAN transporta cada zona?, ¿qué prefijo IPv6 usa cada LAN y cómo se obtiene? Si esas respuestas no están claras, las reglas de firewall serán mucho más difíciles de razonar.

Glosario de la Parte IV

Término	Definición operativa
CIDR	Notación dirección/prefijo que expresa cuántos bits identifican la red.
Ruta conectada	Ruta creada automáticamente por una interfaz que posee un prefijo.
Default route	Ruta menos específica (/0) utilizada cuando ninguna más concreta coincide.
Gateway	Siguiente salto directamente alcanzable hacia otras redes.
Static route	Entrada manual que asocia un prefijo remoto con un gateway.
Policy routing	Selección de gateway mediante una regla, por encima del camino normal esperado.
VLAN	Dominio lógico de capa 2 identificado mediante 802.1Q.
Trunk	Enlace que transporta múltiples VLAN, habitualmente etiquetadas.
Access port	Puerto que presenta normalmente una única VLAN a un dispositivo final.
LAGG	Interfaz lógica que agrupa múltiples enlaces físicos.
LACP	Protocolo de negociación de agregación de enlaces.
Bridge	Constructo de capa 2 que une interfaces en un mismo dominio.
MTU	Tamaño máximo de paquete IP admitido en una interfaz/camino sin fragmentación.
MSS	Tamaño máximo de payload TCP anunciado por un extremo.
SLAAC	Autoconfiguración IPv6 basada en Router Advertisements.
Prefix Delegation	Delegación de un bloque IPv6 a un router para subdividirlo en redes internas.
Track Interface	Mecanismo de pfSense para derivar prefijos IPv6 internos desde una interfaz que recibe delegación.

Fuentes técnicas de contraste

Las fuentes siguientes se han utilizado para verificar el comportamiento actual de pfSense, nombres de funciones y recomendaciones técnicas. Verificación técnica: 8 de octubre de 2026.

- **Interface Configuration:** https://docs.netgate.com/pfsense/en/latest/interfaces/configure.html
- **IPv6 Configuration Types:** https://docs.netgate.com/pfsense/en/latest/interfaces/configure-ipv6.html
- **Virtual LANs (VLANs):** https://docs.netgate.com/pfsense/en/latest/vlan/index.html
- **Gateways:** https://docs.netgate.com/pfsense/en/latest/routing/gateways.html
- **Static Routes:** https://docs.netgate.com/pfsense/en/latest/routing/static.html
- **LAGG (Link Aggregation):** https://docs.netgate.com/pfsense/en/latest/interfaces/lagg.html
- **Bridging:** https://docs.netgate.com/pfsense/en/latest/bridges/index.html
- **Creating a Bridge:** https://docs.netgate.com/pfsense/en/latest/bridges/create.html
- **Bridging and Interfaces:** https://docs.netgate.com/pfsense/en/latest/bridges/interfaces.html
- **Troubleshooting Low Interface Throughput:** https://docs.netgate.com/pfsense/en/latest/troubleshooting/low-throughput.html

pfSense® software

REDES, FIREWALL Y SEGURIDAD

Arquitectura, administración y laboratorios prácticos

PARTE V

PF, reglas, estados y NAT

Oscar de la Cuesta

palentino.es



Primera edición · octubre de 2026

Punto de partida de esta parte

La Parte IV construyó el mapa: subredes, interfaces, VLAN, gateways y rutas. Esta Parte V decide qué tráfico puede utilizar ese mapa y qué cambios de identidad experimentará al atravesar el firewall. Entramos, por tanto, en el núcleo conceptual de pfSense: filtrado con estado, reglas y traducción de direcciones.

Para administrar bien un firewall no basta con saber crear una regla “allow”. Hay que comprender en qué interfaz se evalúa, qué dirección ve PF en ese momento, si la conexión ya tiene un estado, si NAT ha modificado antes el destino o la fuente, qué regla ganó y qué sucederá con el tráfico de respuesta.

> Criterio de esta parte
> La documentación oficial se utiliza como contraste técnico del comportamiento actual. La nomenclatura de ejemplos, tablas, laboratorios y modelos mentales sigue el enfoque didáctico de este libro.

Qué aprenderemos

- Entender el filtrado stateful y por qué el primer paquete de una conexión es especial.
- Saber en qué interfaz se evalúan las reglas normales y por qué “entrada” y “salida” se interpretan desde el firewall.
- Distinguir Pass, Block y Reject y decidir cuándo utilizar cada acción.
- Construir reglas legibles mediante aliases, descripciones, logging y una metodología de mínimo privilegio.
- Comprender el orden Floating → grupos → interfaz y cuándo una floating rule aporta valor real.
- Leer, filtrar y eliminar estados sin tratar la tabla de estados como una caja negra.
- Separar filtrado de NAT: una regla puede permitir y NAT puede traducir, pero son funciones distintas.
- Dominar Port Forward, 1:1 NAT y los modos Automatic, Hybrid y Manual Outbound NAT.
- Comprender Static Port, No NAT, NAT Reflection y por qué Split DNS suele ser una solución más limpia.
- Diagnosticar una publicación de servicio siguiendo el paquete antes y después de las traducciones.

Capítulo 27. PF y el modelo de firewall con estado

pfSense utiliza PF como motor de filtrado. El valor práctico de PF no está en memorizar su sintaxis, sino en comprender el modelo que implementa: los paquetes de una conexión no se evalúan como acontecimientos aislados. El firewall puede recordar que una conexión fue autorizada y permitir el tráfico de respuesta mediante un estado.

27.1. Stateless frente a stateful

Un filtro sin estado compara cada paquete individual contra reglas. Un firewall con estado añade memoria operacional: cuando el primer tráfico de una conexión coincide con una regla de paso, se crea una entrada que describe esa conversación. Los paquetes posteriores pueden coincidir con el estado sin recorrer las mismas reglas como si la comunicación empezara de cero.

```
Cliente 10.20.0.50:53124 → 203.0.113.20:443
Primer paquete → reglas → PASS → crear STATE
Paquetes posteriores/retorno → comprobar STATE → permitir según ese estado
```

Idea clave
Las reglas autorizan el nacimiento de conexiones; la tabla de estados permite que esas conexiones continúen. Esta distinción explica muchos casos en los que se cambia una regla y una sesión existente parece "ignorar" el cambio.

27.2. Qué representa un estado

Un estado registra suficiente información para relacionar el tráfico que pertenece a una conexión: protocolo, extremos, puertos cuando existen, dirección y situación del protocolo. Cuando hay NAT, la visualización puede mostrar identidades antes y después de la traducción, lo que convierte la tabla de estados en una herramienta excepcional para diagnóstico.

Elemento	Ejemplo	Qué nos dice
Protocolo	TCP	Cómo interpretar puertos y fases de conexión.
Origen	10.20.0.50:53124	Cliente y puerto efímero.
Destino	198.51.100.25:443	Servicio al que intenta llegar.
Interfaz	USERS	Dónde quedó ligado el estado.
Estado TCP	ESTABLISHED:ESTABLISHED	Ambos extremos completaron la sesión.
NAT	10.20.0.50 ↔️ IP_WAN	Identidad interna y traducida cuando corresponde.

27.3. Una respuesta no necesita una regla inversa equivalente

Supongamos que USERS permite iniciar HTTPS hacia Internet. Cuando el navegador abre la conexión, la regla de USERS permite el primer tráfico y crea el estado. La respuesta del servidor no necesita una regla WAN que permita “Internet → USERS TCP/443”. El estado ya reconoce que esos paquetes son la respuesta de una conexión autorizada.

Error frecuente

Crear reglas espejo para “la vuelta” de cada conexión. En un firewall stateful, eso suele ampliar superficie innecesariamente. La vuelta de una conexión permitida se gestiona mediante el estado; solo las conexiones nuevas iniciadas desde el otro lado necesitan su propia política.

27.4. Estados y UDP

UDP no establece una sesión con handshake como TCP, pero PF puede seguir flujos UDP mediante estados temporales. Esto permite que una consulta DNS iniciada desde una LAN reciba su respuesta sin abrir una regla genérica desde WAN hacia puertos aleatorios del cliente.

27.5. ICMP también necesita contexto

ICMP no utiliza puertos TCP/UDP, pero tiene tipos y códigos que forman parte del diagnóstico y del funcionamiento de IP. Permitir o bloquear “ICMP” sin distinguir su función puede dañar Path MTU Discovery o IPv6. Más adelante aplicaremos reglas ICMP específicas según escenario.

27.6. Default deny: lo no autorizado no nace

pfSense aplica una filosofía de denegación implícita: si una conexión nueva no coincide con una regla que permita el tráfico, se bloquea. Esta propiedad hace posible construir una política por excepciones controladas en lugar de intentar enumerar todo lo que debería prohibirse.

Seguridad

Una política madura se formula como “qué necesita comunicarse, hacia dónde y para qué”, no como “permitimos todo y luego bloqueamos lo que nos preocupa”. El segundo enfoque envejece peor y dificulta demostrar qué está realmente autorizado.

Capítulo 28. Anatomía de una regla de firewall

Una regla es una condición lógica. Para diseñarla correctamente debemos separar acción, interfaz, dirección, familia IP, protocolo, origen, destino, puertos y opciones de estado. La interfaz web oculta la sintaxis de PF, pero no elimina la necesidad de pensar con precisión.

28.1. Las reglas de interfaz se aplican al tráfico que entra por esa interfaz

En las pestañas normales de interfaz, pfSense filtra en dirección inbound. Si un usuario de la VLAN USERS inicia una conexión hacia Internet, la primera política que nos interesa está en USERS, porque el paquete entra al firewall por esa interfaz. Si un host de Internet inicia una conexión hacia un servicio publicado, el paquete entra por WAN y la política correspondiente se evalúa allí.

USERS → firewall → WAN
Regla principal: pestaña USERS (el paquete entra al firewall por USERS)

Internet → firewall → servidor publicado
Regla principal: WAN (el paquete entra al firewall por WAN)

Qué ocurre realmente
"Inbound" no significa "desde Internet". Significa entrando al firewall por una interfaz concreta. El tráfico de una LAN hacia Internet es inbound en LAN y luego sale por WAN.

28.2. Pass, Block y Reject

Acción	Comportamiento	Uso típico
Pass	Permite el tráfico coincidente y, normalmente, crea estado.	Conexiones autorizadas.
Block	Descarta sin responder.	WAN y tráfico no deseado donde no conviene responder.
Reject	Descarta y devuelve una negativa compatible (p. ej., RST/ICMP).	Redes internas cuando interesa fallar rápido.

En interfaces expuestas, bloquear silenciosamente es una opción habitual. Dentro de la organización, Reject puede mejorar la experiencia de usuario porque una aplicación recibe una negativa inmediata en lugar de esperar un timeout. No existe una regla universal: debe elegirse según el comportamiento que deseamos.

28.3. Origen y destino: describir quién inicia

El origen debe representar al iniciador de la conexión y el destino al recurso que intenta alcanzar. En una regla USERS → DNS, origen puede ser USERS net y destino el alias DNS_CORPORATIVOS. Si el destino se deja en Any por comodidad, la regla ya no expresa el requisito real.

28.4. El puerto de origen suele ser efímero

Para una conexión cliente-servidor, el puerto importante suele ser el de destino. Un navegador podría usar TCP origen 53124 y destino 443. Filtrar origen = 443 por intuición rompe la regla porque el cliente no inicia normalmente desde ese puerto.

Error frecuente

Configurar TCP origen 443 y destino 443 para "permitir HTTPS". En una conexión ordinaria, el cliente elige un puerto origen efímero. Normalmente basta con destino TCP/443.

28.5. Familia de direcciones y protocolo

Una regla puede aplicarse a IPv4, IPv6 o a ambas familias cuando los objetos utilizados sean compatibles. Debemos decidirlo conscientemente. Una política IPv4 no protege automáticamente el mismo flujo por IPv6; en dual stack, ambas pilas requieren una estrategia coherente.

28.6. Regla amplia frente a regla explicable

Regla	Funciona	Es buen diseño
USERS → Any / Any	Sí, probablemente	No demuestra qué necesita la red.
USERS → DNS_CORP UDP/TCP 53	Sí	Expresa un servicio concreto.
USERS → WEB_PROXY TCP 3128	Sí	Es auditable y mantenible.
IOT → Any / Any	Sí	Anula gran parte del valor de segmentar IoT.

28.7. Descripciones que sobreviven al autor

Una descripción debe explicar intención y, cuando tenga sentido, contexto. "Allow traffic" no aporta nada. "USERS → ERP-SQL TCP/1433 · aplicación ERP" permite comprender meses después por qué existe esa excepción.

En producción

Una regla sin descripción debería considerarse deuda técnica. Cuando llega una auditoría o una incidencia, el coste de reconstruir la intención supera con creces los segundos que ahorramos al crearla.

Capítulo 29. Orden de reglas, grupos y Floating Rules

Dos reglas correctas por separado pueden producir un resultado inesperado si se evalúan en un orden diferente al imaginado. La política efectiva depende tanto del contenido como de la posición y del tipo de regla.

29.1. Tres niveles de reglas de capa 3

Para reglas definidas por el administrador, el orden conceptual importante es: reglas Floating, reglas de grupos de interfaces y reglas de la interfaz individual. Si una regla anterior decide el destino del paquete, una regla posterior puede no tener oportunidad de actuar.

1. Floating rules
2. Interface Group rules
3. Interface rules (WAN, LAN, USERS, IOT...)

29.2. Dentro de una pestaña, el orden también importa

Las reglas se procesan de arriba hacia abajo hasta que una regla aplicable determina la acción en el modelo habitual. Por eso las excepciones más específicas suelen colocarse antes que permisos generales.

```
1  Pass  USERS_ADMIN → MGMT_HOSTS  TCP/443
2  Reject USERS      → MGMT_NET    Any
3  Pass  USERS       → Internet    WEB_PORTS
```

La excepción administrativa debe aparecer antes del rechazo de gestión.

29.3. Interface Groups: una política común sin duplicar

Un grupo permite aplicar reglas a varias interfaces relacionadas. Puede ser útil para zonas que comparten una misma política base, pero exige recordar que el grupo se procesa antes que la pestaña individual. Una regla de grupo demasiado amplia puede impedir que una regla posterior en una interfaz consiga restringir el tráfico.

> **Advertencia**
> No utilices grupos únicamente para “ahorrar reglas”. Úsalos cuando las interfaces comparten realmente una política común. La deduplicación no debe ocultar diferencias de seguridad.

29.4. Floating Rules: potencia con coste cognitivo

Las Floating Rules pueden trabajar sobre varias interfaces y en dirección inbound, outbound o ambas. Permiten escenarios difíciles de expresar con reglas normales: marcado de tráfico, políticas egress globales, límites, timeouts especiales, protección frente a fugas por varias salidas o acciones relacionadas con shaping.

Su flexibilidad también las hace peligrosas. Una floating rule puede actuar antes que las reglas de grupos e interfaces y, en salida, ve el tráfico después de determinadas traducciones NAT. Por eso una política que parece correcta al mirar solo la pestaña LAN puede estar siendo alterada por una regla flotante.

29.5. Quick y el concepto de “ya está decidido”

En PF, el comportamiento de evaluación puede depender de Quick. En pfSense, las reglas normales de interfaz se generan de forma que el administrador trabaja con el conocido modelo de primera coincidencia. En Floating Rules, Quick es una decisión explícita especialmente importante. Una regla flotante sin comprender esta opción puede crear un comportamiento muy diferente al esperado.

> **Idea clave**
> Antes de crear una Floating Rule, intenta expresar el requisito con reglas normales. Si no puedes explicar por qué necesitas dirección outbound, varias interfaces o una acción avanzada, probablemente todavía no necesitas una floating rule.

29.6. Logging: registrar decisiones, no inundar el disco

El logging de una regla es esencial para troubleshooting y auditoría. Sin embargo, registrar cada paquete permitido de una red muy activa puede generar ruido. Una estrategia práctica consiste en registrar denegaciones relevantes, excepciones sensibles y reglas que se están validando, ajustando después el nivel de detalle.

Regla	¿Log?	Motivo
Block IOT → MGMT	Sí	Interesa detectar intentos de cruce de zona.
Pass USERS → Internet 443	Normalmente no todo	Volumen enorme y poco valor evento a evento.
Pass proveedor → servidor administración	Sí	Acceso excepcional y sensible.
Regla temporal de diagnóstico	Sí	Necesitamos demostrar qué coincidió.

Capítulo 30. Aliases: convertir reglas en una política legible

Los aliases permiten agrupar hosts, redes o puertos bajo nombres. Técnicamente reducen repetición; operativamente hacen que el ruleset pueda leerse como una política. Una regla "USERS → SERVIDORES_ERP → PUERTOS_ERP" cuenta una historia que una lista de direcciones no cuenta.

30.1. Tipos principales

Tipo	Contenido	Ejemplo
Host	IP individuales o FQDN	ERP01 = 10.30.0.20
Network	Prefijos, rangos, direcciones/FQDN compatibles	REDES_CORP = 10.20.0.0/24 + 10.30.0.0/24
Port	Puertos y rangos	WEB_PORTS = 80,443
URL	Lista descargada al crear/actualizar el alias	Lista externa pequeña o gestionada
URL Table	Tabla persistente actualizada periódicamente	Conjuntos grandes de IP/puertos

30.2. Aliases anidados

Una práctica potente consiste en construir aliases por capas. SERVIDORES_WEB puede agrupar WEB01 y WEB02; SERVIDORES_PRODUCCION puede incluir SERVIDORES_WEB y SERVIDORES_ERP. El objetivo no es crear jerarquías infinitas, sino que el nombre exprese el concepto operativo adecuado para la regla.

```
WEB01 = 10.30.0.21
WEB02 = 10.30.0.22
SERVIDORES_WEB = WEB01 + WEB02
SERVIDORES_PRODUCCION = SERVIDORES_WEB + ERP01 + SQL01
```

30.3. FQDN en aliases y dependencia DNS

Cuando un alias utiliza un FQDN, el firewall resuelve el nombre y mantiene la tabla con las direcciones obtenidas. Esto es útil para destinos con IP cambiante, pero introduce una dependencia: si el DNS del firewall falla o el nombre devuelve direcciones inesperadas, la política puede cambiar de efecto sin haber editado la regla.

En producción
Para reglas críticas, documenta si un alias depende de DNS y revisa Diagnostics > Tables cuando el comportamiento no coincida con lo esperado. La regla puede estar bien escrita y la tabla contener una IP distinta de la imaginada.

30.4. Alias no es Virtual IP

Un alias es una colección que una regla puede consultar. Una Virtual IP agrega una identidad IP que el firewall puede utilizar en una interfaz o función. La similitud de nombres no implica relación funcional.

30.5. Convención de nombres

Prefijo sugerido	Uso	Ejemplo
H_	Host	H_ERP01
N_	Network	N_MGMT
P_	Ports	P_WEB
G_	Grupo conceptual	G_SERVIDORES_CRITICOS
EXT_	Entidad externa	EXT_PROVEEDOR_SOPORTE

No es obligatorio usar prefijos. Lo importante es que exista una convención documentada y que los nombres se mantengan estables. Cambiar nombres por estética cada pocos meses perjudica logs, procedimientos y memoria operativa.

30.6. Diseñar aliases antes de escribir cincuenta reglas

Cuando una política contiene varias zonas y servicios, conviene definir primero los objetos recurrentes. Esto reduce errores tipográficos y permite modificar un grupo de servidores en un solo lugar sin editar cada regla que los referencia.

Laboratorio mental
La aplicación ERP pasa de un servidor a un clúster de tres nodos. Si las reglas apuntan a un alias SERVIDORES_ERP, actualizamos el objeto. Si contienen IP escritas una a una en quince reglas, el cambio se convierte en una búsqueda peligrosa.

Capítulo 31. La tabla de estados: memoria operativa del firewall

La tabla de estados es una de las herramientas más importantes para comprender qué está haciendo realmente pfSense. Muestra conexiones que el firewall reconoce como activas y permite observar protocolo, extremos, traducciones y fase de una sesión.

31.1. Cambiar una regla no siempre interrumpe una sesión existente

Si una conexión ya tiene un estado válido, modificar una regla puede afectar a conexiones nuevas mientras la existente continúa. Esto es especialmente visible durante pruebas: se bloquea un servicio y el navegador sigue comunicándose porque conserva una sesión persistente.

Qué ocurre realmente
Reglas y estados son dos capas distintas. Cambiar la política modifica cómo nacen nuevas conexiones; eliminar estados obliga a que los próximos paquetes vuelvan a pasar por el proceso de creación de una conexión.

31.2. Leer estados TCP

TCP expone fases reconocibles. Ver SYN_SENT en un lado y no llegar a ESTABLISHED ayuda a localizar el fallo: quizá el SYN salió pero no volvió SYN/ACK; quizá la respuesta llegó por otro camino; quizá el servidor no escucha.

Estado visible	Lectura aproximada	Pregunta útil
SYN_SENT	Se intentó iniciar conexión	¿El servidor respondió?
ESTABLISHED	Sesión activa	¿Hay tráfico en ambas direcciones?
FIN_WAIT	Cierre en progreso	¿Es un cierre normal o una sesión atascada?
TIME_WAIT	Cierre reciente	¿Se están creando conexiones con excesiva frecuencia?
CLOSED	Un extremo considera cerrada la sesión	¿Hubo RST o expiración?

31.3. Filtrar por IP, puerto o interfaz

En un firewall con miles de estados, mirar la lista completa no ayuda. Debemos filtrar por el host de interés, destino, puerto o interfaz. Diagnostics > States y sus vistas de resumen permiten convertir una masa de conexiones en preguntas concretas.

31.4. Estados y NAT

Cuando existe traducción, un estado puede mostrar la dirección original y la dirección traducida. Esta información es especialmente útil para comprobar si Outbound NAT utilizó la IP pública esperada o si un Port Forward realmente redirigió hacia el servidor previsto.

```
Antes de NAT: 10.20.0.50:53124 → 198.51.100.20:443
Después de NAT: 203.0.113.10:62001 → 198.51.100.20:443
```

31.5. Eliminar estados de forma quirúrgica

Resetear toda la tabla de estados interrumpe conexiones de todos los usuarios. Para troubleshooting es preferible filtrar y eliminar solo los estados del host o servicio afectado cuando sea posible.

> **Advertencia**
> Borrar todos los estados de un firewall de producción puede cortar VPN, sesiones de aplicaciones, llamadas, conexiones de bases de datos y navegación. No debe usarse como equivalente a “refrescar”.

31.6. State table exhaustion

La tabla de estados tiene límites. Un gran número de conexiones legítimas, una aplicación mal diseñada, P2P, escaneos o ataques pueden consumir estados. Antes de aumentar límites de forma automática hay que identificar quién los genera y si el patrón es normal.

La vista States Summary ayuda a observar concentraciones por origen, destino, pares y puertos. Un único host con decenas de miles de conexiones puede ser una carga esperada —por ejemplo, un proxy— o una señal de problema. El contexto importa.

31.7. pfTop y observación en tiempo real

pfTop ofrece una vista dinámica de los estados y resulta útil cuando queremos observar conexiones a medida que aparecen. La GUI facilita el acceso para administradores menos acostumbrados a consola; la herramienta en línea de comandos es valiosa durante diagnóstico avanzado.

Capítulo 32. NAT: cambiar identidades sin confundirlo con seguridad

NAT modifica direcciones y, en algunos casos, puertos. Firewalling decide si el tráfico está autorizado. Las dos funciones pueden trabajar juntas, pero no son equivalentes. “Está detrás de NAT” no debe utilizarse como sinónimo de “está protegido por una política de firewall”.

32.1. Tres familias que utilizaremos

Familia	Qué cambia	Ejemplo
Port Forward / DNAT	Destino y posiblemente puerto al entrar	IP pública:443 → 10.30.0.20:443
1:1 NAT	Asociación completa entre IP externa e interna	203.0.113.20 ↔️ 10.30.0.20
Outbound NAT / SNAT	Origen al salir	10.20.0.50 → IP_WAN

32.2. El orden NAT/firewall importa

Cuando un paquete entra por una interfaz y coincide con un Port Forward, la traducción de destino ocurre antes de las reglas de firewall correspondientes. Por eso una regla WAN asociada a un Port Forward ve normalmente como destino el host interno ya traducido, no simplemente la dirección WAN original.

Entrada desde Internet:
Paquete en cable WAN → NAT de entrada (Port Forward / 1:1) → reglas firewall WAN → routing → salida

Salida hacia Internet:
reglas de entrada en LAN → routing → 1:1 / Outbound NAT → reglas floating outbound → cable WAN

Qué ocurre realmente
Un sniffer en WAN puede mostrar la IP pública porque observa el paquete en el cable. Una regla evaluada después de DNAT puede estar comparando ya la IP privada. Ambas observaciones son correctas: ocurren en puntos distintos del recorrido.

32.3. tcpdump ve el cable

Una captura en una interfaz muestra paquetes tal como entran o salen físicamente/lógicamente de ese punto. Esta idea permite diagnosticar NAT con dos capturas: una en WAN para demostrar que el tráfico público llega y otra en la interfaz interna para comprobar si aparece ya traducido.

32.4. NAT no reemplaza routing

Si dos redes privadas están conectadas por routing y ambas conocen la ruta de vuelta, no necesitan NAT para comunicarse. Introducir NAT internamente puede ocultar identidades, complicar logs y romper aplicaciones que esperan conocer al cliente real.

> **Idea clave**
> Primero pregunta: “¿puedo enrutarlo?” Después pregunta: “¿necesito traducirlo?”. NAT es una herramienta de direccionamiento y compatibilidad, no el paso obligatorio de toda comunicación entre redes.

32.5. IPv6 cambia la conversación

En despliegues IPv6 normales cada segmento puede utilizar direcciones globales enrutablemente únicas y el control de exposición se realiza con firewall. Esto elimina muchas razones históricas para NAT44. Existen mecanismos de traducción IPv6 para escenarios concretos, pero no deben proyectarse automáticamente hábitos de IPv4 sobre IPv6.

Capítulo 33. Port Forward y publicación controlada de servicios

Un Port Forward permite que una conexión dirigida a una dirección/puerto de una interfaz externa termine en un host y puerto distintos del interior. Es el mecanismo habitual cuando disponemos de una sola IP pública y necesitamos publicar servicios seleccionados.

33.1. Diseñar antes de crear

Pregunta	Ejemplo
¿Qué servicio?	HTTPS de aplicación externa
¿Quién puede iniciarlo?	Internet completo o alias de proveedor
¿A qué IP externa?	WAN address / VIP concreta
¿Qué puerto externo?	TCP/443
¿Qué servidor interno?	10.30.0.20
¿Qué puerto interno?	TCP/443
¿Cómo verificaremos?	Test externo + log + captura WAN/LAN

33.2. NAT y regla de firewall asociada

La GUI puede crear automáticamente una regla de firewall asociada al Port Forward. Esto reduce errores de sincronización: la traducción define a dónde va el tráfico y la regla asociada autoriza la conexión nueva. Conviene revisar ambas, no asumir que “crear NAT” por sí solo es lo mismo que permitir.

33.3. Restringir el origen cuando sea posible

Un panel de administración utilizado solo por un proveedor no debería publicarse a Any si conocemos sus redes. Un alias EXT_PROVEEDOR permite reducir la superficie y hace visible la intención.

```
WAN TCP 8443 desde EXT_PROVEEDOR
  ↓ Port Forward
10.30.0.40 TCP 443
  ↓ Regla WAN asociada
Solo el proveedor puede iniciar
```

33.4. No publicar la WebGUI “temporalmente”

La administración del firewall merece un canal de gestión diseñado: VPN, red de administración o acceso fuera de banda. Crear un Port Forward hacia la propia administración o abrirla en WAN por comodidad durante una intervención incrementa el riesgo precisamente sobre el dispositivo que controla el perímetro.

Seguridad
Los servicios publicados deben ser mínimos, parcheados y monitorizados. El firewall reduce quién puede llegar a ellos, pero no corrige vulnerabilidades del servidor publicado.

33.5. Probar desde fuera de verdad

Probar una IP pública desde la misma LAN puede activar problemas de hairpin/reflection o resolver el nombre a una dirección distinta. Para validar un Port Forward, la prueba más clara procede de una red externa: conexión móvil, VPN externa o un sistema de prueba fuera del perímetro.

33.6. Split DNS frente a NAT Reflection

Cuando usuarios internos deben usar el mismo nombre que los externos, una solución limpia consiste en que DNS interno resuelva el nombre público directamente a la IP privada del servidor. Así el tráfico interno no sale hacia la identidad pública para volver a entrar.

```
Externo: app.empresa.es → 203.0.113.20 → Port Forward → 10.30.0.20
Interno: app.empresa.es → 10.30.0.20 directamente (Split DNS)
```

NAT Reflection permite otros comportamientos cuando se necesita acceder desde dentro mediante la dirección externa, pero añade traducciones y complejidad. Debe usarse porque existe un requisito, no porque no queramos diseñar DNS interno.

En producción
Si controlas el DNS de la organización, Split DNS suele ofrecer un camino más directo y comprensible. NAT Reflection queda como herramienta para escenarios donde no se puede resolver el nombre interno de forma adecuada.

Capítulo 34. 1:1 NAT y Outbound NAT

34.1. 1:1 NAT: una identidad pública dedicada

1:1 NAT asocia una dirección externa con una interna sin limitar la traducción a un único puerto. No significa “permitir todo”: siguen siendo necesarias reglas de firewall. Precisamente por abarcar todos los puertos, un error de filtrado puede tener un impacto mayor que en un Port Forward limitado a un servicio.

203.0.113.25 ↔️ 10.30.0.25
Traducción 1:1 de dirección; los puertos se conservan.
La política WAN decide qué conexiones nuevas se permiten.

Advertencia
Una regla WAN excesivamente amplia combinada con 1:1 NAT puede exponer muchos servicios del host interno. Limita explícitamente protocolos, orígenes y puertos autorizados.

34.2. Precedencia útil

En entrada, un Port Forward puede prevalecer sobre una asociación 1:1 para un puerto concreto. En salida, 1:1 NAT tiene precedencia sobre reglas generales de Outbound NAT. Esto permite construir excepciones, pero también obliga a documentar la intención para que el comportamiento no parezca arbitrario.

34.3. Outbound NAT: quién aparece como origen

En una instalación IPv4 típica, los clientes privados salen a Internet traducidos a la dirección de la WAN. pfSense puede generar esta política automáticamente. Cuando necesitamos controlar identidades públicas, excepciones o puertos de origen, entran los modos Hybrid y Manual.

34.4. Los modos de Outbound NAT

Modo	Qué hace	Cuándo resulta adecuado
Automatic	Genera las reglas necesarias para escenarios habituales.	Instalaciones sencillas sin necesidades especiales.
Hybrid	Mantiene reglas automáticas y permite añadir reglas manuales prioritarias.	La mayoría de personalizaciones puntuales.
Manual	Solo existen las reglas administradas manualmente.	Entornos complejos donde se desea control total y se acepta la carga operativa.

Modo	Qué hace	Cuándo resulta adecuado
Disabled / sin Outbound NAT	No se aplica traducción automática según el modo disponible.	Redes enrutadas donde los prefijos son alcanzables sin NAT, según diseño.

Hybrid suele ser un punto de equilibrio: permite una excepción específica sin obligarnos a reconstruir manualmente todas las reglas automáticas que el sistema mantenía por nosotros.

34.5. Static Port

Normalmente NAT puede cambiar también el puerto de origen. Algunas aplicaciones y protocolos requieren conservarlo. Static Port solicita que la traducción mantenga el puerto origen. Debe activarse para una necesidad identificada, no como una mejora general.

Un ejemplo clásico aparece en determinados escenarios de VoIP o VPN donde el peer espera consistencia de puerto. Antes de activar Static Port, hay que confirmar el requisito y limitar la regla al tráfico afectado.

34.6. Do not NAT

Una regla de Outbound NAT puede utilizarse para evitar traducción de tráfico coincidente. Es útil cuando existe conectividad enrutada real entre redes y necesitamos impedir que una regla más general o automática oculte el origen.

```
N_10_20_USERS → N_PARTNER por VPN/ruta
Do not NAT → el partner ve 10.20.0.50, no IP_WAN
```

34.7. Orden: específico antes que general

Las reglas de Outbound NAT se procesan en orden. Las excepciones específicas deben aparecer antes de reglas generales que también podrían coincidir. La misma disciplina que aplicamos a reglas de firewall se aplica aquí: primero expresar lo particular, después cubrir el caso amplio.

Capítulo 35. Laboratorio integral: publicar, traducir y diagnosticar

Este laboratorio une reglas, estados y NAT sobre la topología empresarial construida en la Parte IV. El objetivo no es terminar con muchas reglas, sino poder demostrar por qué cada flujo funciona o se bloquea.

35.1. Escenario

Zona / objeto	Dirección	Función
WAN	203.0.113.10/29	Salida principal del firewall.
VIP_WEB	203.0.113.11	Identidad pública de la aplicación.
USERS	10.20.0.0/24	Usuarios corporativos.
SERVERS	10.30.0.0/24	Servidores internos.
IOT	10.40.0.0/24	Dispositivos IoT.
GUEST	10.50.0.0/24	Invitados.
WEB01	10.30.0.20	Servidor HTTPS publicado.
ERP01	10.30.0.30	Aplicación empresarial interna.
DNS01	10.30.0.53	DNS corporativo.
ADMIN01	10.10.0.25	Estación autorizada de administración.

35.2. Política deseada

- USERS puede consultar DNS01 y acceder a ERP01 por los puertos de la aplicación.
- USERS puede navegar por HTTP/HTTPS hacia Internet.
- IOT puede resolver DNS y acceder únicamente a servicios externos necesarios; no puede iniciar hacia MGMT ni SERVERS salvo excepciones documentadas.
- GUEST solo puede alcanzar Internet y no puede iniciar hacia redes corporativas.
- Internet puede llegar a WEB01 únicamente por HTTPS mediante VIP_WEB.
- La administración sensible de servidores solo puede iniciarse desde ADMIN01.
- Los clientes internos resuelven web.empresa.es directamente a 10.30.0.20 mediante Split DNS.

35.3. Construir aliases

Alias	Contenido
N_CORPORATIVAS	MGMT + USERS + SERVERS + IOT (según diseño)

Alias	Contenido
H_DNS01	10.30.0.53
H_WEB01	10.30.0.20
H_ERP01	10.30.0.30
H_ADMIN01	10.10.0.25
P_WEB	80,443
P_ERP	puertos definidos por la aplicación ERP

35.4. Reglas USERS

```
1  Pass   USERS net → H_DNS01   TCP/UDP 53    "DNS corporativo"
2  Pass   USERS net → H_ERP01   P_ERP         "Aplicación ERP"
3  Reject USERS net → N_PRIVADAS Any          "No acceso lateral no autorizado"
4  Pass   USERS net → Any       P_WEB         "Navegación web"
```

La regla 3 requiere cuidado: el alias N_PRIVADAS debe reflejar exactamente las redes que queremos proteger y no bloquear destinos privados legítimos que deban ser alcanzables. El ejemplo pretende enseñar el orden, no ofrecer un ruleset universal.

35.5. Reglas IOT y GUEST

```
IOT:
1 Pass   IOT net → H_DNS01   TCP/UDP 53
2 Reject IOT net → N_CORPORATIVAS Any   [LOG]
3 Pass   IOT net → Any       servicios externos estrictamente necesarios

GUEST:
1 Reject GUEST net → N_RED_INTERNA Any [LOG]
2 Pass   GUEST net → Any       P_WEB/DNS según política
```

Seguridad

No copies estas reglas sin adaptar DNS, NTP, captive portal, servicios cloud y necesidades reales. Un laboratorio enseña un método; una política de producción debe derivarse de inventario y requisitos.

35.6. Publicar WEB01

1. Crear la Virtual IP pública correspondiente si el diseño utiliza una IP adicional del bloque.
2. Crear Port Forward TCP/443 desde VIP_WEB hacia H_WEB01 TCP/443.
3. Crear o revisar la regla WAN asociada y limitar origen si el servicio no es público general.
4. Configurar DNS público web.empresa.es → 203.0.113.11.

5. Configurar Split DNS interno web.empresa.es → 10.30.0.20.
6. Probar desde una red externa real.
7. Observar logs y estado creado.
8. Capturar simultáneamente en WAN y SERVERS si algo falla.

35.7. Ver el paquete en cuatro momentos

A. Internet: cliente 198.51.100.50:54000 → 203.0.113.11:443
B. WAN capture: todavía ve 203.0.113.11:443 en el cable
C. Después de Port Forward/regla: destino lógico = 10.30.0.20:443
D. SERVERS capture: paquete hacia 10.30.0.20:443
Retorno: estado + routing + NAT inverso mantienen coherencia para el cliente

35.8. Método de troubleshooting de Port Forward

Paso	Pregunta	Si falla
1. DNS	¿El nombre público apunta a la IP correcta?	Corregir DNS antes de tocar NAT.
2. Llegada WAN	¿tcpdump ve SYN en WAN?	Problema upstream, IP, ISP o prueba no externa.
3. Firewall log	¿La regla permite/bloquea?	Revisar origen, destino traducido y orden.
4. Salida interna	¿tcpdump ve SYN hacia WEB01?	Revisar NAT/regla/routing.
5. Servidor	¿WEB01 escucha y responde?	Firewall local/servicio/gateway del servidor.
6. Vuelta	¿Respuesta regresa por pfSense?	Revisar gateway/rutas asimétricas.
7. Estado	¿Aparece estado coherente?	Filtrar Diagnostics > States y observar NAT.

35.9. La trampa de los estados antiguos

Durante el laboratorio cambiaremos reglas varias veces. Si una prueba se comporta como antes del cambio, filtraremos estados del cliente/servidor y eliminaremos únicamente los relacionados. De esta forma evitamos resetear todas las conexiones del firewall.

35.10. Caso: Outbound NAT específico

Supongamos que WEB01 debe salir a Internet utilizando 203.0.113.11 como identidad pública, mientras el resto utiliza 203.0.113.10. Pasaremos a Hybrid Outbound NAT y añadiremos una regla específica para H_WEB01 antes de las reglas generales.

Outbound NAT (Hybrid):
H_WEB01 → WAN → Translation: VIP_WEB (203.0.113.11)
Resto de redes → reglas automáticas → WAN address (203.0.113.10)

Después de crear la regla, eliminamos los estados existentes de WEB01 para que las conexiones nuevas se creen bajo la política actual y validamos desde un servicio externo cuál es la IP origen observada.

35.11. Caso: socio enrutado sin NAT

Una red de partner accesible por un túnel o router conoce nuestras subredes corporativas. No queremos que pfSense oculte 10.20.0.0/24 detrás de una dirección de WAN. La política correcta puede necesitar una excepción Do not NAT antes de cualquier regla general que coincida.

Qué ocurre realmente
Si el partner necesita distinguir usuarios por IP, NAT elimina esa información. Cuando existe routing bidireccional válido, conservar la dirección origen suele producir logs y políticas más transparentes.

35.12. Matriz de validación final

Prueba	Esperado	Evidencia
USERS → ERP	Permitido solo P_ERP	Log/estado y prueba de aplicación.
USERS → MGMT no autorizado	Bloqueado/rechazado	Regla específica y log.
IOT → SERVERS	Bloqueado salvo excepción	Log de denegación.
GUEST → redes internas	Bloqueado	Captura/log.
GUEST → Web Internet	Permitido	Estado + navegación.
Internet → VIP_WEB:443	Permitido y traducido a WEB01	Capturas WAN/SERVERS + estado.
Internet → VIP_WEB:22	Bloqueado	Sin Port Forward/regla; log si procede.
WEB01 → Internet	Origen público VIP_WEB	Comprobación externa + estado NAT.
Cliente interno → web.empresa.es	Va directo a 10.30.0.20	DNS interno + captura.

35.13. Árbol mental para cualquier incidencia de firewall

```
¿Existe ruta?
  └─ no → resolver routing
  └─ sí → ¿paquete entra por la interfaz esperada?
        └─ no → capa 2/topología/VLAN
        └─ sí → ¿hay estado previo?
              └─ sí → inspeccionar/eliminar selectivamente si procede
              └─ no → ¿qué regla coincide?
                    └─ bloqueo → corregir política si el requisito es válido
                    └─ pass → ¿NAT cambia identidad?
                          └─ sí → comprobar antes/después con captura
                          └─ no → seguir camino y retorno
```

Método
Cuando una conexión falla, evita “añadir una allow any para probar” como primera reacción. Demuestra paso a paso ruta, interfaz, regla, estado, NAT y retorno. El diagnóstico conserva la seguridad y produce conocimiento reutilizable.

Notas avanzadas de la Parte V

NAT64 y traducciones entre familias

pfSense puede participar en escenarios de traducción entre IPv6 e IPv4 mediante NAT64. Es un tema especializado que se abordará con más detalle cuando tratemos servicios IPv6 y arquitecturas de transición. En esta parte basta recordar que las traducciones pueden cambiar incluso la familia de direcciones y que el orden de procesamiento sigue siendo crítico para interpretar reglas y capturas.

Asymmetric routing y estados

PF espera normalmente observar una conexión de forma coherente. Si el camino de ida atraviesa pfSense pero la vuelta utiliza otro router, el firewall puede ver una conversación incompleta. Existen opciones avanzadas para determinados escenarios asimétricos, pero la primera solución debería ser corregir la topología cuando sea posible.

Policy routing y reglas

Una regla puede seleccionar un gateway y forzar un camino distinto del que elegiría la tabla de rutas. Esto se explotará en Multi-WAN y VPN. Desde ahora debemos recordar que una regla no solo puede decir “pass”: también puede influir en por dónde se encamina la conexión.

Reglas automáticas e internas

El ruleset efectivo contiene reglas que el administrador no ha escrito manualmente: protecciones de administración, servicios, DHCP, VPN y otros componentes pueden generar reglas internas. Cuando la GUI no explica por sí sola un comportamiento, las herramientas de diagnóstico y la visualización del ruleset ayudan a ver la política completa.

Cierre de la Parte V

En esta parte hemos pasado de “crear reglas” a comprender el motor que las hace efectivas. Una conexión atraviesa varias decisiones: llega por una interfaz, puede ser traducida, se compara con una política, puede crear un estado y, al salir, puede cambiar de identidad nuevamente. Entender ese recorrido permite diseñar reglas pequeñas y diagnosticar problemas sin desactivar la seguridad.

La siguiente parte se centrará en servicios de infraestructura que descansan sobre estas reglas: DHCP, DNS Resolver, DNS Forwarding, NTP, Dynamic DNS y mecanismos relacionados. Ya podremos tratarlos no como servicios aislados, sino como flujos que deben encajar dentro de una política de red.

Antes de pasar a la Parte VI
El lector debería ser capaz de explicar por qué una regla se coloca en una interfaz determinada, qué diferencia existe entre Block y Reject, cómo una conexión crea estado, cuándo eliminarlo, qué ve una regla después de un Port Forward y qué modo de Outbound NAT elegiría para una excepción concreta.

Glosario de la Parte V

Término	Definición en este libro
PF	Motor de filtrado de paquetes utilizado por pfSense.
State / estado	Entrada que permite al firewall seguir una conexión o flujo autorizado.
Stateful firewall	Firewall que mantiene contexto de las conexiones en lugar de evaluar cada paquete de forma aislada.
Pass	Acción que permite tráfico coincidente.
Block	Descarta tráfico sin respuesta.
Reject	Descarta devolviendo una negativa compatible al origen.
Alias	Objeto que agrupa hosts, redes, puertos o listas para reutilizarlos en reglas.

Término	Definición en este libro
Floating Rule	Regla avanzada aplicable a múltiples interfaces y/o direcciones de flujo.
DNAT / Port Forward	Traducción del destino de una conexión entrante.
SNAT / Outbound NAT	Traducción del origen de tráfico saliente.
1:1 NAT	Asociación de una dirección externa con una interna conservando puertos.
Static Port	Opción de Outbound NAT que conserva el puerto de origen.
Split DNS	Resolución DNS diferente según el contexto, por ejemplo nombre público → IP privada para clientes internos.
NAT Reflection	Mecanismo que permite a clientes internos alcanzar destinos internos mediante la identidad externa/NAT.
Quick	Control de evaluación especialmente relevante en Floating Rules.
State table	Conjunto de conexiones/flujos que PF está siguiendo activamente.

Fuentes técnicas de contraste

Las fuentes siguientes se han utilizado para comprobar el comportamiento vigente de pfSense respecto a reglas, estados, aliases y NAT. Verificación técnica: 8 de octubre de 2026.

- **Rule Methodology:** https://docs.netgate.com/pfsense/en/latest/firewall/rule-methodology.html
- **Configuring Firewall Rules:** https://docs.netgate.com/pfsense/en/latest/firewall/configure.html
- **Floating Rules:** https://docs.netgate.com/pfsense/en/latest/firewall/floating-rules.html
- **Firewall Fundamentals:** https://docs.netgate.com/pfsense/en/latest/firewall/fundamentals.html
- **Aliases:** https://docs.netgate.com/pfsense/en/latest/firewall/aliases.html
- **Alias Types:** https://docs.netgate.com/pfsense/en/latest/firewall/aliases-types.html
- **Alias Features and Limitations:** https://docs.netgate.com/pfsense/en/latest/firewall/aliases-features.html
- **Firewall Table Contents:** https://docs.netgate.com/pfsense/en/latest/monitoring/status/firewall-tables.html
- **Firewall States:** https://docs.netgate.com/pfsense/en/latest/monitoring/status/firewall-states.html
- **Viewing Firewall States in the GUI:** https://docs.netgate.com/pfsense/en/latest/monitoring/status/firewall-states-gui.html
- **Firewall States Summary:** https://docs.netgate.com/pfsense/en/latest/monitoring/status/firewall-states-summary.html

- **Ordering of NAT and Firewall Processing:** https://docs.netgate.com/pfsense/en/latest/nat/process-order.html
- **Network Address Translation:** https://docs.netgate.com/pfsense/en/latest/nat/index.html
- **Choosing a NAT Configuration:** https://docs.netgate.com/pfsense/en/latest/nat/choices.html
- **Outbound NAT:** https://docs.netgate.com/pfsense/en/latest/nat/outbound.html
- **1:1 NAT:** https://docs.netgate.com/pfsense/en/latest/nat/1-1.html
- **Accessing Port Forwards from Local Networks:** https://docs.netgate.com/pfsense/en/latest/recipes/port-forwards-from-local-networks.html
- **Troubleshooting NAT Port Forwards:** https://docs.netgate.com/pfsense/en/latest/troubleshooting/nat-port-forwards.html
- **Troubleshooting Firewall Rules:** https://docs.netgate.com/pfsense/en/latest/troubleshooting/firewall.html

pfSense® software

REDES, FIREWALL Y SEGURIDAD

Arquitectura, administración y laboratorios prácticos

PARTE VI

DHCP, DNS, NTP y servicios de infraestructura

Oscar de la Cuesta

palentino.es



Primera edición · octubre de 2026

Apertura de la Parte VI

La Parte V explicó cómo pfSense decide si un flujo puede cruzar el firewall y cómo NAT modifica determinadas direcciones y puertos. Esta Parte VI cambia de perspectiva: estudia los servicios que hacen que una red sea utilizable sin configurar manualmente cada equipo.

DHCP entrega parámetros de red. DNS convierte nombres en datos utilizables por IP. Router Advertisements permiten a un host IPv6 descubrir su router. NTP mantiene el tiempo coherente. Dynamic DNS relaciona un nombre estable con una dirección WAN que puede cambiar. Cuando cualquiera de estas piezas falla, el usuario suele resumirlo con una frase imprecisa: «no hay Internet».

Modelo mental de esta parte

Presento estos servicios como una cadena de dependencias, no como casillas independientes: un cliente obtiene identidad de red, descubre su puerta de enlace, aprende a quién preguntar por nombres, sincroniza su reloj y, finalmente, puede utilizar servicios locales o remotos de forma predecible.

```
Cliente arranca
  ↓
DHCP / SLAAC / DHCPv6
  ↓
IP + prefijo + gateway/RA + DNS
  ↓
DNS Resolver / Forwarder
  ↓
Routing + Firewall + NAT
  ↓
Servicio remoto
```

En octubre de 2026 pfSense mantiene dos motores DHCP: Kea DHCP e ISC DHCP. Kea es la opción moderna y recomendada; ISC DHCP está en desuso y se conserva temporalmente por compatibilidad. El libro utilizará Kea como referencia principal y explicará las diferencias de migración cuando sean relevantes.

Capítulo 36. DHCP: mucho más que entregar una dirección IP

DHCPv4 automatiza una conversación que, de otro modo, obligaría a introducir dirección, máscara, gateway, DNS y otros parámetros en cada host. El protocolo no sabe si un cliente es «fiable» ni si la dirección concedida tiene permiso para atravesar el firewall: su misión principal es proporcionar configuración de red.

36.1. El intercambio DORA

La secuencia clásica de DHCPv4 puede recordarse como DORA: Discover, Offer, Request y Acknowledge. Lo importante no es memorizar las siglas, sino comprender que al comienzo el cliente todavía no dispone de una dirección IP utilizable y necesita utilizar broadcast para localizar un servidor.

```
Cliente                Servidor DHCP
  |--- DHCPDISCOVER ---------->|
  |<-- DHCPOFFER --------------|
  |--- DHCPREQUEST ------------>|
  |<-- DHCPACK ----------------|
```

Qué ocurre realmente

La primera solicitud DHCP no puede depender de una ruta IP normal porque el cliente aún no tiene una configuración válida. Por eso DHCP funciona dentro del dominio de broadcast y necesita un relay cuando el servidor está en otra red.

36.2. Una concesión no es solo una IP

Dato	Ejemplo	Consecuencia
Dirección	10.20.0.137	Identidad temporal del cliente.
Prefijo	/24	Determina qué destinos considera locales.
Router	10.20.0.1	Siguiente salto para redes externas.
DNS	10.20.0.1	Servidor al que enviará consultas de nombres.
Dominio de búsqueda	corp.ejemplo.es	Permite completar nombres cortos según política.
Lease time	8 horas	Marca renovación y caducidad de la concesión.
Opciones adicionales	NTP, PXE, VoIP…	Permiten automatizar necesidades específicas.

Un error de DHCP puede parecer un error de DNS, routing o aplicación. Por ejemplo, un cliente con IP correcta pero gateway equivocado podrá hablar con hosts locales y fallará al salir; uno con gateway correcto pero DNS erróneo llegará a 1.1.1.1 pero no a un nombre.

36.3. Pools, reservas y exclusiones

El pool define el conjunto de direcciones que el servidor puede conceder dinámicamente. Una reserva o mapeo estático asocia una identidad conocida —habitualmente una MAC— con una dirección concreta. Esto no convierte la dirección en una credencial de seguridad.

Error frecuente

Usar una reserva DHCP como si fuera control de acceso. Un usuario que pueda fijar manualmente una IP o falsificar una MAC puede eludir esa lógica. La autorización pertenece a firewall, 802.1X, NAC, segmentación y controles de capa 2/3, no al hecho de recibir una concesión concreta.

36.4. Lease time y comportamiento operativo

Una concesión excesivamente corta genera renovaciones frecuentes; una excesivamente larga retrasa la reutilización de direcciones y puede conservar configuraciones antiguas durante más tiempo. No existe un valor universal: una red de invitados con alta rotación y una red de puestos fijos tienen necesidades distintas.

Escenario	Criterio de lease
Puestos fijos	Horas o días, según estabilidad y tamaño del pool.
Wi-Fi invitados	Más corto si existe alta rotación de dispositivos.
Laboratorio efímero	Corto para recuperar direcciones con rapidez.
IoT estable	Puede ser largo, aunque conviene reservar y documentar.
Entorno con cambios planificados	Reducir temporalmente antes de una migración puede acelerar adopción.

36.5. DHCP y el firewall

El servidor DHCP puede estar funcionando correctamente y, sin embargo, el cliente no tener acceso a otros destinos. Una concesión no crea por sí sola reglas de firewall. En nuestro modelo, DHCP resuelve configuración; PF decide autorización.

```
DHCP concede 10.50.0.120
        ↓
Cliente queda correctamente configurado
        ↓
Reglas de la interfaz GUEST deciden qué puede hacer 10.50.0.120
```

Capítulo 37. Kea DHCP en pfSense: diseño y operación

Kea es el backend DHCP moderno integrado en pfSense. En las versiones actuales es la elección recomendada y está llamado a sustituir completamente a ISC DHCP. La migración no debe plantearse como un simple cambio de nombre: existen diferencias funcionales, especialmente en alta disponibilidad y registro DNS.

37.1. Backend global, configuración por interfaz

El backend DHCP se selecciona globalmente. Después, cada interfaz con direccionamiento adecuado dispone de su propia configuración de servidor. Este modelo separa dos preguntas: qué motor atiende DHCP y en qué redes se ofrece el servicio.

Nivel	Ejemplo de decisión
Global	Kea o ISC DHCP.
Interfaz	DHCP activado en USERS, desactivado en SERVERS.
Pool	10.20.0.100–10.20.0.220.
Opciones	Gateway, DNS, dominio, NTP, parámetros especiales.
Mapeos	Reservas para impresoras, teléfonos o equipos gestionados.

37.2. Registro DNS dinámico de clientes

Kea puede registrar nombres de clientes DHCP en el DNS Resolver de pfSense. En las versiones actuales esa actualización se realiza dinámicamente y no exige reiniciar Unbound cada vez que cambia una concesión.

Por qué importa

En una red administrativa es mucho más útil resolver pc-contabilidad-07.corp.ejemplo.es que buscar su IP en la tabla de leases. Cuando DHCP y DNS comparten información de forma controlada, la red gana observabilidad.

37.3. Alta disponibilidad con Kea

Kea soporta alta disponibilidad tanto para DHCPv4 como para DHCPv6 mediante un modelo hot-standby. Esta arquitectura se diferencia del mecanismo histórico de ISC y debe diseñarse expresamente; no se debe asumir que una configuración HA antigua migra automáticamente.

Aspecto	Kea
Rol	Primary / Secondary con hot standby.
Ámbito	DHCPv4 y DHCPv6.
Sincronización	Puede utilizar la red SYNC.

Aspecto	Kea
Seguridad	La comunicación de HA puede protegerse con TLS.
Estado	Visible en las páginas de leases/estado correspondientes.

La alta disponibilidad DHCP depende también de hora coherente entre nodos. Una diferencia temporal significativa puede impedir que los peers se comuniquen correctamente.

37.4. Migrar desde ISC sin convertir el cambio en incidente

1. Inventariar pools, mapeos, opciones personalizadas y dependencias existentes.
2. Identificar funciones usadas que puedan comportarse de forma distinta.
3. Crear un backup completo de configuración.
4. Planificar una ventana con consola disponible.
5. Cambiar el backend en un entorno de prueba o durante la ventana acordada.
6. Renovar clientes representativos y comprobar leases.
7. Validar registro DNS, PXE/VoIP u opciones especiales.
8. En HA, configurar el modelo Kea específico en ambos nodos y verificar heartbeat/estado.

En producción

No mantengas ISC únicamente porque «siempre ha funcionado». Está deprecado. Pero tampoco migres a ciegas: primero identifica las opciones concretas que tu red utiliza y valida su equivalente en Kea.

Capítulo 38. DHCP Relay: cuando el servidor está en otra red

Los mensajes iniciales DHCPv4 nacen como broadcast y los routers no reenvían broadcasts de forma ordinaria. Si el servidor se encuentra en otra subred, un relay recibe la solicitud local y la convierte en una comunicación encaminable hacia el servidor remoto.

```
Cliente VLAN 30
  DHCP broadcast
      ↓
pfSense / relay
      ↓ unicast
Servidor DHCP central
      ↓
Respuesta → relay → cliente
```

38.1. Servidor local frente a relay

Modelo	Ventaja	Coste
DHCP en pfSense	Simple, cercano y con menos dependencias.	La lógica DHCP queda distribuida si hay muchos firewalls.
Relay a servidor central	Centraliza scopes y administración.	Añade dependencia de routing, firewall y servidor remoto.
Servidor por sede	Autonomía local.	Más instancias que mantener.

En pfSense, un mismo protocolo no puede utilizar simultáneamente el servidor DHCP y el relay de forma incompatible sobre las interfaces correspondientes. El diseño debe decidir quién es la autoridad DHCP.

38.2. Diagnóstico de relay

Cuando un cliente remoto no obtiene dirección, debemos comprobar dos tramos: cliente→relay y relay→servidor. Capturar solo junto al servidor puede ocultar que el broadcast nunca alcanzó el relay; capturar solo en la VLAN puede ocultar un bloqueo posterior.

```
Prueba A: ¿llega DHCPDISCOVER al interfaz cliente?
Prueba B: ¿sale la solicitud relay hacia el servidor?
Prueba C: ¿responde el servidor?
Prueba D: ¿la respuesta vuelve al cliente?
```

Capítulo 39. IPv6: SLAAC, DHCPv6 y Router Advertisements

IPv6 separa funciones que en IPv4 solemos agrupar mentalmente bajo DHCP. Un host IPv6 descubre routers mediante Router Advertisements (RA). DHCPv6 puede entregar direcciones y otros parámetros, pero no entrega el gateway. Este detalle es fundamental.

Idea clave

En IPv6, «tengo DHCPv6» no implica «tengo router». El siguiente salto se aprende mediante RA. Si se bloquea ICMPv6 o se configura RA de forma incoherente, un cliente puede tener una dirección global y aun así no disponer de conectividad útil.

39.1. SLAAC

Con SLAAC, el router anuncia un prefijo y el host construye su propia dirección. Este modelo reduce dependencia de un servidor de concesiones, pero cambia la forma en la que el administrador observa y controla las direcciones.

39.2. DHCPv6

DHCPv6 puede asignar direcciones y proporcionar información adicional. En pfSense, para que los clientes utilicen DHCPv6, los Router Advertisements deben configurarse de forma compatible, por ejemplo en modos Managed o Assisted según el objetivo.

Mecanismo	Dirección	Gateway	Información adicional
SLAAC	Sí, derivada del prefijo anunciado.	RA	RA/RDNSS según diseño.
DHCPv6	Sí, si es stateful.	RA	DNS y otros parámetros DHCPv6.
RA	No es un servidor de leases.	Sí	Prefijos, flags y datos de router.

39.3. El caso Android

Algunos sistemas móviles, especialmente Android, no implementan un cliente DHCPv6 stateful del modo en que lo hacen otros sistemas y dependen de SLAAC para obtener dirección IPv6. Un diseño que obligue exclusivamente a DHCPv6 puede dejar fuera a estos clientes.

39.4. Prefix Delegation y Track Interface

Un ISP puede entregar a pfSense un prefijo IPv6 mediante DHCPv6 Prefix Delegation. Las interfaces internas pueden derivar subredes de ese prefijo mediante mecanismos de seguimiento. Esto permite adaptar la LAN al prefijo delegado sin introducir manualmente cada red.

```
ISP entrega 2001:db8:1234:5600::/56
                ↓
pfSense recibe Prefix Delegation
  ↓          ↓          ↓
USERS /64    SERVERS /64    GUEST /64
```

Error frecuente

Tratar IPv6 como «IPv4 con direcciones largas» y bloquear ICMPv6 indiscriminadamente. NDP, Router Solicitation, Router Advertisement y Path MTU Discovery dependen de ICMPv6. Romperlo puede generar fallos difíciles de interpretar.

Capítulo 40. DNS Resolver y DNS Forwarder: dos modelos distintos

pfSense incluye dos servicios DNS base con filosofías diferentes. DNS Resolver utiliza Unbound y puede resolver de forma recursiva o actuar como forwarder. DNS Forwarder utiliza dnsmasq y solo reenvía consultas. En instalaciones actuales, Unbound es el servicio predeterminado.

40.1. Resolver recursivo

En modo resolver, Unbound recorre la jerarquía DNS: parte de los servidores raíz, localiza los servidores del TLD y termina consultando a los autoritativos del dominio. No depende de un DNS recursivo de terceros para obtener la respuesta.

```
Cliente → Unbound
          ↓
        raíz
          ↓
        .com/.es/...
          ↓
      autoritativo
          ↓
     respuesta + caché
```

40.2. Forwarding

En modo forwarding, Unbound envía la consulta a los servidores DNS configurados en el sistema o aprendidos mediante interfaces dinámicas. Este modelo puede ser conveniente con DNS over TLS o en determinados diseños Multi-WAN.

Modo	Quién hace la recursión	Ventaja típica
Unbound resolver	El propio firewall	Independencia de forwarders externos y validación DNSSEC.
Unbound forwarding	Servidor upstream	Control de salida, DoT y estrategias Multi-WAN.
dnsmasq	Servidor upstream	Forwarder ligero; no actúa como resolver recursivo.

Qué ocurre realmente

Cuando el cliente pregunta a pfSense por www.ejemplo.es, la WebGUI no 'busca la web'. El daemon DNS recibe una consulta estructurada, decide si puede responder desde caché y, si no, ejecuta el modelo de resolución configurado.

40.3. Caché

La caché reduce latencia y consultas externas. También introduce una consecuencia operativa: después de cambiar un registro, distintos niveles de caché pueden seguir devolviendo el dato anterior hasta que caduque su TTL o se purgue expresamente.

Aplicación/navegador → caché del SO → caché de pfSense → caché/upstream → autoritativo

40.4. DNSSEC

DNSSEC permite validar criptográficamente cadenas de confianza para determinados datos DNS. No cifra la consulta; valida autenticidad e integridad de las respuestas firmadas. Confundir DNSSEC con privacidad DNS es un error conceptual.

Tecnología	Protege principalmente
DNSSEC	Autenticidad/integridad de datos DNS firmados.
DNS over TLS	Confidencialidad del canal entre cliente/forwarder y servidor DoT.
DNS over HTTPS	Confidencialidad mediante HTTPS, normalmente a puerto 443.
Firewall DNS	Control de quién puede consultar a quién.

40.5. Host Overrides y Domain Overrides

Los overrides permiten introducir conocimiento local que el DNS público no tiene o delegar dominios concretos a resolvers específicos. Son especialmente útiles en split DNS, Active Directory, laboratorios y servicios internos.

En producción
Antes de añadir un override, documenta qué problema resuelve. Un override abandonado puede sobrevivir años y explicar por qué solo una parte de la empresa resuelve un nombre hacia una IP antigua.

Capítulo 41. Diseñar DNS interno sin crear una caja negra

DNS suele convertirse en una dependencia invisible porque casi todas las aplicaciones lo utilizan y pocas muestran claramente que están esperando una resolución. Un diseño mantenible debe decidir quién consulta a quién y qué nombres son internos, públicos o divididos.

41.1. Split DNS

Split DNS permite que el mismo nombre tenga una respuesta interna y otra pública. Por ejemplo, portal.ejemplo.es puede resolver a 10.30.0.20 desde la empresa y a una IP pública desde Internet. Esto evita obligar a los clientes internos a salir y volver mediante NAT reflection.

41.2. Active Directory y DNS

En una red con Active Directory, los clientes de dominio suelen necesitar consultar los DNS del dominio para localizar controladores mediante registros SRV y otros datos específicos. Forzar que todos los clientes pregunten directamente a un resolver genérico puede romper autenticación y descubrimiento de servicios.

```
PC de dominio → DNS AD → zonas AD
                  ↓
          forwarders/resolver
                  ↓
              Internet
```

pfSense puede seguir participando como resolver aguas arriba, router y firewall, pero el flujo DNS debe respetar la autoridad del dominio.

41.3. Bloquear o redirigir DNS externo

Una organización puede decidir que los clientes solo utilicen resolvers autorizados. Para ello puede bloquear consultas DNS directas hacia Internet o, con cuidado, redirigir tráfico destinado a puerto 53 hacia el resolver local.

> **Límite práctico**
> Bloquear UDP/TCP 53 no obliga a una aplicación moderna a usar tu DNS si utiliza DoH a través de HTTPS. El control de DNS cifrado exige políticas de endpoint, listas de destinos, proxy/inspección cuando sea apropiado o gestión del navegador.

41.4. DNS rebinding

La protección frente a DNS rebinding busca impedir que una respuesta DNS externa haga que un nombre aparentemente público resuelva hacia direcciones privadas de la red local en circunstancias peligrosas. Algunas aplicaciones legítimas requieren excepciones, que deben ser específicas y documentadas.

41.5. Diagnóstico DNS por preguntas

Pregunta	Prueba
¿El cliente llega al resolver?	Captura o consulta directa a la IP del DNS.
¿El resolver recibe la consulta?	Logs/query logging temporal.
¿Responde desde caché?	Repetir consulta y observar tiempos/estado.
¿Puede resolver aguas arriba?	Consulta desde el propio firewall.
¿Falla solo un dominio?	Comparar autoritativos, DNSSEC, overrides y TTL.
¿Solo falla un cliente?	Vaciar caché local y comparar DNS configurado.

Capítulo 42. NTP y Dynamic DNS: tiempo e identidad externa

NTP y Dynamic DNS parecen servicios menores, pero resuelven dos problemas fundamentales: saber qué hora es y saber cómo encontrar un firewall cuya IP pública puede cambiar.

42.1. NTP: coherencia temporal

pfSense puede sincronizar su reloj con servidores NTP externos y también ofrecer servicio NTP a redes internas. Para robustez se recomienda utilizar varias fuentes de tiempo independientes en lugar de una única referencia.

Uso de la hora	Por qué importa
Logs	Permite correlacionar sucesos entre dispositivos.
TLS/certificados	La validez depende de intervalos temporales.
VPN/autenticación	Protocolos y tokens pueden rechazar desviaciones.
HA	Algunos mecanismos requieren relojes cercanos.
Forense	Una línea temporal incorrecta invalida análisis.

42.2. Servir NTP a clientes internos

El daemon NTP puede escuchar en interfaces seleccionadas. Esto permite que servidores, switches, AP o clientes utilicen una fuente temporal local y que el firewall concentre la sincronización externa.

> **Seguridad**
> No expongas NTP sin necesidad sobre interfaces externas. Como cualquier servicio de red, debe escuchar solo donde tenga un propósito operativo.

42.3. Dynamic DNS

Dynamic DNS mantiene actualizado un registro DNS cuando cambia una dirección WAN. El objetivo es proporcionar un nombre estable —por ejemplo vpn-sede01.ejemplo.net— aunque el proveedor entregue una IP dinámica.

```
WAN cambia 203.0.113.10 → 203.0.113.47
            ↓
pfSense detecta el nuevo valor
            ↓
Actualiza proveedor DDNS
            ↓
vpn-sede01.ejemplo.net → 203.0.113.47
```

42.4. WAN detrás de NAT

Si pfSense recibe una dirección privada en WAN porque existe un router anterior, la IP de la interfaz no coincide con la IP pública. Los clientes DDNS pueden utilizar servicios de comprobación de IP externa para publicar la dirección real observada desde Internet.

Error frecuente

Dynamic DNS no elimina el CGNAT. Si el operador no entrega una dirección pública enrutable hacia el cliente, actualizar un nombre con la IP pública compartida no crea automáticamente una ruta entrante hasta tu firewall.

42.5. RFC 2136

Además de proveedores DDNS basados en HTTP/HTTPS, pfSense puede realizar actualizaciones DNS dinámicas mediante RFC 2136. Este modelo resulta útil cuando la organización controla directamente un servidor DNS autoritativo compatible.

Capítulo 43. Otros servicios de red y control de acceso

pfSense incorpora otros servicios que pueden ser valiosos, pero no deben activarse por costumbre. Cada uno responde a una necesidad concreta y modifica la superficie funcional o de seguridad del firewall.

43.1. SNMP

SNMP permite que una plataforma de monitorización recoja métricas del firewall. Antes de habilitarlo, deben definirse versión, redes de origen permitidas y qué plataforma consumirá la información. En redes actuales, versiones con autenticación y cifrado son preferibles cuando el ecosistema lo permite.

43.2. UPnP IGD y PCP

UPnP IGD y PCP permiten que determinados clientes soliciten mapeos de puertos de forma automática. Esto facilita consolas, juegos y algunas aplicaciones, pero reduce el control manual del administrador sobre las publicaciones.

Seguridad
En una red empresarial no se debería permitir a cualquier host crear aperturas hacia sí mismo sin una política clara. Si UPnP/PCP es necesario, limítalo por interfaz, red y ACL en lugar de habilitarlo de forma global.

43.3. Wake on LAN

Wake on LAN permite enviar magic packets a equipos preparados para despertar desde un estado de bajo consumo. Su fiabilidad depende de NIC, BIOS/UEFI, switch, VLAN y del estado eléctrico del host.

43.4. IGMP Proxy

IGMP Proxy puede facilitar determinados flujos multicast entre interfaces, por ejemplo ciertos servicios IPTV. No sustituye un diseño multicast completo y debe configurarse entendiendo qué red actúa como upstream y cuáles como downstream.

43.5. Captive Portal: acceso condicionado antes de Internet

Captive Portal obliga a los clientes de una interfaz o zona a pasar por una página de acceso antes de obtener conectividad normal. Puede funcionar como aceptación simple, con usuarios locales, con RADIUS o mediante vouchers temporales. Es útil en invitados, hospitality y accesos controlados, pero no sustituye la seguridad Wi-Fi, la segmentación ni una identidad corporativa robusta.

Hay una limitación especialmente importante en el diseño actual: Captive Portal no es compatible con IPv6. Una red de invitados dual stack mal planteada puede permitir que el tráfico IPv6 evite la experiencia de portal prevista. Por ello el comportamiento IPv4/IPv6 debe decidirse y probarse explícitamente antes de desplegar el servicio.

43.6. Traffic shaping y limiters: controlar cola, no fabricar ancho de banda

pfSense dispone de mecanismos de traffic shaping y de limiters. Los limiters utilizan dummynet y permiten aplicar límites de caudal por tráfico, dirección, host o red; además pueden combinarse con colas y algoritmos de gestión activa. Son especialmente útiles para invitados, enlaces saturables y políticas donde se necesita limitar por IP o por segmento.

Para problemas de bufferbloat, FQ_CODEL puede ayudar a mantener la latencia bajo carga cuando se configura con valores de ancho de banda realistas. La metodología correcta es medir primero, limitar ligeramente por debajo de la capacidad efectiva cuando proceda y volver a medir latencia, pérdida y throughput. Un shaper mal dimensionado puede convertirse él mismo en el cuello de botella.

Capítulo 44. Laboratorio: servicios de infraestructura para una pyme segmentada

Retomaremos la empresa de 70 usuarios de las partes anteriores. El firewall ya dispone de VLAN y reglas base. Ahora construiremos una capa de servicios coherente sin mezclar responsabilidades.

44.1. Topología

VLAN	Red	Servicio
MGMT 10	10.10.0.0/24	DHCP limitado o reservas; DNS interno; NTP.
USERS 20	10.20.0.0/24	Kea DHCP; DNS corporativo; NTP.
SERVERS 30	10.30.0.0/24	Preferencia por estáticos/reservas; DNS interno.
IOT 40	10.40.0.0/24	DHCP independiente; DNS filtrado; sin acceso lateral.
GUEST 50	10.50.0.0/24	DHCP corto; DNS controlado; Internet únicamente.
VOICE 60	10.60.0.0/24	DHCP con opciones específicas si la telefonía lo requiere.

44.2. Diseño DHCP

1. Seleccionar Kea como backend.
2. Definir un pool distinto por VLAN y excluir el espacio reservado a infraestructura.
3. Crear mapeos para equipos que necesitan identidad estable.
4. Configurar tiempos de lease acordes al tipo de red.
5. Definir DNS entregado a cada VLAN según su función.
6. Probar renovación, liberación y reobtención desde clientes reales.

44.3. Diseño DNS

USERS y MGMT utilizan DNS corporativo interno; GUEST e IOT consultan Unbound en pfSense bajo una política separada. Los equipos de dominio no saltan directamente a resolvers públicos porque necesitan los registros de Active Directory.

```
USERS → DNS AD → pfSense/Unbound → Internet
MGMT  → DNS AD → pfSense/Unbound → Internet
IOT   → pfSense/Unbound → Internet
GUEST → pfSense/Unbound → Internet
```

44.4. IPv6

Si el ISP delega un /56, cada VLAN interna obtiene un /64. pfSense anuncia los prefijos mediante RA y se elige SLAAC, DHCPv6 o modo Assisted según los clientes. Antes de activar IPv6 globalmente se replican las políticas de seguridad existentes en IPv4.

44.5. NTP

Todos los dispositivos de infraestructura usan el firewall como referencia local o comparten las mismas fuentes NTP autorizadas. Los logs de firewall, switch, AP, hipervisor y servidores deben poder correlacionarse.

44.6. Dynamic DNS

La VPN de administración usa vpn-empresa.ejemplo.net. El cliente DDNS actualiza el registro cuando cambia la WAN. Si la sede estuviera tras CGNAT, el diseño se replantearía porque DDNS no resuelve la ausencia de entrada enrutable.

44.7. Matriz de validación

Prueba	Resultado esperado
Cliente USERS renueva DHCP	Obtiene IP, /24, gateway y DNS correctos.
Cliente GUEST	Recibe lease corto y no resuelve nombres internos protegidos.
PC de dominio	Localiza registros SRV de AD.
Consulta externa	Unbound responde y utiliza caché.
Nombre interno	Devuelve IP privada prevista.
IPv6 SLAAC	Obtiene /64 y router por RA.
NTP	Firewall y clientes muestran hora coherente.
DDNS	El nombre público coincide con la WAN pública prevista.
Fallo DNS simulado	IP externa funciona mientras nombre falla; diagnóstico identifica DNS.
Reinicio firewall	Servicios vuelven y las concesiones se mantienen según backend/configuración.

Resultado del laboratorio

Una red de producción no se considera sana porque un navegador abra una web. Debemos poder demostrar, por separado, que identidad IP, gateway, DNS, tiempo, resolución interna, conectividad IPv6 y publicación DDNS funcionan como se diseñaron.

Capítulo 45. Troubleshooting de servicios: convertir síntomas en pruebas

Los servicios de infraestructura generan fallos engañosos porque una dependencia rota se manifiesta en otra capa. El método correcto es separar adquisición de parámetros, transporte, resolución y aplicación.

45.1. El cliente recibe 169.254.x.x

En Windows, una dirección APIPA sugiere que el cliente no obtuvo una concesión DHCPv4. No debemos empezar modificando DNS. Primero se investiga enlace, VLAN, broadcast, servidor o relay.

45.2. Hay IP, pero no nombres

Si un cliente alcanza una dirección externa pero no resuelve nombres, routing y parte del firewall ya funcionan. La investigación debe concentrarse en DNS: servidor configurado, reachability al puerto 53/DoT según diseño, overrides, DNSSEC y upstream.

45.3. pfSense resuelve, el cliente no

Este patrón indica que la salida DNS del firewall funciona. La diferencia está entre cliente y resolver: DHCP entregó otro DNS, una regla bloquea la consulta, el cliente tiene una VPN/agente local o existe caché incorrecta.

45.4. IPv6 tiene dirección pero no navega

Comprobar RA, default router, reglas IPv6, DNS IPv6, MTU/ICMPv6 y ruta upstream. Tener una dirección global no prueba que exista una ruta por defecto funcional.

45.5. DDNS muestra la IP equivocada

Comparar dirección de la interfaz WAN con la IP observada desde Internet. Si difieren, existe NAT upstream. Después verificar qué método de detección utiliza el cliente DDNS.

45.6. Comandos y observación

```
Windows:
  ipconfig /all
  ipconfig /release
  ipconfig /renew
  ipconfig /flushdns
  nslookup nombre servidor_dns

Linux/Unix:
  ip addr / ip route
  resolvectl status
  dig @servidor nombre
  drill nombre

pfSense/Unbound:
  unbound-control -c /var/unbound/unbound.conf reload
  unbound-control -c /var/unbound/unbound.conf flush <nombre>
```

Método
Captura donde esperas que ocurra el evento. Para DHCP, observa el dominio de broadcast y, si hay relay, también la salida hacia el servidor. Para DNS, captura entre cliente y resolver y, si hace falta, entre resolver y upstream. Una captura en el lugar equivocado puede demostrar únicamente que estás mirando el lugar equivocado.

Glosario de la Parte VI

Término	Definición
DORA	Secuencia DHCPv4 Discover, Offer, Request, Acknowledge.
Lease	Concesión temporal de parámetros DHCP.
Kea	Servidor DHCP moderno utilizado por pfSense como backend recomendado.
ISC DHCP	Backend histórico deprecado.
DHCP Relay	Intermediario que lleva solicitudes DHCP entre subredes.
SLAAC	Autoconfiguración IPv6 basada en anuncios de router.
RA	Router Advertisement; anuncia router y parámetros IPv6.
Prefix Delegation	Delegación de un prefijo IPv6 a otro router.

Término	Definición
Unbound	Resolver DNS recursivo/forwarder usado por DNS Resolver.
dnsmasq	Daemon utilizado por DNS Forwarder.
DNSSEC	Extensiones DNS para validar autenticidad/integridad de datos firmados.
Split DNS	Respuestas DNS diferentes según contexto interno/externo.
NTP	Protocolo de sincronización de tiempo.
Dynamic DNS	Actualización automática de un registro DNS cuando cambia una IP.
RFC 2136	Mecanismo estandarizado para actualizaciones dinámicas de DNS.
UPnP/PCP	Protocolos que permiten solicitar mappings de red de forma automatizada.

Fuentes técnicas de contraste

Las siguientes páginas oficiales se han utilizado para verificar el comportamiento vigente de los servicios descritos. Verificación técnica: 8 de octubre de 2026.

- **DHCP — visión general y backends:** https://docs.netgate.com/pfsense/en/latest/services/dhcp/index.html
- **DHCPv4 Server:** https://docs.netgate.com/pfsense/en/latest/services/dhcp/ipv4.html
- **Kea Settings:** https://docs.netgate.com/pfsense/en/latest/services/dhcp/kea-settings.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
- **DNS Resolver:** https://docs.netgate.com/pfsense/en/latest/services/dns/resolver.html
- **DNS Resolver Configuration:** https://docs.netgate.com/pfsense/en/latest/services/dns/resolver-config.html
- **DNS Resolver Modes:** https://docs.netgate.com/pfsense/en/latest/services/dns/resolver-modes.html
- **DNS Forwarder:** https://docs.netgate.com/pfsense/en/latest/services/dns/forwarder.html
- **Troubleshooting DNS Queries:** https://docs.netgate.com/pfsense/en/latest/troubleshooting/dns-queries.html
- **Troubleshooting DNS Cache:** https://docs.netgate.com/pfsense/en/latest/troubleshooting/dns-cache.html
- **NTP Server Configuration:** https://docs.netgate.com/pfsense/en/latest/services/ntpd/server.html
- **Dynamic DNS:** https://docs.netgate.com/pfsense/en/latest/services/dyndns/index.html
- **Configuring a Dynamic DNS Client:** https://docs.netgate.com/pfsense/en/latest/services/dyndns/client.html

- Captive Portal: https://docs.netgate.com/pfsense/en/latest/captiveportal/index.html
- Captive Portal Vouchers: https://docs.netgate.com/pfsense/en/latest/captiveportal/vouchers.html
- Traffic Shaper / Limiters: https://docs.netgate.com/pfsense/en/latest/trafficshaper/limiters.html
- CoDel Limiters for Bufferbloat: https://docs.netgate.com/pfsense/en/latest/recipes/codel-limiters.html
- **Services overview:** https://docs.netgate.com/pfsense/en/latest/services/index.html
- **Kea HA conversion:** https://docs.netgate.com/pfsense/en/latest/recipes/high-availability-kea-convert.html

Cierre de la Parte VI

Con los servicios base dominados, el firewall ya no es únicamente un punto de paso: se ha convertido en parte de la infraestructura que configura, resuelve, sincroniza y da identidad a los clientes. La siguiente parte abordará una capa todavía más sensible: VPN, criptografía, certificados, acceso remoto y túneles entre sedes.

pfSense® software

REDES, FIREWALL Y SEGURIDAD

Arquitectura, administración y laboratorios prácticos

PARTE VII

VPN, criptografía y acceso seguro

Oscar de la Cuesta

palentino.es



Primera edición · octubre de 2026

Apertura de la Parte VII

Hasta aquí el libro ha construido un firewall funcional, una topología segmentada, una política de filtrado y una capa de servicios de infraestructura. La siguiente pregunta es inevitable: ¿cómo conectamos de forma segura usuarios, sedes y redes que ya no comparten el mismo medio físico?

Una VPN no es simplemente «un túnel cifrado». Es una combinación de identidad, autenticación, negociación criptográfica, encapsulación, rutas, reglas de firewall, resolución DNS y políticas de acceso. Una VPN puede negociar perfectamente y, aun así, no transportar el tráfico esperado. También puede transportar tráfico y estar mal diseñada desde el punto de vista de identidad o privilegios.

Principio de esta parte

No elegiremos WireGuard, OpenVPN o IPsec por popularidad. Primero definiremos requisitos: quién se conecta, desde dónde, con qué identidad, qué redes necesita, qué interoperabilidad existe, cómo se revoca acceso y qué rendimiento se espera. Después elegiremos la tecnología.

Mapa de la Parte VII

Capítulo	Objetivo
46	Entender qué resuelve realmente una VPN y qué no.
47	Construir una base de criptografía y PKI suficiente para administrar VPN con criterio.
48	Elegir entre WireGuard, OpenVPN e IPsec según requisitos.
49	Diseñar y operar WireGuard.
50	Diseñar y operar OpenVPN.
51	Diseñar y operar IPsec con especial atención a IKEv2 y VTI.
52	Acceso remoto, identidades, RADIUS/LDAP, certificados y MFA.
53	Site-to-site, rutas, DNS y redes solapadas.
54	Rendimiento, Multi-WAN, HA y operación segura.
55	Troubleshooting y laboratorio integral.

Capítulo 46. Qué resuelve una VPN

Una VPN crea una relación lógica entre extremos que pueden estar separados por Internet, por una red de operador o incluso por varias capas de NAT. Esa relación permite transportar tráfico que, desde el punto de vista de los hosts, pertenece a redes privadas o a una interfaz virtual.

46.1. Las cinco preguntas de cualquier VPN

Pregunta	Ejemplo
¿Quién es el peer?	Firewall de la sede B, portátil de Ana, teléfono del técnico.
¿Cómo demuestra su identidad?	Clave pública, certificado, usuario/contraseña, RADIUS, EAP.
¿Qué protege el canal?	Algoritmos de cifrado e integridad acordados.
¿Qué tráfico entra al túnel?	Redes, Allowed IPs, selectors, rutas o default route.
¿Qué puede hacer al salir del túnel?	Reglas PF, segmentación y permisos por identidad/red.

Separar estas preguntas evita un error habitual: creer que autenticar un peer equivale a autorizar todo su tráfico. La criptografía demuestra o protege; el firewall aplica política.

46.2. Plano exterior y plano interior

```
PAQUETE EXTERIOR
IP pública A ── Internet ── IP pública B
        [ UDP/ESP + datos cifrados ]
                  ↓ descifrado
PAQUETE INTERIOR
10.20.0.15 ──────────────→ 10.80.0.20
```

El paquete exterior permite que Internet transporte el túnel. El paquete interior es el tráfico que realmente queremos comunicar. Las reglas que permiten establecer una VPN y las reglas que gobiernan el tráfico dentro de ella son responsabilidades diferentes.

Qué ocurre realmente

Que UDP 51820, UDP 1194 o IKE lleguen a WAN solo permite que el protocolo de VPN intente establecerse. Después del descifrado, PF todavía debe decidir si el tráfico interno puede pasar.

46.3. Remote access y site-to-site

Modelo	Identidad dominante	Rutas típicas
Acceso remoto	Usuario/dispositivo	Pool de túnel hacia redes corporativas.
Site-to-site	Firewall/peer remoto	Subredes completas de ambos extremos.
Hub-and-spoke	Sedes contra un concentrador	Rutas por sede; posible tránsito por hub.
Full mesh	Cada sede con varias sedes	Mayor número de peers y complejidad.
VPN de salida	Firewall hacia proveedor VPN	Default route o políticas selectivas.

46.4. Split tunnel frente a full tunnel

En split tunnel solo se envían por la VPN las redes corporativas definidas. En full tunnel, el cliente utiliza la VPN también para Internet. Ninguno es universalmente superior: el full tunnel ofrece mayor control central, pero consume ancho de banda y puede introducir latencia; el split tunnel reduce carga, pero el endpoint conserva tráfico directo a Internet.

Seguridad
El full tunnel no convierte en seguro un endpoint comprometido, y el split tunnel no es automáticamente inseguro. La decisión debe combinar EDR, postura del dispositivo, DNS, acceso a recursos y capacidad de monitorización.

Capítulo 47. Criptografía y PKI para administradores de red

No hace falta ser criptógrafo para administrar una VPN, pero sí entender qué secreto protege cada mecanismo. El objetivo de este capítulo es reconocer los componentes y evitar errores operativos como compartir una clave privada, reutilizar una CA indiscriminadamente o confundir cifrado con autenticación.

47.1. Cifrado simétrico y asimétrico

Tipo	Idea	Uso VPN
Simétrico	La misma clave protege y recupera los datos.	Cifrado eficiente del tráfico de datos.
Asimétrico	Par de clave pública y privada.	Identidad, intercambio/establecimiento y firmas.
Hash/MAC	Comprueba integridad/autenticidad según mecanismo.	Detectar alteraciones y autenticar mensajes.
KDF	Deriva claves a partir de material secreto.	Generar claves de sesión separadas.

En una VPN moderna la criptografía asimétrica ayuda a establecer confianza o claves de sesión, mientras que el tráfico masivo se protege con algoritmos simétricos mucho más eficientes.

47.2. Perfect Forward Secrecy

PFS persigue que la pérdida futura de una clave de larga duración no permita descifrar automáticamente sesiones históricas capturadas. Se consigue derivando material efímero durante la negociación en lugar de reutilizar una única clave para todo.

47.3. Qué es una PKI

```
        CA
    /   |    \
 servidor  usuario1  usuario2
certificado certificado certificado
   + clave privada en cada titular
```

Una autoridad certificadora firma certificados. El certificado contiene información pública y una clave pública; la clave privada correspondiente debe permanecer bajo control del titular. La clave privada de la CA merece una protección todavía mayor porque permite emitir identidades que los sistemas confiarán.

Regla crítica

Para distribuir confianza se entrega el certificado de la CA. No se distribuye la clave privada de la CA. Si esa clave se compromete, un atacante puede crear certificados que parezcan legítimos para toda la PKI.

47.4. Certificado de servidor y certificado de usuario

El certificado de servidor demuestra la identidad del concentrador VPN. Un certificado de usuario o dispositivo identifica a un cliente concreto. Utilizar certificados individuales permite revocar uno sin reemplazar los de todos los demás.

47.5. Revocación mediante CRL

Cuando un portátil se pierde o un empleado deja la organización, esperar a que caduque su certificado puede ser inaceptable. Una Certificate Revocation List permite declarar que un certificado previamente válido ya no debe aceptarse.

En producción

La capacidad de revocar es parte del diseño inicial. No esperes al primer equipo perdido para descubrir que todos los usuarios comparten la misma identidad criptográfica.

47.6. Renovar, reemitir y caducar

Los certificados no son permanentes. Una política de ciclo de vida debe contemplar duración, renovación, sustitución de claves, revocación y distribución del nuevo material. El inventario de certificados es una tarea operativa, no únicamente criptográfica.

Capítulo 48. Elegir tecnología: WireGuard, OpenVPN o IPsec

pfSense ofrece varias familias de VPN. Las tres principales pueden resolver site-to-site y distintos escenarios de acceso remoto, pero no comparten el mismo modelo de identidad, automatización ni interoperabilidad.

Criterio	WireGuard	OpenVPN	IPsec
Modelo	Peers y cryptokey routing	Servidor/cliente sobre TLS	Estándares IKE/IPsec
Transporte	UDP	UDP o TCP; normalmente UDP	IKE UDP 500/4500 + ESP/NAT-T
Identidad	Claves públicas por peer	Certificados y/o usuarios	PSK, certificados, EAP, RADIUS…
Cliente nativo SO	Variable	Normalmente app	IKEv2 nativo en muchos SO
Interoperabilidad appliance	Media	Media	Muy alta
Configuración masiva	Más manual	Muy flexible	Flexible, pero compleja
Routing dinámico	Posible con diseño	Posible	VTI facilita integración
MFA de usuario	No nativo	Sí vía autenticación externa	Sí según EAP/RADIUS
Facilidad conceptual	Alta al inicio	Media	Menor por número de conceptos

48.1. Cuándo elegir WireGuard

- Túneles simples entre peers bajo nuestro control.
- Necesidad de buen rendimiento con configuración compacta.
- Site-to-site donde la gestión de claves y Allowed IPs es asumible.
- Acceso remoto pequeño o mediano cuando no se necesita autenticación de usuario centralizada en el propio protocolo.

48.2. Cuándo elegir OpenVPN

- Acceso remoto con certificados, usuario/contraseña y RADIUS/LDAP.
- Necesidad de empujar rutas, DNS y múltiples parámetros al cliente.
- Entornos donde atravesar NAT y firewalls restrictivos es prioritario.
- Organizaciones que necesitan un modelo de gestión de usuarios y clientes muy flexible.

48.3. Cuándo elegir IPsec

- Interoperabilidad site-to-site con routers y firewalls de terceros.
- Uso de clientes IKEv2 integrados en sistemas operativos.
- Necesidad de VTI y routing dinámico con una semántica de interfaz enrutada.
- Entornos donde IPsec es un requisito corporativo o contractual.

Decisión profesional

La mejor VPN es la que cumple requisitos de identidad, interoperabilidad, revocación, rutas y operación con la menor complejidad necesaria. Un benchmark de throughput no decide por sí solo una arquitectura.

Capítulo 49. WireGuard: simple en la superficie, preciso en el routing

WireGuard es una VPN de capa 3 con un conjunto pequeño de conceptos: interfaz/túnel, clave privada local, clave pública, peers, endpoint y Allowed IPs. Su simplicidad reduce opciones, pero obliga a entender muy bien el routing criptográfico.

En pfSense, WireGuard se utiliza mediante el paquete correspondiente, disponible para ediciones actuales de pfSense Plus y CE.

49.1. No hay cliente y servidor estrictos

WireGuard modela peers. Un extremo puede comportarse operativamente como servidor porque escucha siempre y el remoto inicia, pero el protocolo no define esos roles del mismo modo que OpenVPN.

49.2. Claves

Cada túnel local tiene una clave privada y su correspondiente clave pública. A cada peer se le configura la clave pública remota. Opcionalmente puede añadirse una pre-shared key como capa criptográfica adicional.

49.3. Allowed IPs: identidad de routing

Allowed IPs cumple dos papeles: asocia redes a un peer para la selección criptográfica y limita qué direcciones internas se consideran válidas para ese peer. En un túnel con varios peers, las redes no pueden solaparse arbitrariamente.

```
Peer SEDE-B
Public key: <clave pública B>
Allowed IPs:
  10.255.0.2/32     ← IP de túnel
  10.80.0.0/16      ← redes detrás de B
```

Error frecuente

Añadir 10.80.0.0/16 a Allowed IPs no crea necesariamente una ruta completa en la tabla del sistema. En pfSense las rutas adicionales deben diseñarse mediante interfaz asignada, gateway/rutas estáticas o routing dinámico según el caso.

49.4. Un peer por túnel frente a varios peers

Un único túnel con varios peers puede ser compacto, pero obliga a mantener listas Allowed IPs específicas y sin ambigüedad. Un túnel por peer simplifica determinados escenarios de routing dinámico y retorno, a costa de crear más interfaces lógicas.

49.5. Interfaz asignada y reglas

Asignar WireGuard como interfaz permite tratar un túnel concreto como una interfaz pfSense: reglas dedicadas, gateway, routing y comportamiento de retorno más explícito. Las reglas del grupo WireGuard son útiles para políticas comunes; las interfaces asignadas permiten granularidad.

49.6. NAT y keepalive

Un peer detrás de NAT puede necesitar Persistent Keepalive para conservar el mapeo del dispositivo intermedio cuando no hay tráfico durante un tiempo. No es un mecanismo de autenticación; únicamente mantiene actividad suficiente para que el estado NAT no desaparezca.

49.7. WireGuard de acceso remoto

Para teletrabajo, cada dispositivo recibe claves y una dirección de túnel. No existe autenticación de usuario integrada: revocar acceso significa eliminar o invalidar el peer y su clave. En organizaciones con cientos de usuarios, esa administración puede requerir herramientas adicionales.

Seguridad
Una configuración WireGuard exportada contiene material privado. Debe entregarse por un canal seguro, almacenarse como un secreto y eliminarse o revocarse cuando el dispositivo deja de estar autorizado.

Capítulo 50. OpenVPN: identidad, políticas y flexibilidad

OpenVPN combina transporte TLS, certificados X.509 y, si se desea, autenticación de usuario. Esta combinación lo hace especialmente útil en acceso remoto, donde la identidad puede necesitar revocarse por usuario y donde el servidor debe distribuir rutas, DNS y otros parámetros.

50.1. Modos de identidad

Modo conceptual	Qué demuestra el cliente	Uso
SSL/TLS	Certificado/clave	Dispositivos o usuarios con identidad criptográfica individual.
User Auth	Usuario/contraseña contra backend	Integración con RADIUS/LDAP; certificado individual no obligatorio.
SSL/TLS + User Auth	Certificado + credenciales	Mayor separación de factores y revocación.

Para acceso remoto, combinar identidad criptográfica individual con autenticación de usuario permite que la pérdida de una contraseña o de un certificado no sea, por sí sola, suficiente para suplantar al usuario.

50.2. tun frente a tap

El modo tun transporta capa 3 y es el enfoque natural para redes enrutadas. tap puede transportar Ethernet y habilitar bridging, pero añade broadcast, dependencia de capa 2 y peor compatibilidad en clientes móviles. Para diseños modernos, tun suele ser preferible.

50.3. Red del túnel y redes locales

El pool del túnel identifica a los clientes VPN. Las redes locales indican qué prefijos deben conocer los clientes. El hecho de empujar una ruta no crea permiso de firewall: solo enseña al cliente por dónde enviar el paquete.

```
Cliente recibe 10.250.0.10
Servidor empuja 10.20.0.0/24
    ↓
Cliente crea ruta hacia OpenVPN
    ↓
PF decide si 10.250.0.10 puede acceder a USERS/SERVERS
```

50.4. TLS key / tls-crypt y canal de control

OpenVPN puede proteger adicionalmente su canal de control con una clave compartida. Esto añade una barrera previa a la negociación TLS y reduce exposición frente a tráfico no autorizado.

50.5. DCO

Data Channel Offload mueve gran parte del procesamiento de datos cifrados al kernel y puede mejorar de forma importante el rendimiento. En pfSense, DCO es una característica de pfSense Plus; no está disponible en pfSense CE. No todas las opciones de OpenVPN son compatibles con DCO, por lo que debe validarse por túnel.

Rendimiento
DCO no cambia el protocolo que ve el peer; cambia cómo procesa el endpoint los datos. Aun así, determinadas funciones avanzadas de OpenVPN no son compatibles con su modelo actual, por lo que rendimiento y funcionalidad deben evaluarse juntos.

50.6. Exportar clientes

El paquete Client Export facilita generar configuraciones adecuadas para los distintos sistemas. Es una herramienta de distribución, no una excusa para enviar perfiles con claves privadas por correo sin protección.

50.7. Revocación

Los certificados individuales permiten revocar un dispositivo o usuario mediante una CRL. El servidor OpenVPN debe estar configurado para consultar la lista correspondiente. La baja de un usuario debe contemplar tanto credenciales como certificados.

Capítulo 51. IPsec: IKE, SA, políticas y VTI

IPsec no es un único protocolo, sino un conjunto de mecanismos que protegen tráfico IP. La negociación IKE establece asociaciones de seguridad y material criptográfico; después el tráfico se protege mediante IPsec, habitualmente ESP.

51.1. IKEv1 e IKEv2

IKEv2 es la elección moderna cuando ambos extremos lo soportan. Simplifica varios aspectos de negociación, movilidad y NAT y es la base recomendada para nuevos despliegues de acceso remoto actuales.

51.2. Phase 1 y Phase 2 como modelo operativo

En la interfaz de pfSense, Phase 1 representa principalmente la relación IKE entre peers: identidad, autenticación, algoritmos y gateway remoto. Phase 2 describe el tráfico protegido o el modo de interfaz que viajará bajo esa relación.

```
Phase 1: ¿quién eres y cómo protegemos la negociación?
Phase 2: ¿qué tráfico protegemos dentro de esa relación?
```

51.3. IKE, ESP y NAT-T

IKE utiliza normalmente UDP 500. Cuando hay NAT, NAT Traversal encapsula el tráfico IPsec sobre UDP 4500 para evitar problemas con ESP a través de dispositivos que traducen direcciones.

51.4. Policy-based frente a route-based VTI

Modelo	Cómo decide el tráfico	Ventaja
Policy-based	Selectors/local-remote networks	Muy interoperable y directo para pocas redes.
VTI	Interfaz de capa 3 + routing	Se integra mejor con rutas estáticas y protocolos dinámicos.

VTI separa la protección IPsec de la selección de rutas: el sistema enruta hacia una interfaz y el túnel protege ese tráfico. Esto resulta especialmente útil cuando existen muchas redes o routing dinámico.

51.5. Propuestas criptográficas

Los peers deben compartir propuestas compatibles. Ofrecer demasiados algoritmos antiguos «por compatibilidad» amplía superficie y dificulta saber qué se negoció. Conviene usar conjuntos modernos acordes con los endpoints y evitar algoritmos obsoletos.

Error frecuente

Un fallo de Phase 1 no se arregla tocando rutas internas. Un fallo de Phase 2 no se arregla cambiando la contraseña IKE al azar. Identifica primero en qué fase se interrumpe la negociación.

51.6. Mobile IPsec

pfSense soporta varios estilos de acceso remoto IPsec. En clientes modernos, IKEv2 es la opción preferente. EAP-MSCHAPv2 puede validar usuarios, EAP-RADIUS delega autenticación a RADIUS y EAP-TLS utiliza certificados individuales.

51.7. Clientes nativos

Una ventaja de IKEv2 es que Windows, macOS, iOS, Android moderno y muchos sistemas Linux disponen de clientes compatibles sin instalar un cliente OpenVPN o WireGuard específico, aunque las opciones exactas dependen del sistema.

Capítulo 52. Acceso remoto: identidades, RADIUS, LDAP y MFA

La VPN de teletrabajo es una puerta de entrada a la organización. Por eso la pregunta principal no es qué cifrado usa, sino cómo demuestra el usuario su identidad y cómo se revoca esa identidad cuando deja de ser válida.

52.1. Factores

Factor	Ejemplo
Algo que sabes	Contraseña/PIN.
Algo que tienes	Certificado, clave privada, token OTP, dispositivo.
Algo que eres	Biometría, cuando interviene en el sistema de identidad/endpoint.

La combinación certificado + credenciales de usuario ya separa dos elementos: posesión del material criptográfico y conocimiento de una contraseña. Un servidor RADIUS puede añadir un OTP o integrar otro mecanismo MFA.

52.2. Local Database

La base local funciona bien para laboratorios y despliegues pequeños. Su límite aparece cuando la organización ya posee un directorio corporativo y necesita altas, bajas, grupos y políticas centralizadas.

52.3. LDAP

LDAP permite consultar un directorio, pero el canal y los permisos del bind deben protegerse. No todos los protocolos VPN consumen LDAP directamente del mismo modo; en pfSense se integra a través de las fuentes de autenticación admitidas.

52.4. RADIUS

RADIUS es especialmente útil como capa AAA entre el firewall y un sistema de identidad. Puede integrar Active Directory/NPS, FreeRADIUS u otros proveedores y añadir atributos de autorización.

> **Seguridad**
> El enlace entre pfSense y RADIUS debe protegerse mediante una red de gestión confiable o un túnel. No asumas que el protocolo clásico RADIUS cifra todo su contenido.

52.5. OTP con FreeRADIUS

El paquete FreeRADIUS disponible en pfSense soporta mecanismos de contraseña de un solo uso. Puede utilizarse como ejemplo de MFA para OpenVPN y otros servicios que autentican contra RADIUS. En una empresa también puede delegarse MFA a una plataforma externa.

52.6. Onboarding y offboarding

Alta	Baja
Crear identidad nominal.	Deshabilitar identidad.
Emitir certificado/peer cuando proceda.	Revocar certificado/eliminar peer.
Asignar grupos/permisos mínimos.	Eliminar grupos/permisos.
Entregar perfil de forma segura.	Retirar perfiles de dispositivos gestionados.
Registrar propietario y dispositivo.	Conservar evidencia de revocación.

Principio de mínimo privilegio
Entrar por VPN no debe equivaler a «estar en la LAN». Crea grupos o redes de túnel que permitan únicamente los recursos que el rol necesita.

Capítulo 53. Site-to-site: routing, DNS y redes solapadas

Una VPN entre sedes suele ser estable durante años. Precisamente por eso conviene diseñarla con claridad: prefijos no solapados, routing de ida y vuelta, DNS interno y una política que sobreviva a futuras subredes.

53.1. Ruta de ida y ruta de vuelta

```
10.20.0.25 (Sede A)
  ↓ ruta a 10.80.0.0/16 por VPN
pfSense A === TÚNEL === pfSense B
                    ↓
                10.80.0.10
                  ↑
      debe existir retorno a 10.20.0.0/24
```

Que el paquete llegue a B no garantiza que la respuesta vuelva por el túnel. Las pruebas site-to-site deben validar ambos sentidos y comprobar que no existe una ruta por defecto que desvíe el retorno.

53.2. Redes solapadas

Dos sedes con 192.168.1.0/24 representan un problema de identidad: cuando un host intenta alcanzar 192.168.1.50, su sistema considera el destino local y ni siquiera lo envía al firewall. NAT dentro del túnel puede resolver ciertos casos, pero añade traducción y complejidad. La solución estratégica es renumerar cuando sea viable.

53.3. DNS entre sedes

La conectividad por IP no basta para una experiencia operativa útil. Los resolvers deben poder consultar las zonas remotas adecuadas, mediante forwarding condicional, Active Directory integrado u otra arquitectura coherente.

53.4. Dynamic routing

Cuando una organización tiene muchas redes, actualizar manualmente cada túnel al añadir una VLAN se vuelve frágil. Con interfaces enrutadas y protocolos como BGP u OSPF, las rutas pueden anunciarse dinámicamente. WireGuard, OpenVPN e IPsec VTI pueden integrarse con routing dinámico bajo diseños apropiados.

53.5. Hub-and-spoke

En un modelo hub-and-spoke, las sedes remotas se conectan a un concentrador. Si una sede debe hablar con otra, puede hacerlo a través del hub si las reglas y rutas permiten tránsito. Esto simplifica el número de túneles frente a un full mesh, pero convierte el hub en punto crítico.

En producción

Documenta cada red que viaja por cada túnel. La frase «la VPN está levantada» no demuestra que la ruta, la política o el DNS de una nueva VLAN se hayan incorporado.

Capítulo 54. Rendimiento, Multi-WAN, alta disponibilidad y operación

El rendimiento VPN depende de CPU, algoritmo, tamaño de paquetes, latencia, pérdida, implementación del protocolo y capacidad de ambos extremos. No debe estimarse únicamente a partir del ancho de banda de la WAN.

54.1. UDP frente a TCP dentro y fuera

OpenVPN suele preferir UDP para transporte. Encapsular un flujo TCP dentro de un túnel OpenVPN sobre TCP puede provocar interacciones indeseables entre dos capas de control de congestión y retransmisión. TCP puede ser útil en redes donde UDP está bloqueado, pero no es la primera elección de rendimiento.

54.2. CPU y paralelismo

WireGuard e IPsec tienen integración eficiente en kernel. OpenVPN tradicional históricamente ha tenido más coste de cambio entre espacio de usuario y kernel; DCO reduce ese coste y añade mejor aprovechamiento del paralelismo en pfSense Plus.

54.3. MTU y MSS

Cada encapsulación añade cabeceras y reduce el espacio disponible para el paquete interior. Si Path MTU Discovery no funciona correctamente, pueden aparecer páginas que cargan a medias, RDP inestable o transferencias que se detienen.

54.4. Multi-WAN

Una VPN puede estar ligada a una WAN concreta o diseñarse para failover. El simple hecho de disponer de dos gateways no mueve automáticamente todos los túneles de uno a otro. Deben revisarse endpoint, bind, rutas, reglas, DNS y comportamiento específico de cada protocolo.

54.5. Alta disponibilidad

En un par CARP, la alta disponibilidad de una VPN no consiste solamente en replicar su configuración. Hay que estudiar estados, dirección virtual utilizada, sincronización, certificados/claves y cómo percibe el peer remoto el cambio de nodo.

54.6. Monitorización

Métrica	Qué puede revelar
Handshake/estado	Peer inaccesible o negociación fallida.
Bytes TX/RX	Túnel levantado sin tráfico útil o asimetría.
Latencia/pérdida	Problema del underlay, no necesariamente de VPN.
CPU	Límite criptográfico o de procesamiento.

Métrica	Qué puede revelar
Rutas	Prefijo ausente o gateway equivocado.
Logs auth	Credenciales, certificados o backend fallando.
MTU/retransmisiones	Encapsulación y Path MTU.

54.7. Rotación de claves y secretos

PSK, claves WireGuard, certificados, credenciales RADIUS y perfiles de cliente forman parte del inventario de secretos. Debe existir un procedimiento para rotarlos sin dejar accesos huérfanos o perfiles imposibles de revocar.

Operación segura
Una VPN no termina el día que se pone en producción. Requiere revisión de usuarios, certificados, peers, algoritmos, versiones de cliente, logs y accesos que ya no deberían existir.

Capítulo 55. Troubleshooting y laboratorio integral

El diagnóstico VPN es mucho más sencillo cuando se separa en cuatro planos: transporte exterior, negociación/autenticación, routing interior y autorización.

1. UNDERLAY: ¿los peers se alcanzan por Internet/WAN?
2. TÚNEL: ¿negocian claves, certificados y parámetros?
3. ROUTING: ¿el prefijo destino entra por la VPN y vuelve?
4. POLICY: ¿las reglas permiten el tráfico descifrado?

55.1. El túnel no inicia

- Verificar DNS del endpoint si se usa un nombre.
- Confirmar puerto/protocolo y regla WAN cuando corresponda.
- Comprobar NAT upstream y CGNAT.
- Comparar hora si intervienen certificados.
- Revisar que las claves/PSK/certificados pertenezcan al peer correcto.

55.2. Negocia pero no hay tráfico

- Comprobar rutas del sistema y del cliente.
- Revisar Allowed IPs/selectors/redes locales-remotas.
- Comprobar reglas en la pestaña o interfaz VPN adecuada.
- Verificar ruta de retorno.
- Buscar subredes solapadas.
- Capturar tráfico en interfaz VPN y LAN destino.

55.3. Solo funciona ping

Ping demuestra únicamente que ICMP atraviesa el camino. Si HTTPS, SMB o RDP fallan, revisar reglas por puerto, MTU/MSS, firewall del host, DNS y políticas de aplicación.

55.4. Solo funciona por IP

La VPN y el routing pueden estar correctos. El problema se desplaza a DNS: servidor entregado al cliente, rutas hacia ese DNS, split DNS, sufijos o registros internos.

55.5. Un usuario falla y otros no

Este patrón apunta a identidad específica: certificado revocado/caducado, contraseña, grupo RADIUS/LDAP, perfil antiguo, clave WireGuard o dirección de túnel duplicada.

55.6. Laboratorio A: acceso remoto OpenVPN con identidad individual

Objetivo: un empleado accede únicamente a ERP y DNS corporativo desde Internet. El diseño utilizará certificados individuales y autenticación de usuario; en una evolución posterior, el backend podrá ser RADIUS con MFA.

Elemento	Diseño
Pool VPN	10.250.10.0/24
Recursos permitidos	ERP 10.30.0.20:443 y DNS interno.
Autenticación	SSL/TLS + User Auth.
Certificados	Uno por usuario/dispositivo.
Internet del cliente	Split tunnel.
Revocación	Usuario + CRL.
Administración firewall	No accesible desde grupo de usuarios.

1. Crear una CA específica para el nivel de confianza de esta VPN.
2. Crear certificado de servidor y certificados de usuarios.
3. Configurar un servidor OpenVPN con red de túnel dedicada.
4. Empujar únicamente las redes necesarias.
5. Crear reglas OpenVPN que permitan ERP y DNS, bloqueando el resto.
6. Exportar el perfil de un usuario por un canal seguro.
7. Conectar desde una red externa real o simulada.
8. Validar rutas, DNS, ERP y ausencia de acceso administrativo.
9. Revocar el certificado de prueba y demostrar que deja de autenticar.

55.7. Laboratorio B: site-to-site WireGuard

Sede A	Sede B
LAN 10.20.0.0/24	LAN 10.80.0.0/24
WG 10.255.7.1/30	WG 10.255.7.2/30
WAN pública A	WAN pública B o DDNS
Peer B: 10.255.7.2/32 + 10.80.0.0/24	Peer A: 10.255.7.1/32 + 10.20.0.0/24

1. Instalar y habilitar el paquete WireGuard en ambos firewalls.
2. Crear claves independientes en ambos extremos.
3. Intercambiar únicamente claves públicas.
4. Crear túnel y peer en cada lado.
5. Definir Allowed IPs sin solapamientos.

6. Asignar interfaces si el diseño utilizará gateways/rutas explícitas.
7. Crear rutas y reglas únicamente para los flujos de negocio necesarios.
8. Validar ida y vuelta con captura en ambos firewalls.
9. Simular caída del túnel y observar logs/handshake/monitorización.

55.8. Laboratorio C: IPsec IKEv2 interoperable

Objetivo: conectar una sede pfSense con un firewall de otro fabricante. Se utilizará IKEv2 y propuestas criptográficas comunes. Si ambas plataformas soportan VTI, se comparará el modelo route-based con un Phase 2 policy-based.

1. Inventariar identificadores, IP públicas, prefijos y algoritmos soportados.
2. Crear Phase 1 IKEv2 con autenticación acordada.
3. Crear Phase 2 o VTI según interoperabilidad.
4. Abrir únicamente las redes requeridas.
5. Verificar NAT-T si existe traducción intermedia.
6. Comprobar SA, rutas, counters y tráfico descifrado.
7. Documentar exactamente qué parámetros deben coincidir en ambos vendors.

55.9. Matriz de pruebas final

Prueba	Interpretación
Peer exterior alcanzable	Underlay correcto.
Handshake/SA estable	Negociación correcta.
Ruta a red remota	Selección de túnel correcta.
Captura muestra tráfico interior	Encapsulación/descapsulación funciona.
Respuesta vuelve por VPN	Routing simétrico suficiente.
DNS interno resuelve	Servicios auxiliares correctos.
Solo recursos autorizados accesibles	Política mínima aplicada.
Revocación bloquea usuario/peer	Ciclo de vida de identidad funciona.
Reinicio conserva servicio	Configuración persistente y documentada.

Resultado esperado

El lector debe terminar esta Parte VII siendo capaz de distinguir un problema de Internet, de negociación, de routing, de identidad y de firewall. Esa separación es mucho más valiosa que memorizar un asistente de configuración.

Glosario de la Parte VII

Término	Definición
VPN	Relación lógica protegida que transporta tráfico entre extremos.
Peer	Extremo criptográfico de un túnel.
PKI	Infraestructura de claves públicas basada en CA, certificados y claves.
CA	Autoridad que firma certificados.
CRL	Lista de certificados revocados.
PFS	Propiedad que limita el impacto histórico de comprometer claves de larga duración.
Allowed IPs	Redes asociadas a un peer WireGuard para selección/validación criptográfica.
DCO	OpenVPN Data Channel Offload; procesamiento de datos en kernel en pfSense Plus.
IKE	Protocolo de negociación y establecimiento de SA para IPsec.
SA	Security Association; conjunto de parámetros criptográficos negociados.
ESP	Protocolo IPsec utilizado para proteger datos.
NAT-T	Encapsulación de IPsec sobre UDP 4500 para atravesar NAT.
VTI	Interfaz virtual route-based para IPsec.
EAP	Marco de autenticación utilizado, entre otros, en acceso remoto IKEv2.
RADIUS	Protocolo AAA para autenticación, autorización y accounting.
Split tunnel	Solo determinados prefijos viajan por VPN.
Full tunnel	La ruta por defecto del cliente se envía por VPN.
MFA	Autenticación basada en más de un factor.

Fuentes técnicas de contraste

Las fuentes oficiales siguientes se han utilizado para contrastar el comportamiento y la disponibilidad técnica de las funciones descritas. Verificación técnica: octubre de 2026.

- **Virtual Private Networks / selección:** https://docs.netgate.com/pfsense/en/latest/vpn/selection.html
- **VPNs and Firewall Rules:** https://docs.netgate.com/pfsense/en/latest/vpn/firewall-rules.html
- **Certificate Management:** https://docs.netgate.com/pfsense/en/latest/certificates/index.html
- **Certificate Authority Management:** https://docs.netgate.com/pfsense/en/latest/certificates/ca.html
- **Certificate Revocation Lists:** https://docs.netgate.com/pfsense/en/latest/certificates/crl.html
- **WireGuard overview:** https://docs.netgate.com/pfsense/en/latest/vpn/wireguard/
- **WireGuard Design Considerations:** https://docs.netgate.com/pfsense/en/latest/vpn/wireguard/design.html
- **WireGuard Routing:** https://docs.netgate.com/pfsense/en/latest/vpn/wireguard/routing.html
- **OpenVPN overview:** https://docs.netgate.com/pfsense/en/latest/vpn/openvpn/
- **OpenVPN Remote Access:** https://docs.netgate.com/pfsense/en/latest/recipes/openvpn-ra.html
- **OpenVPN DCO:** https://docs.netgate.com/pfsense/en/latest/vpn/openvpn/dco.html
- **IPsec overview:** https://docs.netgate.com/pfsense/en/latest/vpn/ipsec/index.html
- **IPsec Phase 1:** https://docs.netgate.com/pfsense/en/latest/vpn/ipsec/configure-p1.html
- **Choosing Mobile IPsec Style:** https://docs.netgate.com/pfsense/en/latest/vpn/ipsec/mobile-choices.html
- **IKEv2 EAP-TLS example:** https://docs.netgate.com/pfsense/en/latest/recipes/ipsec-mobile-ikev2-eap-tls.html
- **User Management and Authentication:** https://docs.netgate.com/pfsense/en/latest/usermanager/index.html
- **RADIUS Authentication Servers:** https://docs.netgate.com/pfsense/en/latest/usermanager/radius.html
- **FreeRADIUS package:** https://docs.netgate.com/pfsense/en/latest/packages/freeradius.html
- **Using Mobile One-Time Passwords with FreeRADIUS:** https://docs.netgate.com/pfsense/en/latest/recipes/freeradius-otp.html

Cierre de la Parte VII

Con esta parte, pfSense ya puede unir redes físicamente separadas y proporcionar acceso remoto con identidad y política. El siguiente paso natural es proteger con mayor profundidad el perímetro y las redes internas: IDS/IPS, bloqueo por reputación y DNS, paquetes de seguridad, segmentación avanzada y hardening.

pfSense® software

REDES, FIREWALL Y SEGURIDAD

Arquitectura, administración y laboratorios prácticos

PARTE VIII

Seguridad avanzada, IDS/IPS y hardening

Oscar de la Cuesta

palentino.es



Primera edición · octubre de 2026

Apertura de la Parte VIII

La seguridad de una red no aparece al instalar un paquete IDS/IPS ni al importar una lista de reputación. Surge de una arquitectura que reduce exposición, separa zonas, limita privilegios, mantiene el software actualizado y produce evidencia suficiente para detectar comportamientos anómalos. Las herramientas avanzadas solo aportan valor cuando se colocan encima de esa base.

Esta parte estudia tres planos distintos que a menudo se mezclan: el hardening del propio firewall, la inspección del tráfico y la inteligencia de bloqueo basada en firmas, reputación, geografía o nombres. También aborda una idea esencial: bloquear más no significa necesariamente estar más seguro. Una política excesivamente ruidosa puede ocultar incidentes reales entre miles de falsos positivos.

Modelo mental de esta parte

Primero reducimos la superficie de ataque. Después limitamos quién puede hablar con quién. A continuación observamos el tráfico. Solo entonces añadimos detección y prevención. El orden importa porque un IDS/IPS no compensa una WebGUI expuesta, una contraseña débil o una segmentación inexistente.

Capítulo	Objetivo
56	Construir un modelo de amenaza y defensa en profundidad antes de instalar paquetes.
57	Endurecer la administración y el plano de control de pfSense.
58	Comprender IDS, IPS, firmas, falsos positivos y puntos de inspección.
59	Diseñar Suricata con criterios de rendimiento y operación.
60	Entender Snort, reglas, reputación y el contexto actual de Snort 3.
61	Afinar reglas, excepciones y respuesta para que IDS/IPS sea utilizable.
62	Aplicar pfBlockerNG, DNSBL, listas IP y GeoIP con criterio.
63	Reforzar segmentación, egress filtering y servicios críticos.
64	Mantener seguridad: versiones, parches, logs, backups y monitorización.
65	Integrar todo en un laboratorio empresarial y practicar respuesta a incidentes.

Capítulo 56. Seguridad antes de los paquetes: modelo de amenaza y defensa en profundidad

Un firewall no puede proteger eficazmente aquello que no se ha definido. Antes de hablar de firmas o listas, debemos identificar activos, caminos de ataque y consecuencias. No necesita ser un análisis formal de cientos de páginas: una pyme puede obtener mucho valor con una matriz sencilla que relacione activo, exposición, amenaza y control.

56.1. Activos, amenazas y controles

Activo	Amenaza plausible	Control principal
WebGUI de pfSense	Credenciales robadas o fuerza bruta	Red de gestión, VPN, HTTPS, cuentas nominales y login protection.
ERP interno	Movimiento lateral desde un puesto comprometido	Segmentación, reglas mínimas, IDS/IPS y logs.
Servidor publicado	Explotación de vulnerabilidad web	DMZ, reverse proxy/WAF si procede, parcheo, IDS/IPS y mínimo acceso interno.
DNS corporativo	Manipulación o bypass de políticas	Control de resolvers, reglas e inspección.
VPN de teletrabajo	Robo de identidad o dispositivo	MFA/PKI, revocación, mínimos permisos y monitorización.
Backups	Ransomware o destrucción deliberada	Aislamiento, copias offline/inmutables y cuentas separadas.

56.2. Superficie de ataque

La superficie de ataque es el conjunto de interfaces, servicios, credenciales y rutas mediante las que un atacante puede interactuar con un activo. Reducir superficie suele ser más eficaz que intentar detectar cada ataque posible.

- Desactivar servicios que no tienen una necesidad documentada.
- No publicar la administración en WAN si puede usarse VPN.
- Separar gestión, usuarios, servidores, IoT e invitados.
- Evitar reglas any-to-any como estado permanente.
- Eliminar cuentas, certificados y peers que ya no son necesarios.
- Mantener solo paquetes que aporten una función real.

Idea clave

Una función desactivada no necesita firma IDS. Un puerto que no está expuesto no necesita ser defendido frente a Internet. La reducción de superficie elimina clases completas de riesgo antes de que aparezca la detección.

56.3. Defensa en profundidad

```
Internet
  ↓
Perímetro / PF
  ↓
Segmentación por zonas
  ↓
IDS/IPS y reputación
  ↓
Seguridad del host / EDR
  ↓
Identidad y mínimo privilegio
  ↓
Backups + monitorización + respuesta
```

Cada capa parte de la posibilidad de que otra falle. El firewall no sustituye EDR; EDR no sustituye segmentación; una VPN no sustituye MFA; un backup no impide el ataque, pero puede reducir su impacto.

56.4. Riesgo frente a comodidad

La seguridad introduce fricción. El objetivo no es maximizarla indiscriminadamente, sino colocarla donde reduce riesgo de forma proporcionada. Una regla que impide a todos los usuarios acceder a servicios necesarios será deshabilitada tarde o temprano. Una política útil debe ser operable.

En producción

Si una medida de seguridad genera excepciones constantes, quizá el problema no sea la resistencia del usuario sino un diseño demasiado amplio o mal ubicado. Mide excepciones, falsos positivos y tiempo operativo consumido.

Capítulo 57. Hardening del propio firewall

pfSense es simultáneamente dispositivo de seguridad y sistema administrable. Por ello su plano de control merece una protección más estricta que la de un servidor corriente: quien controla el firewall puede alterar rutas, reglas, DNS, VPN y visibilidad.

57.1. Administración por una red específica

La práctica más robusta consiste en permitir la WebGUI únicamente desde una red de gestión o a través de una VPN administrativa. La configuración predeterminada facilita acceso desde LAN, pero en una empresa madura conviene separar gestión de usuarios.

```
MGMT 10.10.0.0/24 → WebGUI/SSH permitidos
USERS 10.20.0.0/24 → WebGUI bloqueada
GUEST 10.50.0.0/24 → WebGUI bloqueada
WAN → WebGUI bloqueada
```

Acceso remoto

La opción preferente para administrar el firewall desde Internet es entrar primero por VPN y después usar la dirección interna de gestión. Publicar directamente la GUI debe considerarse una excepción y restringirse al máximo.

57.2. HTTPS y certificados

La WebGUI debe utilizar HTTPS. Un certificado firmado por una CA interna o pública, según el contexto, evita acostumbrar al administrador a ignorar advertencias TLS. La confianza visual también forma parte de la disciplina operativa: no deberíamos normalizar “aceptar el riesgo” en el dispositivo más sensible de la red.

57.3. Cuentas nominales y privilegios

La cuenta admin existe y no puede eliminarse, pero no tiene por qué ser la identidad cotidiana de todos los técnicos. pfSense permite definir usuarios, grupos y privilegios específicos en la GUI. Una cuenta que solo necesita consultar estado no debería poder escribir config.xml.

Rol	Permiso orientativo
Administrador principal	Cambios completos, VPN, reglas, actualizaciones.
Operador NOC	Dashboard, estados, logs, diagnóstico; cambios limitados.
Técnico soporte	Ping/DNS/leases concretos; sin configuración crítica.
Auditor	Lectura de estado y logs; denegar escritura de configuración.

57.4. Autenticación externa

RADIUS y LDAP permiten centralizar autenticación. En una organización con un directorio ya consolidado, esto simplifica bajas y políticas. No obstante, conviene conservar una vía local de recuperación controlada para escenarios en los que el servicio externo no esté disponible.

57.5. SSH solo cuando exista una necesidad

SSH está desactivado inicialmente. Si se habilita, las claves públicas son preferibles a contraseñas. Exponer SSH en WAN requiere una justificación fuerte, reglas de origen estrictas y autenticación robusta. Cambiar el puerto reduce ruido automático, pero no sustituye controles reales.

Login protection
pfSense utiliza sshguard para reaccionar ante intentos repetidos de autenticación contra GUI y SSH. Es una capa adicional, no una razón para publicar servicios administrativos sin restricciones.

57.6. Consola física y seguridad física

Quien tiene acceso físico al firewall dispone de potentes vías de recuperación. En ubicaciones compartidas conviene proteger el equipo, el puerto de consola y, cuando el escenario lo justifique, exigir contraseña para el menú de consola. La seguridad lógica no puede compensar un dispositivo accesible a cualquiera.

57.7. Sesiones y estaciones administrativas

Un timeout infinito de sesión facilita que un navegador abandonado conserve acceso. La estación desde la que se administra el firewall también debe estar endurecida: MFA corporativo, disco cifrado, EDR, bloqueo de pantalla y ausencia de software innecesario.

Error frecuente
Crear una VLAN de gestión y después permitir que cualquier usuario llegue a ella. Una zona solo es de gestión si el routing y las reglas la convierten realmente en una zona de confianza limitada.

Capítulo 58. IDS/IPS: observar no es lo mismo que bloquear

Un IDS analiza tráfico y genera alertas. Un IPS añade capacidad de impedir tráfico considerado malicioso. La diferencia parece pequeña, pero operativamente es enorme: una firma equivocada en modo IDS genera ruido; la misma firma en modo IPS puede detener un proceso de negocio.

58.1. Firma, evento y contexto

Una regla IDS/IPS describe un patrón: protocolo, direcciones, puertos, contenido, flujo o metadatos. Cuando el motor encuentra coincidencia genera un evento. Ese evento no es automáticamente un incidente. Necesita contexto: qué activo estaba implicado, si la conexión tuvo éxito, si la firma es relevante para el sistema y qué ocurrió después.

Concepto	Pregunta operativa
Firma	¿Qué patrón busca?
Alerta	¿Qué tráfico coincidió?
Severidad	¿Qué impacto sugiere la regla?
Activo	¿Qué sistema estaba implicado?
Contexto	¿Era ese tráfico esperado?
Respuesta	¿Investigar, suprimir o bloquear?

58.2. IDS primero, IPS después

En un despliegue nuevo suele ser más prudente comenzar en modo detección. Durante varios días o semanas se observa qué firmas aparecen y cuáles son falsos positivos. Solo después se promueven a bloqueo categorías que se entienden suficientemente bien.

> **Regla de operación**
> No actives miles de firmas en bloqueo el viernes por la tarde y confíes en que el lunes todo funcionará. Empieza observando, clasifica el ruido y convierte a prevención únicamente lo que puedas explicar.

58.3. Dónde inspeccionar

Colocar un IDS/IPS en WAN, LAN o una VLAN concreta cambia lo que puede observar. En WAN se ve el tráfico exterior antes o después de ciertas traducciones según el modo; en interfaces internas se conserva mejor la identidad de los hosts. En redes segmentadas puede ser más útil inspeccionar las zonas críticas que intentar analizar todo indiscriminadamente.

58.4. Cifrado y visibilidad

Un IDS de red no puede leer mágicamente el contenido de TLS correctamente cifrado. Puede analizar metadatos, direcciones, handshake y otros indicadores, pero el payload de una sesión HTTPS no está disponible sin un punto de descifrado autorizado. Esto reduce la eficacia de firmas basadas en contenido y aumenta el valor de telemetría de endpoint, DNS, SNI cuando es visible y comportamiento.

58.5. Coste de inspección

Snort y Suricata consumen CPU, RAM y almacenamiento. Las reglas, la profundidad de inspección y el volumen de tráfico importan tanto como los Gbit/s nominales. El hardware debe dimensionarse para el conjunto: estados PF + VPN + IDS/IPS + paquetes + logs.

Qué ocurre realmente

El firewall recibe el paquete, el motor IDS/IPS analiza una copia o lo procesa en línea según el modo, compara el flujo con reglas y mantiene estructuras de seguimiento. Cuantas más reglas y más sesiones simultáneas, mayor memoria y trabajo de CPU.

Capítulo 59. Suricata: IDS/IPS multihilo y operación en línea

Suricata es un motor IDS/IPS de alto rendimiento disponible como paquete. Su arquitectura multihilo le permite aprovechar varios núcleos y, sobre hardware compatible, puede trabajar en modo IPS en línea mediante mecanismos como netmap. Esta capacidad no elimina la necesidad de afinar reglas y medir impacto.

59.1. Diseño por interfaces

Cada instancia debe responder a una pregunta concreta. Por ejemplo: proteger servidores publicados en WAN/DMZ, observar movimiento lateral hacia SERVERS o analizar tráfico de IoT. Crear instancias “porque sí” en todas las interfaces multiplica carga y eventos duplicados.

Interfaz	Objetivo razonable
WAN	Detectar intentos contra servicios realmente publicados.
SERVERS	Observar acceso a activos críticos con identidad interna clara.
IOT	Detectar comunicaciones inesperadas, escaneo o C2.
GUEST	Normalmente menor prioridad salvo requisitos específicos.
MGMT	Muy sensible; reglas estrictas y bajo volumen.

59.2. Reglas y fuentes

Suricata puede utilizar conjuntos de reglas compatibles, incluidos feeds comunitarios o comerciales según el paquete y la fuente elegida. La decisión no debe basarse solo en cantidad de firmas. Importan frecuencia de actualización, calidad, cobertura, condiciones de licencia y capacidad del equipo para procesarlas.

59.3. HOME_NET y EXTERNAL_NET

Los motores IDS necesitan distinguir qué redes consideramos internas. Definir HOME_NET de forma correcta ayuda a que muchas reglas interpreten origen y destino como fue diseñado. Una red añadida a la organización pero olvidada en estas variables puede producir detecciones incoherentes o ausentes.

59.4. Inline IPS y netmap

En modo inline, el motor participa directamente en la decisión de permitir o descartar paquetes. El rendimiento y la compatibilidad dependen de NIC, driver y configuración. Antes de activar prevención en una interfaz crítica, debe existir una prueba de carga y una vía de rollback.

Error frecuente

Suponer que “inline” equivale a “mejor”. En una red donde el riesgo operativo de bloquear tráfico legítimo es alto, un IDS bien monitorizado puede aportar más valor que un IPS mal afinado.

59.5. Almacenamiento de logs

Las alertas y capturas pueden crecer con rapidez. La documentación actual recomienda almacenamiento SSD/HDD para Suricata. En un appliance con eMMC pequeño o almacenamiento muy limitado, el diseño de retención debe ser conservador y puede ser preferible enviar eventos a un sistema externo.

59.6. Estrategia de despliegue

1. Instalar el paquete y documentar la versión.
2. Elegir una única interfaz inicial y modo IDS.
3. Definir HOME_NET y servidores críticos.
4. Activar un conjunto pequeño de categorías relevantes.
5. Actualizar reglas y observar alertas durante un periodo base.
6. Crear suppressions/pass lists solo con motivo documentado.
7. Promover a bloqueo categorías de alta confianza.
8. Medir CPU, memoria, drops y latencia tras cada cambio.

Capítulo 60. Snort: firmas, reputación y evolución hacia Snort 3

Snort es uno de los IDS/IPS más conocidos y también está disponible como paquete en pfSense. Puede trabajar en detección o bloqueo, utilizar reglas comunitarias y comerciales, listas de reputación y OpenAppID para identificar determinadas aplicaciones.

60.1. Fuentes de reglas

El paquete clásico admite, entre otros, conjuntos Snort, reglas comunitarias GPLv2, Emerging Threats Open/Pro y detectores OpenAppID. Algunas fuentes son gratuitas; otras requieren registro o suscripción. En un entorno comercial, la frescura de las firmas puede ser un criterio relevante.

60.2. Variables de servidores

Definir qué direcciones contienen servidores web, DNS, correo u otros servicios permite reducir trabajo innecesario y mejorar precisión. Si una firma de servidor web se evalúa contra toda la red, el motor consume recursos buscando un contexto que quizá no existe.

60.3. Pass Lists y Suppression

Una pass list evita bloqueos para determinados hosts o redes en los modos que la soportan. Una suppression reduce o silencia una firma bajo condiciones concretas. Son herramientas distintas: “no bloquear este host” no equivale a “no generar esta alerta”.

60.4. Reputation

El preprocesamiento de reputación puede comparar direcciones con listas permitidas o bloqueadas. La reputación es útil para señales conocidas, pero debe tratarse como una fuente de contexto. Una IP puede cambiar de propietario, pertenecer a un CDN compartido o aparecer erróneamente en una lista.

60.5. Snort 3 y Netgate Nexus

En el estado actual del producto existe además un paquete Snort 3 disponible exclusivamente para pfSense Plus a través de la interfaz Netgate Nexus. Su GUI ha sido rediseñada y no debe confundirse con el paquete clásico. Para este libro, el valor conceptual está en comprender IDS/IPS; las pantallas concretas pueden cambiar entre generaciones.

Nota de edición
No vincularemos la enseñanza a un menú de Snort 3 que pueda cambiar. El lector debe saber definir activos, seleccionar reglas, interpretar alertas y afinar una política aunque la interfaz gráfica evolucione.

Capítulo 61. Afinar IDS/IPS: del ruido a una señal útil

El éxito de un IDS/IPS no se mide por cuántas alertas produce, sino por cuántas alertas relevantes puede investigar el equipo. Un sistema que genera 50 000 eventos diarios sin priorización termina siendo ignorado.

61.1. Baseline

Antes de bloquear, necesitamos conocer el tráfico habitual. El baseline no significa considerar "seguro" todo lo visto; significa disponer de una referencia para reconocer cambios. Una pyme puede registrar durante dos semanas los principales servicios, destinos, alertas y ventanas de actividad.

61.2. Clasificar falsos positivos

Tipo	Ejemplo	Respuesta
Regla irrelevante	Firma de IIS contra un servidor Linux sin IIS	Desactivar categoría/regla para ese contexto.
Tráfico legítimo parecido a ataque	Escáner de vulnerabilidades corporativo	Suprimir por origen/controlar ventana.
Aplicación heredada	Protocolo antiguo necesario temporalmente	Excepción documentada + plan de retirada.
Lista reputacional errónea	CDN compartido marcado	Validar fuente y excepción mínima.
Evento real benigno	Administrador ejecuta nmap autorizado	Registrar contexto y limitar por horario/origen.

61.3. No suprimir demasiado

Una suppression amplia puede ocultar el ataque que queríamos detectar. La excepción debe ser lo más específica posible: firma + host + dirección del flujo, no "desactivar toda la categoría" si solo falla una aplicación.

61.4. Prioridad por activos

Una alerta contra un honeypot, un servidor ERP o un portátil de invitados no tiene el mismo impacto. Etiquetar activos críticos y definir aliases reutilizables ayuda a priorizar la respuesta.

61.5. Ciclo de vida de una regla

```
Nueva firma
  ↓
Modo alerta
  ↓
¿relevante para nuestros activos?
  ↓ sí
Validar falsos positivos
  ↓
Bloqueo controlado
  ↓
Revisión periódica / retirada si deja de aportar valor
```

61.6. Respuesta a una alerta

1. Confirmar hora, interfaz, IP origen/destino y firma.
2. Revisar si el host destino ejecuta el servicio afectado.
3. Comprobar estados PF y conexiones relacionadas.
4. Correlacionar con DNS, logs del servidor y EDR.
5. Capturar tráfico si el incidente sigue activo y es seguro hacerlo.
6. Decidir contención: bloqueo temporal, aislamiento de VLAN, revocación o ninguna acción.
7. Documentar resultado para futuras alertas de la misma firma.

Error frecuente

Bloquear una IP externa y dar el incidente por cerrado. Si el host interno ya fue comprometido, el problema no es la IP que inició el acceso sino la persistencia, las credenciales y el movimiento posterior.

Capítulo 62. pfBlockerNG, DNSBL, GeoIP y reputación

pfBlockerNG amplía la lógica de aliases y automatiza listas de direcciones, países y dominios. Puede construir listas para reglas PF y utilizar DNSBL con Unbound. Es potente porque convierte fuentes externas dinámicas en controles del firewall, pero precisamente por eso hereda la calidad y los errores de esas fuentes.

62.1. Listas IP

Una lista IP puede utilizarse para negar entrada, negar salida o alimentar aliases que después se emplean en reglas propias. El enfoque “Alias Only” es especialmente interesante cuando queremos separar inteligencia de bloqueo y política de firewall.

```
Feed externo → pfBlockerNG → alias BAD_IPS
                    ↓
              regla PF propia
USERS → destino BAD_IPS → block + log
```

62.2. DNSBL

DNSBL bloquea por nombre mediante el DNS Resolver. Esto es eficaz para dominios conocidos de malware, publicidad o tracking según las listas escogidas, pero solo puede controlar consultas que pasan por el resolver que aplicará la política.

Límite

Un usuario que consulta un DNS externo o una aplicación que utiliza DoH puede saltarse un bloqueo DNS tradicional si la organización no controla esas rutas. Además, DNSBL bloquea nombres, no todo el tráfico posible hacia una dirección.

62.3. GeoIP

El bloqueo por país puede tener sentido cuando un servicio se presta exclusivamente en una región y existe muy poco motivo legítimo para recibir tráfico desde otros lugares. Sin embargo, la geolocalización IP no identifica nacionalidad ni intención. VPN, cloud, CDN y proveedores globales reducen su precisión como control de seguridad.

Principio

GeoIP debe ser una reducción de superficie basada en requisitos de negocio, no una clasificación moral de países. Si una aplicación es global, bloquear regiones por intuición puede romper proveedores legítimos sin detener a un atacante que use infraestructura cercana.

62.4. Calidad de feeds

Criterio	Pregunta
Procedencia	¿Quién mantiene la lista?
Frecuencia	¿Cada cuánto se actualiza?
Falsos positivos	¿Existe mecanismo de corrección?
Licencia	¿Podemos utilizarla en este contexto?
Volumen	¿Cabe y se procesa con el hardware disponible?
Objetivo	¿Malware, spam, C2, publicidad, país, ASN...?

62.5. DNS filtering no sustituye seguridad web

Bloquear un dominio por DNS puede evitar que un usuario llegue a él por nombre, pero no inspecciona una aplicación web legítima comprometida ni contenido servido desde un dominio permitido. Es una capa útil, no un sustituto de seguridad de endpoint, navegador, correo o proxy.

Capítulo 63. Segmentación avanzada, egress filtering y control lateral

Gran parte del daño moderno ocurre después del acceso inicial. Un puesto comprometido intenta descubrir otros equipos, alcanzar servicios administrativos o comunicarse con infraestructura externa. La segmentación y el filtrado de salida reducen esa libertad.

63.1. East-west frente a north-south

Dirección	Ejemplo	Control
North-south	USERS → Internet	Firewall de salida, DNS, reputación, proxy/IDS.
South-north	Internet → servidor publicado	Port forward, DMZ, IPS, mínimo acceso.
East-west	USERS → SERVERS	Segmentación, reglas por servicio, IDS interno.
Lateral dentro de VLAN	PC → PC en misma VLAN	No siempre pasa por pfSense; requiere switch/NAC/host firewall.

Límite de arquitectura

pfSense no puede filtrar tráfico que nunca atraviesa pfSense. Dos hosts en la misma VLAN se comunican a través del switch. Para controlar ese movimiento se necesita segmentar, usar firewalls de host, ACL de switch o tecnologías adicionales.

63.2. Egress filtering

Muchas redes permiten cualquier salida porque “los clientes necesitan Internet”. Una política más madura limita protocolos y destinos de infraestructura: DNS solo a resolvers autorizados, SMTP únicamente desde servidores de correo, administración remota únicamente desde MGMT, NTP desde fuentes previstas y bloqueo de puertos que no son necesarios.

63.3. DNS como punto de control

Obligar a los clientes gestionados a utilizar resolvers corporativos mejora visibilidad y permite DNSBL. Para hacerlo de forma coherente se bloquea o redirige DNS clásico según la política y se aborda DoH/DoT desde endpoint, navegador o controles de red adicionales.

63.4. IoT

Los dispositivos IoT suelen necesitar pocos destinos y protocolos. Una cámara que solo debe alcanzar NTP, DNS y un grabador interno no necesita acceso general a USERS o a toda Internet. Las reglas de allow-list son especialmente valiosas en este tipo de red.

63.5. DMZ real

Una DMZ no es simplemente “otra VLAN”. Debe existir una política asimétrica: Internet puede llegar solo a servicios publicados; la DMZ tiene acceso muy limitado hacia LAN; administración llega desde MGMT; las respuestas necesarias están permitidas por estados. Si un servidor DMZ cae, no debería convertirse en trampolín hacia Active Directory.

63.6. RFC1918 en WAN y bogons

Los controles de direcciones privadas o bogon en interfaces externas deben entenderse según la topología. Si WAN está detrás de un router privado, bloquear RFC1918 en WAN puede ser incompatible con el diseño. La seguridad correcta depende del contexto, no de activar todas las casillas disponibles.

Capítulo 64. Seguridad operativa: actualizaciones, parches, logs y copias

El hardening no es un estado fijo. Un firewall seguro hoy puede quedar expuesto mañana por una vulnerabilidad, una cuenta abandonada o una regla temporal que nadie retiró. La seguridad operativa convierte revisiones repetibles en parte del mantenimiento.

64.1. Versiones y paquetes

Antes de instalar un paquete conviene comprobar mantenimiento, compatibilidad y recursos. El sistema de paquetes permite ampliar pfSense sin inflar la base, pero cada paquete añade código, configuración y ciclo de actualización. “Disponible” no significa “necesario”.

64.2. System Patches

En las ramas actuales, el paquete System Patches viene instalado por defecto en pfSense Plus 26.03 y pfSense CE 2.9.0 y posteriores. Puede aplicar parches recomendados específicos de una versión entre releases. Las listas dependen de la versión y no siempre existen parches pendientes.

El paquete puede autoaplicar parches recomendados si el administrador lo habilita, pero el propio paquete debe actualizarse para recibir nuevas listas. En entornos controlados conviene combinar revisión humana, backup y ventana de cambio.

Precaución

Los parches personalizados cambian código del firewall. Utiliza fuentes confiables, documenta motivo y rollback y evita convertir el firewall en una colección de modificaciones irrepetibles.

64.3. Logs locales y remotos

Los logs locales son útiles para diagnóstico inmediato, pero un atacante con control administrativo podría alterarlos o el firewall podría perderlos tras un fallo de almacenamiento. En entornos relevantes conviene enviar eventos a un syslog/SIEM externo.

Fuente	Eventos útiles
Firewall PF	Pass/block, interfaz, regla, origen/destino.
VPN	Autenticación, handshake, peer y errores.
IDS/IPS	Firma, acción, flujo y categoría.
DNS	Consultas específicas durante investigación.
DHCP	Identidad temporal IP/MAC/hostname.
Sistema	Servicios, actualizaciones, reinicios y fallos.

64.4. Reloj y correlación

Todos los dispositivos de seguridad deben compartir una referencia temporal fiable. Un SIEM con logs de firewall cinco minutos adelantados y EDR tres minutos atrasados convierte una investigación en conjeturas.

64.5. Backups protegidos

config.xml contiene la arquitectura de seguridad del firewall y puede contener material sensible. Las copias deben salir del dispositivo, cifrarse o protegerse adecuadamente y probarse. Una copia antigua puede restaurar también una regla antigua vulnerable, por lo que debe conocerse su fecha y contexto.

64.6. Revisión periódica

Frecuencia orientativa	Revisión
Semanal	Alertas críticas, fallos de actualización, estado de feeds, almacenamiento.
Mensual	Usuarios, peers VPN, paquetes, parches recomendados, backups.
Trimestral	Reglas temporales, aliases, exposición WAN, certificados próximos a caducar.
Anual / cambio mayor	Arquitectura, amenazas, capacidad hardware y continuidad.

64.7. Monitorización

SNMP, Telegraf, Zabbix, syslog-ng u otras herramientas pueden sacar métricas y logs hacia plataformas externas. La elección importa menos que las preguntas: ¿sabemos si la CPU está saturada por IDS? ¿si el disco se llena? ¿si un túnel cae? ¿si las actualizaciones fallan?

Capítulo 65. Laboratorio integral de hardening y respuesta a incidentes

El laboratorio reúne la empresa segmentada utilizada en partes anteriores. El objetivo no es “activar todo”, sino demostrar una estrategia por capas con evidencia y rollback.

65.1. Escenario

Zona	Red	Riesgo principal
MGMT	10.10.0.0/24	Compromiso del plano administrativo.
USERS	10.20.0.0/24	Phishing, malware y movimiento lateral.
SERVERS	10.30.0.0/24	ERP, DNS/AD y datos críticos.
DMZ	10.35.0.0/24	Servidor web publicado.
IOT	10.40.0.0/24	Firmware débil y comunicaciones externas.
GUEST	10.50.0.0/24	Dispositivos no gestionados.

65.2. Fase A — Hardening del firewall

1. Crear reglas que permitan WebGUI/SSH únicamente desde MGMT y VPN administrativa.
2. Mantener HTTPS y utilizar un certificado confiable para los administradores.
3. Crear cuentas nominales y grupos de privilegios.
4. Desactivar SSH si no es necesario; si se usa, preferir claves.
5. Revisar timeout de sesión y login protection.
6. Proteger acceso físico/consola según ubicación.
7. Eliminar paquetes sin uso y registrar los instalados.

65.3. Fase B — Política por zonas

Origen	Destino permitido	Principio
USERS	ERP/DNS/Internet	Servicios necesarios, no SERVERS completo.
IOT	DNS/NTP/grabador/updates específicos	Allow-list.
GUEST	Internet	Sin RFC1918 ni administración.

Origen	Destino permitido	Principio
DMZ	Backends estrictamente necesarios	No acceso general a LAN.
MGMT	Infraestructura	Administración, auditada.

65.4. Fase C — IDS inicial

1. Elegir Suricata o Snort para el laboratorio, no ambos simultáneamente en la misma interfaz.
2. Comenzar en modo IDS en DMZ o SERVERS.
3. Definir HOME_NET y aliases de servidores.
4. Activar un conjunto razonable de reglas.
5. Generar tráfico normal durante varios días de laboratorio.
6. Clasificar diez alertas: verdadero positivo, falso positivo o irrelevante.
7. Convertir a prevención solo una categoría de alta confianza.

65.5. Fase D — pfBlockerNG

1. Crear una lista IP de reputación en modo alias antes de bloquear.
2. Revisar qué reglas usarán el alias y en qué dirección.
3. Activar una lista DNSBL pequeña y documentada.
4. Obligar a la VLAN de laboratorio a utilizar el resolver corporativo para DNS clásico.
5. Probar un falso positivo deliberado y crear una excepción mínima.
6. Evitar GeoIP global; aplicarlo solo a un servicio cuya audiencia esté realmente limitada.

65.6. Fase E — Simulación de incidente

Simularemos un puesto USERS que empieza a consultar un dominio de prueba bloqueado y a intentar acceder por SMB a múltiples servidores. No se utilizará malware real: el objetivo es practicar la correlación de señales.

```
08:42:10 DNS → dominio de prueba marcado
08:42:12 PF  → conexión saliente bloqueada por alias
08:43:05 IDS → patrón de escaneo SMB desde 10.20.0.87
08:43:20 PF  → múltiples intentos a SERVERS
08:44:00 SOC → aislamiento temporal de 10.20.0.87
```

65.7. Proceso de respuesta

1. Confirmar identidad del host mediante DHCP/inventario.
2. Validar si la alerta IDS corresponde a la actividad observada.
3. Revisar DNS y destinos externos del host.

4. Comprobar estados PF y conexiones recientes.
5. Aplicar una contención temporal específica: alias QUARANTINE o bloqueo por host.
6. Notificar al equipo de endpoint para análisis del equipo.
7. No borrar logs antes de exportar la evidencia necesaria.
8. Retirar la contención solo cuando exista una decisión de recuperación.
9. Documentar IOC, causa, reglas creadas y cambios temporales.

65.8. Alias de cuarentena

Un alias manual QUARANTINE puede ser útil como mecanismo operativo: una regla temprana bloquea hosts internos incluidos en él. Debe existir un procedimiento claro para añadir, justificar y retirar entradas, porque una lista de cuarentena olvidada se convierte en deuda operativa.

65.9. Qué no hacer durante un incidente

- No desactivar todo PF para “ver si así funciona”.
- No borrar estados, logs y configuración sin necesidad.
- No aplicar diez cambios simultáneos.
- No asumir que la primera IP marcada es la causa raíz.
- No reinstalar el firewall como primera reacción.
- No convertir una regla temporal any-to-any en solución permanente.

65.10. Matriz final de validación

Prueba	Resultado esperado
WebGUI desde USERS	Bloqueada.
WebGUI desde MGMT	Permitida por HTTPS.
SSH no requerido	Servicio desactivado.
USERS → ERP	Solo puertos necesarios.
IOT → USERS	Bloqueado.
DMZ → SERVERS	Solo backend definido.
IDS en modo alerta	Eventos visibles sin impacto.
Regla IPS seleccionada	Bloquea el patrón probado.
DNSBL	Bloquea dominio de prueba y permite excepción documentada.
Feed reputación	Se aplica mediante alias/regla conocida.
Syslog remoto	Recibe firewall/IDS/sistema.
Backup	Copia externa posterior al hardening.

Prueba	Resultado esperado
Restauración de configuración	Procedimiento documentado.

Resultado esperado
La seguridad avanzada deja de ser una suma de casillas. El lector termina con una arquitectura en la que cada control tiene propósito, alcance, evidencia y mecanismo de reversión.

Glosario de la Parte VIII

Término	Definición
Attack surface	Conjunto de puntos mediante los que un atacante puede interactuar con el sistema.
Defense in depth	Uso de capas independientes para reducir probabilidad e impacto de fallo.
IDS	Sistema que detecta y alerta sobre actividad sospechosa.
IPS	Sistema que puede impedir tráfico detectado como malicioso.
Signature	Patrón utilizado para reconocer tráfico o comportamiento.
False positive	Alerta que identifica como malicioso un evento legítimo.
HOME_NET	Conjunto de redes consideradas internas por un motor IDS/IPS.
Suppression	Regla que reduce o silencia alertas bajo condiciones específicas.
Pass list	Lista de hosts/redes que un motor trata como excepción de bloqueo según su modo.
Reputation	Uso de listas de IP/dominios con una clasificación previa.
DNSBL	Bloqueo basado en nombres DNS.
GeoIP	Estimación de ubicación asociada a una dirección IP.
Egress filtering	Restricción del tráfico saliente según política.
Lateral movement	Movimiento de un atacante entre sistemas tras el acceso inicial.

Término	Definición
Hardening	Reducción deliberada de superficie y privilegios.
IOC	Indicador de compromiso.
SIEM	Plataforma de agregación y correlación de eventos de seguridad.
Quarantine	Aislamiento temporal de un host o identidad durante investigación.

Fuentes técnicas de contraste

Las fuentes oficiales siguientes se han utilizado para verificar capacidades, comportamiento y estado de las funciones descritas. Verificación técnica: octubre de 2026.

- **Packages overview:** https://docs.netgate.com/pfsense/en/latest/packages/index.html
- **Package List:** https://docs.netgate.com/pfsense/en/latest/packages/list.html
- **IDS / IPS — Snort and Suricata:** https://docs.netgate.com/pfsense/en/latest/packages/snort/index.html
- **Configuring the Snort Package:** https://docs.netgate.com/pfsense/en/latest/packages/snort/setup.html
- **Snort Server Definitions:** https://docs.netgate.com/pfsense/en/latest/packages/snort/define-servers.html
- **Snort 3:** https://docs.netgate.com/pfsense/en/latest/nexus/snort/index.html
- **pfBlocker-NG Package:** https://docs.netgate.com/pfsense/en/latest/packages/pfblocker.html
- **Blocking Websites:** https://docs.netgate.com/pfsense/en/latest/recipes/block-websites.html
- **Blocking External Client DNS Queries:** https://docs.netgate.com/pfsense/en/latest/recipes/dns-block-external.html
- **Admin Access:** https://docs.netgate.com/pfsense/en/latest/config/advanced-admin.html
- **Remote firewall administration:** https://docs.netgate.com/pfsense/en/latest/recipes/remote-firewall-administration.html
- **User Management and Authentication:** https://docs.netgate.com/pfsense/en/latest/usermanager/index.html
- **Privileges:** https://docs.netgate.com/pfsense/en/latest/usermanager/privileges.html
- **System Patches Package:** https://docs.netgate.com/pfsense/en/latest/development/system-patches.html
- **Recommended System Patches:** https://docs.netgate.com/pfsense/en/latest/development/patches/recommended.html
- **pfSense 26.03 New Features and Changes:** https://docs.netgate.com/pfsense/en/latest/releases/26-03.html
- **Hardware Sizing Guidance:** https://docs.netgate.com/pfsense/en/latest/hardware/size.html

Cierre de la Parte VIII

Con esta parte el firewall deja de ser únicamente un punto de filtrado y pasa a formar parte de un programa operativo de seguridad. El siguiente bloque se centrará en continuidad y disponibilidad: Multi-WAN, monitorización de gateways, balanceo, CARP, pfsync, XMLRPC y diseño de alta disponibilidad.

pfSense® software

REDES, FIREWALL Y SEGURIDAD

Arquitectura, administración y laboratorios prácticos

PARTE IX

Multi-WAN y alta disponibilidad

Oscar de la Cuesta

palentino.es



Primera edición · octubre de 2026

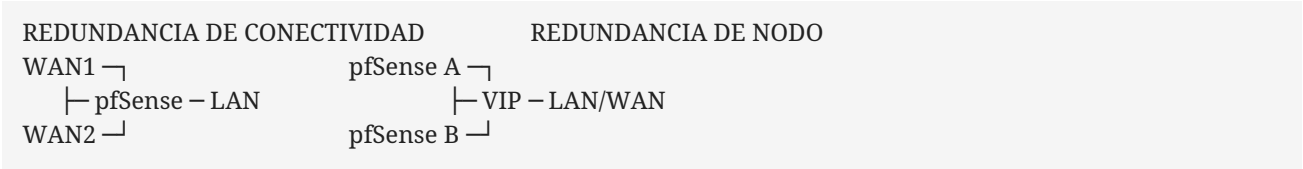
Apertura de la Parte IX

Hasta ahora hemos construido un firewall capaz de enrutar, filtrar, traducir, ofrecer servicios, terminar VPN y aplicar controles de seguridad. En una red real aparece entonces una pregunta incómoda: ¿qué ocurre cuando falla aquello de lo que depende todo? Puede caer una línea de Internet, el router del operador, un transceptor, una NIC, un switch, el propio firewall o incluso la alimentación de un rack.

La disponibilidad no consiste en duplicar componentes al azar. Consiste en identificar puntos únicos de fallo, detectar de forma fiable cuándo un camino ya no sirve, retirar ese camino del servicio, conservar el estado cuando sea posible y devolver el tráfico a una ruta estable sin crear oscilaciones.

Dos problemas diferentes

Multi-WAN protege frente a la pérdida o degradación de caminos de salida. La alta disponibilidad de firewalls protege frente a la pérdida del nodo que ejecuta pfSense. Pueden combinarse, pero no son lo mismo y deben probarse por separado.



Mapa de la Parte IX

Capítulo	Pregunta principal
66	¿Qué significa disponibilidad y qué fallo intentamos cubrir?
67	¿Cómo sabe pfSense que un gateway funciona, está degradado o ha caído?
68	¿Cómo se construyen failover y balanceo con Gateway Groups?
69	¿Cómo dirige policy routing tráfico diferente por WAN distintas?
70	¿Qué cambia en DNS, NAT, servicios y VPN cuando hay varias WAN?
71	¿Qué aporta CARP y qué no aporta?
72	¿Cómo sincroniza pfsync los estados y por qué importa?
73	¿Cómo replica XMLRPC la configuración y qué queda fuera?

Capítulo	Pregunta principal
74	¿Cómo se diseña un clúster HA completo sin nuevos puntos únicos de fallo?
75	¿Cómo se prueba, opera y diagnostica un sistema redundante?

Capítulo 66. Disponibilidad: diseñar antes de duplicar

El error más caro de una arquitectura redundante suele ocurrir antes de configurar pfSense: duplicar el firewall pero mantener un único switch, una única alimentación, un único ONT o un único enlace entre racks. La alta disponibilidad solo cubre los fallos que el diseño contempla.

66.1. Punto único de fallo

Un Single Point of Failure es un componente cuya pérdida interrumpe una función crítica sin alternativa automática o aceptable. No tiene por qué ser un dispositivo: puede ser una VLAN, una dirección IP, un puerto, una fuente de alimentación o incluso una dependencia de gestión.

Elemento	Fallo	Posible mitigación
ISP principal	Pérdida de Internet	Segundo ISP con ruta física independiente.
ONT/router operador	Corte aunque la fibra externa siga activa	CPE redundante o segundo acceso distinto.
pfSense	Reinicio, avería, actualización fallida	Par HA activo/pasivo.
Switch de core	Ambos firewalls quedan aislados	Dos switches/stack/MLAG según plataforma.
Alimentación	Apaga firewall y switch a la vez	PSU redundante, UPS, PDUs o circuitos separados.
SYNC	Se pierde sincronización	Enlace dedicado y monitorizado; diseño que falle de forma segura.

66.2. RTO y RPO en una red

RTO describe cuánto tiempo de indisponibilidad puede tolerarse. RPO suele asociarse a datos, pero en red puede usarse de forma conceptual para pensar cuánto estado operativo puede perderse. Un clúster con pfsync intenta que las conexiones existentes sobrevivan a un cambio de nodo; sin sincronización, el servicio puede volver rápido, pero las sesiones se reinician.

66.3. Disponibilidad no equivale a continuidad perfecta

Algunos protocolos toleran un cambio de ruta mejor que otros. Una descarga TCP puede sobrevivir si los estados y direcciones permanecen coherentes; una llamada en tiempo real puede notar una interrupción mínima; una VPN puede renegociar. El objetivo debe expresarse como servicio medible, no como promesa de “cero cortes”.

Pregunta de arquitectura

¿Qué debe sobrevivir: nuevas conexiones, conexiones ya abiertas, direcciones públicas, VPN, administración o todo a la vez? La respuesta determina qué mecanismos hacen falta.

66.4. Active/passive frente a active/active

La alta disponibilidad tradicional de pfSense se comporta como un clúster activo/pasivo: un nodo actúa como MASTER para las direcciones virtuales y el otro permanece preparado para asumirlas. Esto no debe confundirse con repartir una misma sesión de firewall entre dos nodos activos simultáneamente.

Capítulo 67. Gateway monitoring: medir el camino real

Un failover fiable depende de una pregunta aparentemente simple: ¿está disponible el enlace? La respuesta no puede basarse únicamente en que la interfaz tenga carrier. Un módem puede seguir enlazado, el gateway local puede responder y, sin embargo, Internet estar roto más allá.

67.1. Gateway frente a monitor IP

El gateway es el siguiente salto de una ruta. La monitor IP es el destino que pfSense utiliza para juzgar la salud del camino. En muchos casos pueden coincidir, pero no necesariamente deberían hacerlo.

```
Firewall ── gateway ISP ── red operador ── Internet ── monitor IP
  link UP       responde         X fallo aguas arriba
```

Error frecuente

Monitorizar únicamente la IP del módem o del router del operador puede producir un falso “Online”: el equipo local responde aunque el acceso a Internet esté roto después.

67.2. dpinger

pfSense utiliza dpinger para medir reachability, latencia y pérdida hacia las direcciones de monitorización. Sus eventos alimentan el estado de gateways y pueden disparar decisiones de los Gateway Groups.

Medida	Qué indica	Riesgo de interpretar mal
Reachability	Hay respuestas al monitor	No demuestra que todos los destinos de Internet funcionen.
Latencia	Tiempo de ida y vuelta	Puede subir por congestión, cola o ruta remota.
Pérdida	Porcentaje de sondeos sin respuesta	El monitor puede limitar ICMP y no representar la calidad real.
Estado de interfaz	Carrier / enlace	No detecta fallos aguas arriba.

67.3. Umbrales y triggers

Un gateway puede considerarse no utilizable no solo cuando deja de responder por completo. Los grupos permiten reaccionar ante pérdida, latencia o ambas, según el tipo de tráfico. Una sede de VoIP puede preferir abandonar una línea con pérdida alta aunque todavía responda; un backup de datos puede tolerarla más tiempo.

67.4. Evitar flapping

Si un circuito oscila cerca del umbral, el gateway puede entrar y salir repetidamente del grupo. Esto provoca cambios de estados, rutas y sesiones. Los umbrales deben elegirse con medidas reales de la línea, no copiando cifras de Internet.

Qué ocurre realmente

El failover no "ve" Internet. Ve el resultado de una medición concreta. Elegir un mal monitor significa automatizar una decisión sobre una señal incorrecta.

67.5. Leer logs de gateway

Los logs del subsistema de gateways muestran alarmas, recuperaciones, latencia y pérdida registradas por dpinger. En una incidencia conviene correlacionar el instante del evento con logs de firewall, VPN y aplicaciones.

Capítulo 68. Gateway Groups: failover, balanceo y tiers

Los Gateway Groups no mueven tráfico por sí solos. Definen una política de selección de gateways que después debe ser utilizada por reglas, por el gateway por defecto o por funciones compatibles.

68.1. Tier es prioridad, no velocidad

Los números de tier expresan preferencia. Tier 1 se utiliza antes que Tier 2. Dos gateways en el mismo tier pueden participar en balanceo por conexiones.

WAN1	WAN2	Comportamiento
Tier 1	Tier 2	Preferir WAN1; usar WAN2 si WAN1 falla.
Tier 2	Tier 1	Preferir WAN2.
Tier 1	Tier 1	Balancear conexiones entre ambas y retirar la que falle.
Tier 1	Tier 2 con trigger pérdida/latencia	Failover por calidad además de caída.

68.2. Balanceo por conexión

pfSense distribuye conexiones, no paquetes de una misma conexión. Una descarga TCP única no suma automáticamente dos accesos de 500 Mbit/s para convertirse en 1 Gbit/s. Muchas conexiones simultáneas sí pueden aprovechar la capacidad agregada de forma estadística.

Idea clave
Multi-WAN no es bonding del ISP. Sin cooperación del proveedor, una sesión concreta mantiene un único camino de salida.

68.3. Weighted balancing

Cuando dos enlaces tienen capacidades diferentes, los pesos pueden sesgar cuántas conexiones recibe cada gateway. El mecanismo no mide el ancho de banda consumido en tiempo real: distribuye conexiones según el peso.

68.4. Sticky connections

Algunos servicios asocian una sesión web a la IP pública del cliente. Si conexiones sucesivas salen por WAN distintas, la aplicación puede invalidar la sesión. Sticky connections intenta mantener un cliente asociado al mismo gateway durante un período, aunque reduce la capacidad de repartir sus conexiones.

68.5. Gateway group por defecto

Una práctica útil es disponer de un grupo de failover apto como gateway por defecto del firewall, de modo que servicios iniciados por el propio sistema conserven una ruta viable. Esto debe combinarse con el comportamiento específico del DNS Resolver, actualizaciones, NTP, VPN y paquetes.

Capítulo 69. Policy routing: decidir por dónde sale cada tráfico

El routing convencional pregunta por el destino y busca la mejor ruta. Policy routing añade otra dimensión: una regla de firewall puede seleccionar un gateway o Gateway Group para el tráfico que coincide con esa política.

69.1. Orden de reglas

Como en el resto de PF, las reglas se evalúan en el orden previsto y una política más específica debe colocarse antes de una regla general. Si todo USERS coincide primero con “salir por WAN1”, una regla posterior para que VoIP use WAN2 jamás se aplicará.

1. VOIP_NET → SIP/RTP → PreferWAN2
2. BANKS_ALIAS → HTTPS → PreferWAN1
3. USERS_NET → any → LoadBalance
4. resto → política general

69.2. Tráfico local al firewall

Policy routing se utiliza para tráfico que atraviesa el firewall. El tráfico destinado al propio pfSense —por ejemplo, consultar la WebGUI o el DNS Resolver local— no debe forzarse hacia una WAN externa. Las reglas deben excluir redes locales y destinos del firewall antes de aplicar gateways.

Error frecuente

Una regla “LAN net → any → Gateway Group” demasiado amplia puede intentar aplicar policy routing incluso a destinos internos si no se excluyen adecuadamente. El resultado puede parecer un fallo de DNS, acceso a GUI o rutas locales.

69.3. Matar estados al cambiar de WAN

PF es stateful. Una conexión ya abierta conserva su decisión de ruta mientras exista el estado. Cuando se prueba failover, los estados previos pueden dar la impresión de que la regla nueva no funciona. En pruebas controladas puede ser necesario limpiar estados específicos.

69.4. Asimetría

Si un flujo entra por WAN1 y su respuesta se fuerza por WAN2, el peer ve otra IP pública o un camino inesperado. Policy routing debe diseñarse junto con NAT, estados y servicios publicados para conservar simetría cuando el protocolo lo requiera.

69.5. Cuando las rutas estáticas dejan de escalar: FRR

En redes con varias sedes, múltiples enlaces o muchos prefijos, mantener rutas estáticas manuales puede convertirse en una fuente de errores. El paquete FRR permite que pfSense participe en routing dinámico y aprenda o anuncie rutas mediante protocolos estándar.

FRR no debe activarse solo porque una red sea “grande”. Introduce vecindades, políticas, métricas y una nueva capa de troubleshooting. Tiene sentido cuando el cambio dinámico de rutas aporta un beneficio operativo claro.

Protocolo	Uso habitual	Ámbito
BGP	Intercambio de rutas con otros sistemas autónomos, proveedores o diseños empresariales complejos.	IPv4 e IPv6
OSPFv2	Routing interno dinámico dentro de una organización.	IPv4
OSPFv3 / OSPF6	Routing interno dinámico equivalente para IPv6.	IPv6

Capítulo 70. Multi-WAN con DNS, NAT, VPN y servicios

Añadir una segunda WAN multiplica combinaciones. Ya no basta con preguntar si existe ruta: debemos saber qué dirección pública usa cada salida, qué DNS depende de cada camino, qué servicio escucha en qué WAN y cómo falla cada VPN.

70.1. Outbound NAT

Cada WAN necesita traducciones coherentes para las redes que puedan salir por ella. En modo automático pfSense genera gran parte de estas reglas. Los diseños Hybrid o Manual deben revisar explícitamente todas las redes y gateways para evitar que el tráfico cambie de WAN pero conserve una traducción incorrecta.

70.2. Publicaciones entrantes

Un Port Forward asociado a WAN1 no aparece mágicamente en WAN2. Si un servicio debe sobrevivir a la pérdida de un ISP, hacen falta direcciones y DNS públicos capaces de representar ambos accesos, o una arquitectura externa que resuelva el problema.

70.3. DNS

En modo resolver recursivo, un gateway por defecto con failover ayuda a que Unbound conserve salida. En modo forwarding, puede ser necesario asociar resolvers diferentes a gateways distintos para no enviar consultas a un servidor inaccesible a través del enlace equivocado.

70.4. Dynamic DNS

Con varias WAN, cada registro DDNS debe observar y publicar la dirección de la interfaz correspondiente. Un único nombre puede no ser suficiente para representar políticas complejas de entrada o failover entre proveedores.

70.5. OpenVPN, WireGuard e IPsec

Las VPN deben diseñarse específicamente para Multi-WAN. Algunas pueden utilizar Gateway Groups solo en modo failover, otras dependen del endpoint remoto, de la dirección a la que hacen bind o de rutas adicionales. Un túnel que negocia sobre WAN1 no se traslada necesariamente a WAN2 sin renegociación o configuración adicional.

En producción

Prueba el fallo de WAN con cada servicio crítico por separado: navegación, DNS, VPN, correo saliente, actualizaciones, VoIP y publicaciones. “Internet vuelve” no significa que todo el sistema haya hecho failover.

Capítulo 71. CARP: redundancia de direcciones

CARP permite que varios nodos compartan direcciones IP virtuales y que uno de ellos actúe como MASTER mientras los demás permanecen en BACKUP. Cuando el MASTER deja de anunciar correctamente, otro nodo puede asumir la dirección virtual.

71.1. Dirección real y dirección virtual

```
WAN nodo A: 198.51.100.2
WAN nodo B: 198.51.100.3
CARP VIP:   198.51.100.1  ← dirección que usan NAT/servicios

LAN nodo A: 10.20.0.2
LAN nodo B: 10.20.0.3
CARP VIP:   10.20.0.1     ← gateway de los clientes
```

Los clientes no deberían depender de la IP física del nodo activo. Utilizan la VIP, que puede moverse entre nodos.

71.2. VHID y anuncios

Cada VIP CARP tiene un identificador y parámetros de anuncio que determinan prioridad. El nodo con mejor prioridad opera como MASTER salvo que un cambio de estado provoque la transición.

71.3. CARP no sincroniza estados ni configuración

Distinción fundamental

CARP mueve direcciones. pfsync replica estados. XMLRPC replica configuraciones compatibles. Llamar a todo “CARP” oculta tres mecanismos con fallos y diagnósticos diferentes.

71.4. Requisitos de capa 2

Los nodos y la VIP deben coexistir en segmentos donde los anuncios y las direcciones virtuales funcionen correctamente. Algunos switches, hipervisores o proveedores de hosting aplican restricciones de MAC, multicast o direcciones virtuales que deben comprobarse antes del despliegue.

71.5. CARP y mantenimiento

Una ventaja práctica de HA es poder despromover temporalmente el primario, validar el secundario y realizar mantenimiento con menor impacto. Pero esta capacidad solo es fiable si el failover se prueba periódicamente.

Capítulo 72. pfsync: conservar la tabla de estados

Un firewall stateful conoce cada flujo activo. Si el nodo secundario toma la VIP pero desconoce esos estados, las conexiones existentes pueden romperse. pfsync replica información de estados para que el nodo de respaldo pueda continuar gran parte de los flujos.

72.1. Interfaz SYNC

La recomendación habitual es utilizar una interfaz dedicada para sincronización. Ese segmento transporta pfsync, XMLRPC y otras funciones de sincronización. No debería depender de la misma ruta cuya caída pretende sobrevivir el clúster.

72.2. Qué necesita pfsync

- Activación de sincronización de estados en ambos nodos.
- Conectividad directa y estable por la interfaz seleccionada.
- Orden de interfaces coherente entre nodos.
- Reglas que permitan el protocolo pfsync donde corresponda.
- Filter Host IDs distintos y conocidos.
- Preferiblemente peer IP explícita en diseños donde se quiera máxima previsibilidad.

72.3. Estado no significa aplicación

pfsync conserva la visión de PF sobre una conexión, pero no replica la memoria interna de todos los servicios. Una sesión puede depender además de una VPN, un proxy, un daemon o una aplicación remota. Por eso la continuidad debe validarse por servicio.

72.4. Seguridad de SYNC

Seguridad
La red SYNC transporta información operativa sensible. Debe permanecer en un segmento controlado, sin usuarios, y con acceso limitado únicamente a los nodos que lo necesiten.

Capítulo 73. XMLRPC: mantener dos configuraciones coherentes

Administrar manualmente dos firewalls casi idénticos parece sencillo hasta que una regla urgente se modifica solo en uno. XMLRPC reduce ese riesgo copiando desde el nodo primario numerosas áreas compatibles hacia el secundario.

73.1. Dirección de sincronización

En un clúster de dos nodos, la sincronización de configuración se habilita únicamente en el primario. El secundario recibe los cambios; no debe intentar replicarlos de vuelta.

73.2. Qué se sincroniza y qué no

Suele sincronizar	Normalmente específico de nodo
Reglas de firewall y aliases	Asignación física de interfaces.
Usuarios y certificados	Direcciones IP propias de cada nodo.
VPN y muchas configuraciones de servicios	Determinados ajustes del sistema/instalación.
Rutas, gateways y objetos compatibles	Datos ligados a hardware local.

El principio es lógico: lo que describe la política común puede replicarse; lo que identifica físicamente a cada nodo debe permanecer diferenciado.

73.3. Dependencias de XMLRPC

Para sincronizar, el primario debe alcanzar la WebGUI del secundario por el protocolo y puerto correctos, con credenciales válidas. Hora, reglas de firewall, protocolo HTTPS/HTTP y puerto deben ser coherentes.

73.4. Cambiar desde el primario

Disciplina operativa
En un clúster sincronizado, los cambios de política se realizan en el primario. Editar directamente el secundario crea drift y el siguiente sync puede sobrescribir lo realizado.

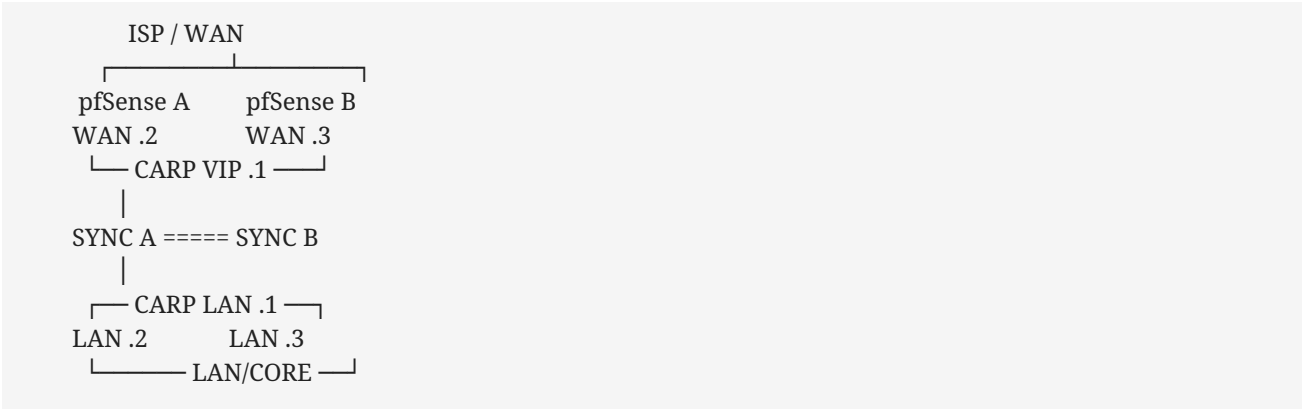
73.5. Backup de ambos nodos

Aunque gran parte de la configuración se replique, cada nodo sigue teniendo valores propios. Conviene conservar backups de ambos y documentar qué partes se regeneran por sincronización y cuáles deben restaurarse de forma individual.

Capítulo 74. Diseñar un clúster HA completo

El diseño completo combina direcciones virtuales, estados y configuración, pero también switches, ISP, routing, DNS y alimentación. La meta es que el fallo de un único nodo no obligue a los clientes a cambiar de gateway ni a reconfigurar servicios.

74.1. Topología mínima



74.2. IP por nodo + VIP por red

Cada red redundante necesita una IP propia por nodo y una VIP compartida cuando los clientes o servicios deban seguir una dirección estable. Esto requiere planificar subredes con suficientes direcciones y evitar usar toda la red como si existiera un único firewall.

74.3. NAT con VIP

Para que la salida mantenga una dirección pública estable independientemente del nodo activo, NAT debe utilizar la VIP apropiada cuando el diseño lo requiera. Si cada nodo sale con su dirección real, el failover cambia la identidad pública y puede romper sesiones.

74.4. DHCP en HA

El servicio DHCP también requiere diseño de alta disponibilidad coherente con el backend utilizado. Con Kea, la arquitectura actual utiliza mecanismos HA propios y debe integrarse con el par de firewalls; no debe suponerse que la sincronización de configuración por sí sola replica todas las concesiones activas.

74.5. Switches y doble conexión

Dos firewalls conectados al mismo switch único siguen compartiendo un SPOF. Para mayores requisitos de disponibilidad, el core debe tener su propia redundancia. La técnica exacta —stack, MLAG, chasis redundante, dos switches independientes— depende de la plataforma y queda fuera de pfSense, pero forma parte del diseño.

74.6. Multi-WAN + HA

Cuando se combinan dos nodos y dos ISP aparecen cuatro caminos físicos y varias VIP. Cada WAN necesita direccionamiento de ambos nodos, una VIP si se requiere identidad compartida y monitorización coherente. El número de escenarios de fallo aumenta y debe existir una matriz de pruebas explícita.

Evento	Resultado deseado
Falla WAN1	Nodo activo usa WAN2 sin cambiar de firewall.
Falla nodo A	Nodo B asume VIP y mantiene WAN disponible.
Falla WAN1 y nodo A	Nodo B opera por WAN2.
Falla SYNC	El clúster sigue filtrando, pero se alerta; no se ignora la pérdida de sincronización.
Falla switch de acceso	Solo sobrevive si la topología de switching también es redundante.

Capítulo 75. Pruebas de fallo, operación y troubleshooting

Una arquitectura redundante no se valida mirando iconos verdes. Se valida provocando fallos controlados y midiendo qué ocurre. Cada prueba debe tener condición inicial, acción, tiempo de detección, tiempo de recuperación, impacto observado y resultado esperado.

75.1. Laboratorio A: failover de dos WAN

Elemento	Diseño
WAN1	Fibra principal, Tier 1.
WAN2	4G/segunda fibra, Tier 2.
Monitor WAN1	Destino externo estable y exclusivo.
Monitor WAN2	Destino externo diferente.
Grupo	PreferWAN1.
LAN	10.20.0.0/24 con policy routing al grupo.

1. Confirmar ambos gateways Online y registrar latencia/pérdida base.
2. Abrir varias conexiones desde clientes y anotar IP pública de salida.
3. Interrumpir WAN1 aguas arriba, no solo desconectar un cable que cambie otro elemento.
4. Medir cuándo dpinger genera alarma y cuándo las nuevas conexiones usan WAN2.
5. Observar qué conexiones antiguas se reinician o sobreviven.
6. Restaurar WAN1 y medir recuperación.
7. Repetir con pérdida/latencia artificial si el laboratorio lo permite.
8. Guardar logs de gateways y estados para correlación.

75.2. Laboratorio B: balanceo

Configurar ambas WAN en el mismo tier y generar múltiples conexiones independientes. Verificar que el reparto es por conexiones y que una transferencia única no suma ambas velocidades. Repetir con sticky connections y comparar comportamiento.

75.3. Laboratorio C: failover de nodo

1. Comprobar que A es MASTER y B BACKUP para las VIP.
2. Verificar estado de pfsync y sincronización XMLRPC.
3. Abrir sesiones TCP de larga duración y tráfico interactivo.
4. Forzar CARP demotion o apagar controladamente el nodo A.

5. Observar transición de VIP al nodo B.
6. Comprobar continuidad de sesiones y servicios.
7. Revisar que nuevas conexiones usan las mismas VIP/NAT esperadas.
8. Recuperar A y observar su retorno sin crear split-brain.
9. Documentar tiempos reales.

75.4. Fallo de CARP

- Comprobar que ambos nodos están en el mismo dominio de capa 2 cuando sea necesario.
- Revisar VHID, direcciones, máscaras y parámetros de anuncio.
- Buscar restricciones de switch, hipervisor o proveedor sobre MAC virtuales/multicast.
- Capturar tráfico CARP para comprobar anuncios.
- Revisar si otra interfaz está provocando demotion del nodo.

75.5. Fallo de pfsync

- Confirmar Synchronize States en ambos nodos.
- Validar conectividad directa por SYNC.
- Revisar reglas que permitan pfsync.
- Comprobar Filter Host IDs y estado de sincronización.
- Comparar orden de interfaces entre nodos.

75.6. Fallo de XMLRPC

- Contraseña/usuario de sincronización correctos.
- Mismo protocolo y puerto de WebGUI en los nodos.
- Regla que permita acceso al puerto de sincronización.
- Hora razonablemente sincronizada.
- XMLRPC configurado solo en el primario.
- Cambios realizados en un área realmente sincronizable.

75.7. Runbook de incidente

Paso	Acción
1. Detectar	Identificar si falla WAN, gateway, nodo, CARP, pfsync o servicio.
2. Contener	Evitar cambios simultáneos en ambos nodos; preservar evidencia.
3. Confirmar rol	MASTER/BACKUP, gateways Online/Alarm, rutas y estados.
4. Restaurar servicio	Failover automático o intervención mínima documentada.
5. Validar	DNS, VPN, NAT, publicaciones y aplicaciones críticas.
6. Analizar	Correlacionar logs, tiempos y causa raíz.

Paso	Acción
7. Mejorar	Actualizar runbook, umbrales y pruebas.

Resultado de la Parte IX

El lector debe ser capaz de distinguir un fallo de ISP, un fallo de monitorización, un fallo de policy routing, un fallo de CARP, un fallo de pfsync y un fallo de sincronización de configuración. Solo entonces “alta disponibilidad” deja de ser una casilla y se convierte en una arquitectura verificable.

Glosario de la Parte IX

Término	Definición
Multi-WAN	Uso de múltiples caminos WAN para failover, balanceo o políticas de salida.
Gateway Group	Conjunto de gateways organizado por tiers y triggers de fallo.
Tier	Nivel de prioridad de un gateway dentro de un grupo.
dpinger	Daemon utilizado para monitorizar reachability, pérdida y latencia de gateways.
Policy routing	Selección de gateway mediante reglas según características del tráfico.
Sticky connection	Afinidad temporal de un cliente con un gateway en balanceo.
CARP	Protocolo de redundancia de direcciones IP virtuales.
VIP	Dirección IP virtual compartida por nodos.
pfsync	Mecanismo de sincronización de estados de PF.
XMLRPC Sync	Sincronización de áreas de configuración desde primario a secundario.
MASTER	Nodo que posee activamente una VIP CARP.
BACKUP	Nodo preparado para asumir una VIP.
SYNC	Red/interfaz dedicada a funciones de sincronización.
SPOF	Punto único de fallo.
Failover	Cambio a un recurso alternativo tras detectar fallo/degradación.
Load balancing	Distribución de conexiones entre caminos disponibles.

Fuentes técnicas de contraste

Las siguientes fuentes oficiales se han utilizado para verificar el funcionamiento vigente de Multi-WAN y alta disponibilidad en pfSense. Verificación técnica: octubre de 2026.

- **Multiple WAN Connections:** https://docs.netgate.com/pfsense/en/latest/multiwan/index.html
- **Multi-WAN Terminology and Concepts:** https://docs.netgate.com/pfsense/en/latest/multiwan/concepts.html
- **Gateway Groups:** https://docs.netgate.com/pfsense/en/latest/routing/gateway-groups.html
- **Load Balancing and Failover with Gateway Groups:** https://docs.netgate.com/pfsense/en/latest/multiwan/load-balance-and-failover.html
- **Policy Routing, Load Balancing and Failover Strategies:** https://docs.netgate.com/pfsense/en/latest/multiwan/strategies.html
- **Summary of Multi-WAN Requirements:** https://docs.netgate.com/pfsense/en/latest/multiwan/requirements.html
- **Troubleshooting Multi-WAN:** https://docs.netgate.com/pfsense/en/latest/troubleshooting/multi-wan.html
- **Gateway Logs:** https://docs.netgate.com/pfsense/en/latest/monitoring/logs/gateway.html
- FRR Package: https://docs.netgate.com/pfsense/en/latest/packages/frr/index.html
- Dynamic Routing Protocol Basics: https://docs.netgate.com/pfsense/en/latest/recipes/dynamic-routing-basics.html
- **High Availability:** https://docs.netgate.com/pfsense/en/latest/highavailability/index.html
- **High Availability Configuration Example:** https://docs.netgate.com/pfsense/en/latest/recipes/high-availability.html
- **XMLRPC Config Sync Overview:** https://docs.netgate.com/pfsense/en/latest/highavailability/xmlrpc-sync.html
- **Troubleshooting High Availability:** https://docs.netgate.com/pfsense/en/latest/troubleshooting/high-availability.html

Cierre de la Parte IX

Después de esta parte, pfSense deja de ser un único equipo conectado a una única línea: pasa a formar parte de un sistema tolerante a fallos. La Parte X aborda la visibilidad necesaria para operar ese sistema a largo plazo: monitorización, logs, métricas, packet capture, diagnóstico avanzado y metodología de troubleshooting.

pfSense® software

REDES, FIREWALL Y SEGURIDAD

Arquitectura, administración y laboratorios prácticos

PARTE X

Monitorización y troubleshooting avanzado

Oscar de la Cuesta

palentino.es



Primera edición · octubre de 2026

Apertura de la Parte X

Un firewall bien configurado puede fallar; un firewall mediocremente configurado puede parecer sano durante meses. La diferencia entre administrar y adivinar está en la observabilidad: disponer de señales, saber dónde mirarlas y convertirlas en hipótesis comprobables.

Esta parte no pretende convertir al lector en analista de paquetes de bajo nivel, sino darle un método profesional. Aprenderemos a mirar el mismo problema desde varias perspectivas: sistema, interfaz, routing, PF, estado, NAT, DNS, servicio y paquete. Cuando dos perspectivas coinciden, la causa probable se reduce de forma drástica.

Regla de diagnóstico

Antes de cambiar una configuración, recoge evidencia. Después cambia una sola variable y vuelve a medir. Si modificas reglas, NAT, DNS y rutas simultáneamente, puedes resolver el síntoma sin aprender la causa y crear un problema nuevo.

Mapa de la Parte X

Capítulo	Contenido
76	Observabilidad: qué mirar antes de que ocurra un incidente.
77	Logs locales, firewall log y syslog remoto.
78	Estados, pfTop, pfInfo y lectura de conexiones.
79	Packet capture, tcpdump y Wireshark.
80	Routing, ARP/NDP, ping, traceroute, DNS Lookup y Test Port.
81	CLI y pfctl para diagnóstico seguro.
82	Rendimiento: CPU, RAM, estados, interfaces, disco y gráficos.
83	Métodos de troubleshooting por capas y por trayectoria.
84	Casos reales: Internet, NAT, DNS, VPN, HA y servicios.
85	Laboratorio integral y runbook de incidentes.

Capítulo 76. Observabilidad: medir antes de intervenir

Monitorizar no significa llenar una pantalla de gráficas. Significa disponer de una línea base que permita responder una pregunta decisiva: ¿qué cambió respecto al funcionamiento normal? Sin esa referencia, un 65 % de CPU puede parecer alto o perfectamente habitual, y 35.000 estados pueden ser normales o el inicio de una saturación.

76.1. Cuatro planos de observación

Plano	Preguntas
Sistema	¿CPU, RAM, almacenamiento, temperatura y procesos están sanos?
Red	¿Interfaces, errores, gateways, rutas y vecinos son correctos?
Firewall	¿Reglas, estados, tablas y NAT están comportándose como se diseñó?
Servicio	¿DNS, DHCP, VPN, NTP, IDS/IPS y paquetes responden?

76.2. Dashboard como panel de situación

El Dashboard es útil para construir una vista rápida del estado actual, especialmente con widgets de gateways, interfaces, servicios, firewall logs, CARP, OpenVPN/IPsec, Dynamic DNS, uso de recursos e información del sistema. No sustituye los logs ni las métricas históricas: ofrece contexto inmediato.

Diseño del dashboard

Un buen dashboard no intenta mostrar todo. Para un firewall de empresa debería permitir detectar en segundos: WAN caída, servicio crítico detenido, CARP en estado inesperado, consumo anómalo de recursos y eventos recientes del firewall.

76.3. Línea base

Durante una semana normal conviene registrar valores aproximados de CPU, memoria, número de estados, throughput, latencia y pérdida por gateway. No hace falta perseguir una precisión científica; el objetivo es reconocer desviaciones.

Indicador	Línea base posible	Alarma contextual
Estados	8.000–15.000 en horario laboral	Crecimiento rápido a 80.000 sin cambio conocido.
WAN RTT	8–15 ms	Picos sostenidos por encima de 100 ms.

Indicador	Línea base posible	Alarma contextual
Pérdida	0–1 %	20 % sostenido o fluctuación coincidente con quejas.
CPU	10–30 %	100 % durante minutos sin tarea planificada.
RAM	Estable	Crecimiento continuo sin retorno.
Errores NIC	0 o casi 0	Incremento sostenido de errores/drops.

76.4. Histórico frente a fotografía

Status y Diagnostics muestran el presente. Status > Monitoring conserva series históricas en RRD para CPU, memoria, estados, tráfico, paquetes, calidad de enlace y otras métricas. La diferencia es fundamental: un incidente que terminó hace veinte minutos puede haber desaparecido del dashboard y seguir siendo visible en una gráfica.

Qué ocurre realmente

Una gráfica no explica la causa; muestra correlación temporal. Si el RTT sube exactamente cuando la WAN alcanza su límite de subida, ya existe una hipótesis útil: congestión/bufferbloat. Después se valida con tráfico, colas y captura.

Capítulo 77. Logs: reconstruir lo que ocurrió

Los logs son una cronología parcial del firewall. No contienen cada paquete ni cada decisión interna, pero permiten reconstruir eventos administrativos, bloqueos, negociaciones VPN, cambios de gateway, DHCP, DNS, autenticación y procesos del sistema.

77.1. Logs por subsistema

Área	Qué buscar
System	Arranques, servicios, errores generales, configuración.
Firewall	Bloqueos y reglas registradas; tráfico PF.
Gateways	Alarmas y recuperaciones de dpinger.
Routing	RA, FRR, IGMP Proxy, routing dinámico.
DNS	Unbound/dnsmasq y eventos de resolución.
DHCP	Leases, errores de servidor/relay/cliente.
VPN	IPsec, OpenVPN y autenticación asociada.
Authentication	Inicios de sesión y fallos de autenticación.
NTP	Sincronización y eventos del reloj.
Packages	Eventos de paquetes que integran logging.

77.2. El firewall log no demuestra todo

Por defecto, pfSense registra el tráfico bloqueado y no registra todo el tráfico permitido. Por tanto, ausencia de una entrada roja compatible con el flujo reduce la probabilidad de que PF lo esté bloqueando, pero no demuestra que el servicio destino responda. Para demostrar paso efectivo, la tabla de estados y las capturas son mejores evidencias.

Método

Para una conexión sospechosa: 1) mira el log del firewall; 2) busca estado; 3) captura en la interfaz de entrada; 4) captura en la salida. Cada paso elimina familias enteras de causas.

77.3. Identificar la regla que actuó

Las entradas de firewall log contienen información de la regla. En la GUI es posible saltar desde una entrada a la regla asociada en muchos casos. Activar temporalmente logging en una regla pass concreta puede ayudar a confirmar que el flujo coincide con esa política.

77.4. Logs locales y rotación

Las versiones modernas de pfSense utilizan logs de texto plano bajo /var/log/ y los rotan para limitar el consumo de almacenamiento. Herramientas tradicionales como cat, tail y grep resultan útiles desde shell. La rotación implica que el histórico local es deliberadamente finito.

```
tail -F /var/log/filter.log | filterparser.php
grep -i 'error' /var/log/system.log
grep '10.20.0.25' /var/log/filter.log
```

77.5. Syslog remoto

Para retención de meses, correlación entre dispositivos o SIEM, los logs deben salir del firewall. El syslog remoto permite copiar categorías seleccionadas a un servidor central. La implementación syslog clásica utilizada por pfSense envía por UDP y sin cifrado, por lo que debe circular por una red confiable, una VPN o un mecanismo adicional de protección.

Seguridad

Un log puede incluir IP, nombres, usuarios y datos operativos sensibles. No lo envíes en claro por Internet. Si necesitas TCP o capacidades adicionales, evalúa un colector o paquete compatible como syslog-ng.

77.6. Correlación temporal

La hora correcta es parte del diagnóstico. Si el firewall, switch, hipervisor y servidor difieren varios minutos, la secuencia real de un incidente queda distorsionada. NTP y zona horaria coherentes convierten logs aislados en una línea temporal común.

Capítulo 78. Estados, pfTop y pfInfo: ver qué está haciendo PF

pfSense es stateful: una conexión permitida crea normalmente un estado que permite asociar los paquetes posteriores a esa conversación. La tabla de estados es por tanto uno de los mejores lugares para responder: «¿ha permitido el firewall esta conexión?»

78.1. Leer un estado

Diagnostics > States permite filtrar por IP, puerto y otros criterios. Cuando existe NAT, la vista puede mostrar direcciones antes y después de la traducción. En TCP, estados como SYN_SENT, ESTABLISHED, FIN_WAIT o TIME_WAIT ayudan a localizar en qué punto se encuentra la conversación.

Patrón	Interpretación probable
SYN_SENT sin respuesta	El SYN salió o se vio, pero no llegó respuesta útil.
ESTABLISHED	PF observa una sesión TCP establecida.
Muchos estados a un mismo destino	Servicio muy utilizado, escaneo o comportamiento anómalo; requiere contexto.
Estado con NAT visible	La traducción se está aplicando a ese flujo.
Sin estado tras intentar conexión	Regla no permitió, tráfico no llegó al firewall o flujo no crea estado según diseño.

Idea clave
Si una regla pass debería autorizar un TCP y aparece un estado coherente, PF ya ha hecho una parte importante de su trabajo. El siguiente sospechoso suele ser routing de retorno, firewall del host o el propio servicio.

78.2. No borrar estados como primera reacción

Eliminar estados puede ser necesario después de cambios de política o gateways, pero también destruye evidencia y corta conexiones legítimas. Antes de hacerlo, identifica qué estado estás eliminando y por qué. En producción, vaciar toda la tabla es una acción disruptiva.

78.3. States Summary

Diagnostics > States Summary agrupa conexiones por origen, destino, pares y puertos. Es útil para detectar un host que abre miles de sesiones o un servidor que concentra una carga inesperada. En tablas enormes el cálculo puede ser pesado, por lo que no debe convertirse en una consulta compulsiva durante una saturación extrema.

78.4. pfTop

pfTop ofrece una visión dinámica del estado de PF. Puede ordenar por bytes, tasa, antigüedad o tamaño, y dispone de vistas centradas en reglas, colas y estados. Es una herramienta excelente para responder «quién está consumiendo ahora» sin depender de una gráfica agregada.

```
pftop
# ideas de uso en la GUI: ordenar por Rate, Size o Age
# filtrar por host/red/protocolo según la investigación
```

78.5. pfInfo

Diagnostics > pfInfo muestra contadores internos: paquetes pasados/bloqueados, búsquedas en la tabla de estados, inserciones, eliminaciones, límites, timers y estadísticas de interfaces. Un alto ritmo de inserciones puede reflejar muchas conexiones nuevas; los limit counters pueden revelar que una regla está alcanzando límites configurados.

Indicador pfInfo	Qué puede sugerir
State inserts/s alto	Tormenta de conexiones, escaneo, carga legítima intensa.
State table cerca del máximo	Riesgo de nuevas conexiones rechazadas o presión de recursos.
Limit counters incrementando	Una política de límite está actuando.
Interface counters anómalos	Drops/errores o tráfico inesperado.
Search rate elevado	Muchos paquetes sobre estados existentes; contextualizar con throughput.

78.6. Conexiones del equipo y estados del firewall

La tabla de estados de pfSense muestra el flujo observado por el firewall, pero no siempre identifica el proceso que lo origina. En un cliente Windows, **Modern Terminal AI** permite relacionar conexiones TCP/UDP con el proceso y su PID, los extremos, puertos y estado, y consultar reglas relacionadas del Firewall de Windows.

Enfoque de diagnóstico: observar primero el extremo en Windows y después contrastar estados, reglas, NAT y capturas en pfSense. Son perspectivas complementarias, no equivalentes.



Recurso complementario: modernterminal-ai.com

Capítulo 79. Packet capture y tcpdump: observar el paquete real

Cuando logs y estados no bastan, la captura de paquetes elimina gran parte de la especulación. pfSense integra una interfaz gráfica para tcpdump y también permite utilizar tcpdump desde shell. La captura ve el tráfico tal como aparece en una interfaz concreta.

79.1. Elegir la interfaz correcta

La primera pregunta no es «qué filtro uso», sino «en qué punto quiero observar el paquete». Para un cliente LAN sin Internet, empieza en LAN. Para un port forward, empieza en WAN y después captura en la interfaz interna. Para IPsec/OpenVPN, puede interesar comparar la interfaz exterior con la interfaz lógica/encapsulada.

Marco de referencia

En una interfaz de entrada, la captura ve el paquete antes de que PF/NAT completen su procesamiento. En una interfaz de salida lo ve después. Por eso el mismo flujo puede mostrar direcciones diferentes a cada lado de NAT.

79.2. Reducir ruido

Capturar todo un enlace de 10 Gb/s sin filtro produce más datos de los que una persona puede analizar. Filtra por host, puerto, protocolo y duración; aumenta el alcance solo si la primera captura no contiene la evidencia buscada.

```
tcpdump -ni igb1 host 10.20.0.25
tcpdump -ni igb1 tcp port 443
tcpdump -ni igb1 port 53
tcpdump -ni igb1 icmp
tcpdump -ni igb1 'host 10.20.0.25 and host 10.30.0.20'
```

79.3. No resolver nombres durante la captura

La opción -n evita resolución de nombres y acelera la lectura, además de impedir que el propio tcpdump genere consultas DNS que contaminan la captura. -i selecciona interfaz y, combinada como -ni, es una base práctica para diagnóstico.

79.4. Dos capturas, una trayectoria

```
WAN:  203.0.113.50:50000 → 198.51.100.20:443
                  ↓ DNAT
LAN:  203.0.113.50:50000 → 10.30.0.20:443
```

Si el SYN aparece en WAN y no aparece en LAN, el fallo está dentro del firewall: NAT, reglas o routing. Si aparece en LAN y el servidor nunca responde, la investigación se desplaza al host, su gateway o su firewall local. Si responde en LAN y no sale respuesta por WAN, volvemos a mirar estado, NAT y ruta de retorno.

79.5. TCP: tres señales esenciales

Señal	Lectura
SYN → SYN/ACK → ACK	Handshake correcto.
SYN repetido sin SYN/ACK	No hay respuesta: filtrado, ruta o servicio ausente.
RST	Host o dispositivo rechaza/cierra activamente.
Retransmisiones	Pérdida, congestión, MTU o aplicación lenta, según contexto.

79.6. Guardar PCAP y usar Wireshark

La GUI permite descargar una captura para analizarla posteriormente en Wireshark. Esto es preferible cuando se necesita seguir streams, inspeccionar flags, medir tiempos o compartir evidencia con otro técnico. El PCAP puede contener datos sensibles; debe custodiarse como evidencia técnica.

Privacidad
Una captura puede incluir credenciales en protocolos inseguros, nombres, direcciones, cookies o contenido sin cifrar. Limita el alcance y elimina PCAP innecesarios cuando termina la investigación.

Capítulo 80. Routing, vecinos y pruebas activas

Muchas incidencias atribuidas al firewall son en realidad errores de capa 2, direccionamiento o routing. Las herramientas Diagnostics permiten comprobar cada pieza desde el propio pfSense y elegir la dirección origen, algo esencial en un equipo con múltiples interfaces.

80.1. Tabla de rutas

Diagnostics > Routes muestra las rutas que conoce el sistema. En shell, netstat -rWn ofrece una vista equivalente y route -n get permite preguntar qué camino usaría para un destino concreto.

```
netstat -rWn
route -n get 8.8.8.8
route -n get 10.80.0.20
```

Método

No preguntes solo «¿existe una ruta?». Pregunta «¿qué ruta selecciona para ESTE destino y con qué interfaz/gateway?». Longest prefix match puede hacer que una ruta más específica gane a la default.

80.2. ARP y NDP

ARP Table muestra vecinos IPv4 observados en redes directamente conectadas; NDP Table cumple el papel equivalente para IPv6. Una entrada Incomplete indica que pfSense ha preguntado por el vecino pero no ha recibido una respuesta válida.

Síntoma	Hipótesis
ARP Incomplete	Host apagado, VLAN incorrecta, cable/switch, máscara o capa 2.
MAC inesperada	IP duplicada, proxy ARP, topología distinta a la documentada.
NDP Incomplete	Problema de vecino IPv6, VLAN, RA/NDP o conectividad L2.
Sin entrada	El host quizá no ha hablado recientemente con el firewall o no es vecino directo.

80.3. Ping con origen

El origen seleccionado cambia la prueba. Hacer ping a una sede VPN desde WAN no valida el mismo camino que hacerlo desde la IP LAN. Para reproducir el tráfico de un cliente, selecciona como origen una dirección que siga la misma ruta esperada.

80.4. Traceroute

Traceroute ayuda a localizar saltos y rutas inesperadas. La ausencia de respuesta de un hop no implica necesariamente caída: muchos routers filtran las respuestas necesarias. Lo útil es comparar dónde deja de progresar el camino y si el destino final responde.

80.5. Test Port

Test Port realiza una conexión TCP desde el firewall hacia un host/puerto. Es útil para distinguir «no hay red» de «el servicio concreto no acepta TCP». No sirve para verificar un servicio UDP de la misma forma.

80.6. DNS Lookup

DNS Lookup permite consultar nombres y comparar tiempos de respuesta de los servidores DNS configurados. Es especialmente valioso para demostrar que el firewall resuelve correctamente aunque un cliente no lo haga, o para detectar que un upstream concreto no responde.

80.7. Herramientas complementarias: Modern Terminal AI

La prueba desde pfSense no siempre explica lo que sucede en el cliente. **Modern Terminal AI** es una herramienta para Windows que reúne diagnóstico de red, análisis de puertos y conexiones TCP/UDP y asistencia opcional mediante IA. Ayuda a investigar el proceso de origen antes de comparar evidencias con el firewall.



Ejemplo de investigación

1. Identificar en Windows el proceso, el destino y el puerto de una conexión.
2. Buscar en pfSense el estado correspondiente y contrastar regla, NAT y ruta.
3. Si no coincide, revisar DNS, firewall local, camino de ida y retorno.

Criterio: la IA puede explicar un puerto o una conexión, pero sus conclusiones deben contrastarse con registros y capturas. Utilizar las pruebas de puertos solo en sistemas autorizados; revisar los datos enviados si se utiliza IA remota.

Sitio oficial · modernterminal-ai.com Ver una captura real del Centro TCP/UDP

Esquema editorial del proceso de diagnóstico; no es una captura de la aplicación.

Capítulo 81. CLI y pfctl: entrar debajo de la WebGUI sin romper el sistema

La shell ofrece visibilidad extraordinaria, pero pfSense no debe administrarse como un FreeBSD genérico. Muchos archivos se regeneran desde config.xml. Modificar a mano reglas o archivos generados puede perderse al aplicar cambios y crear discrepancias difíciles de reproducir.

Advertencia

Utiliza shell y Diagnostics > Command Prompt para diagnóstico y operaciones conocidas. No conviertas cambios manuales no persistentes en configuración de producción.

81.1. pfctl como herramienta de lectura

pfctl consulta el estado de PF: reglas cargadas, estados, estadísticas, tablas y counters. En un libro de administración interesa principalmente como instrumento de verificación, no para sustituir la WebGUI.

```
pfctl -si            # información/estadísticas PF
pfctl -ss            # estados
pfctl -sr            # reglas cargadas
pfctl -sn            # reglas NAT
pfctl -sa            # información amplia
pfctl -t NOMBRE -T show  # contenido de una tabla/alias
```

81.2. Correlacionar GUI y reglas cargadas

La GUI expresa intención; PF ejecuta reglas generadas. Ante una duda avanzada, comparar el objeto configurado con la regla cargada ayuda a descubrir diferencias causadas por NAT, aliases, grupos, floating rules o reglas automáticas.

81.3. Sockets

Diagnostics > Sockets muestra procesos que escuchan o mantienen conexiones. Si esperas que un servicio del firewall atienda un puerto y no aparece ningún socket, el problema está antes de las reglas de cliente: el daemon no está escuchando donde creías.

81.4. top y System Activity

Diagnostics > System Activity ejecuta una vista equivalente a top con procesos e hilos. Cuando la CPU se dispara, identificar qué proceso consume tiempo permite diferenciar Unbound, IDS/IPS, PHP, routing, OpenVPN u otra carga.

81.5. Command Prompt

Diagnostics > Command Prompt ejecuta comandos como un shell privilegiado. Los comandos deben terminar; una captura o ping sin límite puede no devolver salida en esa interfaz. Para tareas interactivas o continuas, la consola/SSH es más apropiada.

Capítulo 82. Rendimiento: buscar el cuello de botella correcto

Un firewall lento no siempre necesita una CPU mayor. Puede estar limitado por un enlace, NIC, interrupciones, estados, cifrado, IDS/IPS, MTU, pérdida del ISP, disco o incluso por un servidor destino. Antes de comprar hardware hay que localizar el recurso que satura.

82.1. CPU

Observa carga total y proceso/hilo responsable. Un solo flujo puede no utilizar todos los núcleos dependiendo del protocolo y del camino de procesamiento. La frecuencia, aceleración criptográfica y diseño del software importan tanto como el número de cores.

82.2. Memoria

FreeBSD utiliza memoria de forma agresiva para cachés; «poca memoria libre» no equivale automáticamente a falta de RAM. Lo relevante es la presión real, swapping inesperado, crecimiento continuo de procesos y límites de estados/tablas.

82.3. State table

Un número alto de estados puede ser normal en redes con miles de clientes, pero debe compararse con el máximo y la capacidad del hardware. Un malware, P2P o escaneo puede multiplicar estados con poco throughput.

82.4. Interfaces

Errores, drops, velocidad/duplex negociados incorrectamente, transceptores defectuosos o enlaces saturados generan problemas que el firewall no puede solucionar con reglas. Las estadísticas de interfaz y del switch deben compararse.

82.5. Disco y logs

Un almacenamiento degradado o lleno puede afectar logs, paquetes y comportamiento del sistema. SMART, uso del filesystem y mensajes de I/O forman parte de una revisión de salud. En appliances con almacenamiento flash, la política de escritura también merece consideración.

82.6. Monitoring Graphs

Las gráficas RRD permiten correlacionar CPU, estados, tráfico y calidad de gateway. Una gráfica útil compara variables relacionadas, por ejemplo throughput de WAN frente a RTT/pérdida, o estados frente a CPU.

Patrón observado	Hipótesis a validar
Upload al 100 % + RTT alto	Congestión/bufferbloat.
CPU 100 % + VPN al máximo	Límite de cifrado/protocolo.
Estados suben, tráfico estable	Muchas conexiones pequeñas, escaneo o P2P.

Patrón observado	Hipótesis a validar
Errores NIC suben	Físico/transceptor/duplex/driver.
Pérdida gateway sin saturación	ISP, medio físico o monitor target.

82.7. Gateway monitoring como señal, no oráculo

dpinger mide el camino hacia una dirección de monitor. Si esa dirección deja de responder, pfSense puede declarar alarma aunque Internet siga parcialmente disponible. El monitor debe representar bien la salud del enlace y cada gateway debe utilizar un objetivo apropiado.

Capítulo 83. Tres métodos de troubleshooting que deben convertirse en hábito

83.1. Método por capas

1. Física / enlace
2. VLAN / capa 2
3. IP / prefijo / vecino
4. Routing / gateway
5. Firewall / estado / NAT
6. DNS / servicios auxiliares
7. Aplicación

La ventaja de este método es que impide investigar DNS cuando el cliente no tiene enlace, o NAT cuando el servidor ni siquiera escucha.

83.2. Método por trayectoria

```
ORIGEN → switch/VLAN → interfaz pfSense entrada → PF/NAT/route
    → interfaz pfSense salida → red destino → host/servicio
    ←              retorno              ←
```

Se observa el mismo flujo en puntos sucesivos. El último punto donde aparece correctamente y el primero donde desaparece delimitan el problema.

83.3. Método por evidencia

1. Escribir el síntoma exacto sin interpretación: «10.20.0.25 no abre https://10.30.0.20».

2. Definir qué debería ocurrir según el diseño: ruta, regla y servicio esperados.

3. Recoger una evidencia barata: IP del cliente, ruta, log, estado.

4. Formular una hipótesis falsable: «PF bloquea el SYN en USERS».

5. Elegir una prueba que pueda demostrar que la hipótesis es falsa o verdadera.

6. Cambiar una sola variable únicamente si la evidencia lo justifica.

7. Repetir la prueba y registrar el resultado.

8. Documentar causa raíz y prevención, no solo el cambio que devolvió servicio.

Ejemplo

Hipótesis mala: «pfSense está fallando». Hipótesis útil: «el SYN llega a LAN, crea estado, sale por SERVERS pero no vuelve SYN/ACK; el servidor o su gateway no responde».

83.4. No confundir correlación con causa

Que un problema aparezca después de una actualización no demuestra que la actualización sea la causa. Puede coincidir con renovación DHCP, caída del ISP, cambio de certificado o reinicio de un switch. La línea temporal orienta; la captura y las pruebas confirman.

Capítulo 84. Casos de diagnóstico reproducibles

84.1. «Los usuarios no tienen Internet»

1. Comprobar si afecta a todos o a una VLAN.
2. Desde pfSense, ping a una IP externa usando WAN.
3. Desde pfSense, DNS Lookup de un nombre.
4. Desde pfSense, ping externo usando como origen la IP LAN/VLAN afectada.
5. Desde cliente, comprobar IP/prefijo/gateway/DNS.
6. Comprobar gateway status y rutas.
7. Buscar estados del cliente y revisar firewall log.
8. Capturar en interfaz cliente y WAN si sigue sin explicación.

Si pfSense alcanza Internet desde WAN pero falla al originar desde LAN, NAT/routing/policy routing son candidatos. Si el cliente alcanza IP externa pero no nombres, DNS sube al primer puesto.

84.2. «Un port forward no funciona»

```
Internet
  ↓ captura WAN: ¿llega SYN?
PF/NAT: ¿aparece estado/traducción?
  ↓ captura LAN/DMZ: ¿sale hacia servidor?
Servidor: ¿responde?
  ↑ retorno: ¿usa pfSense como camino?
WAN: ¿sale SYN/ACK traducido?
```

Este procedimiento evita culpar automáticamente a NAT cuando el ISP no entrega el paquete o el servidor tiene su propio firewall activo.

84.3. «La web abre por IP pero no por nombre»

Routing y conectividad IP ya están parcialmente demostrados. Comprobar DNS entregado por DHCP, consulta directa al resolver, Unbound, overrides, DNSSEC, split DNS y cachés. No cambies reglas de NAT salvo que la evidencia las implique.

84.4. «La VPN está up pero no pasa tráfico»

Separar underlay, túnel, routing y policy. Un handshake WireGuard o una SA IPsec solo demuestra la capa criptográfica. Revisar rutas/Allowed IPs/selectors, reglas VPN, retorno y subredes solapadas.

84.5. «CARP cambió de MASTER sin razón aparente»

Comparar logs CARP/sistema, interfaz, pfsync/SYNC, gateway monitoring y pérdida de red entre nodos. Un cambio de estado puede ser consecuencia de demotion, interfaz física o decisión de gateway, no necesariamente de CARP en sí.

84.6. «El firewall está lento»

Definir lento: ¿GUI, throughput, latencia, VPN, DNS o creación de conexiones? Después correlacionar CPU, procesos, estados, interfaces, RRD, gateway RTT/pérdida y paquetes. Sin definir la métrica, “lento” no es diagnosticable.

84.7. «Solo una aplicación falla»

Si otras aplicaciones sobre la misma red funcionan, reducir el alcance: DNS específico, puerto/protocolo, MTU, TLS/certificado, proxy, firewall local, dependencia externa. Packet capture ayuda a ver si la sesión falla en SYN, TLS o después de establecer TCP.

Capítulo 85. Laboratorio integral: investigar sin adivinar

Este laboratorio utiliza la pyme segmentada construida en partes anteriores. Introduciremos fallos controlados y el alumno deberá localizar la causa utilizando un runbook, sin mirar primero la configuración que fue alterada.

85.1. Topología base

Zona	Red	Elemento
USERS	10.20.0.0/24	Clientes y DNS corporativo.
SERVERS	10.30.0.0/24	ERP 10.30.0.20:443.
IOT	10.40.0.0/24	Dispositivos aislados.
GUEST	10.50.0.0/24	Internet-only.
VPN	10.250.10.0/24	Teletrabajo OpenVPN.
WAN1/WAN2	Proveedores distintos	Multi-WAN.

85.2. Incidente A: DNS equivocado por DHCP

Síntoma entregado al alumno: USERS llega por IP a Internet pero no resuelve nombres. Debe demostrar primero conectividad IP, después comparar DNS del cliente y DNS Lookup desde pfSense, revisar lease y localizar la opción incorrecta.

85.3. Incidente B: gateway de retorno incorrecto en ERP

Síntoma: el SYN de USERS llega a 10.30.0.20, pero no aparece respuesta en pfSense. La captura en SERVERS demuestra la llegada. El siguiente paso es el servidor: gateway local o firewall. El ejercicio enseña cuándo dejar de tocar pfSense.

85.4. Incidente C: ruta VPN ausente

El túnel WireGuard muestra handshake reciente, pero una nueva VLAN de sede remota no funciona. States y captura muestran que el tráfico no entra por el túnel adecuado. La causa es una red no incluida en routing/Allowed IPs según el diseño.

85.5. Incidente D: WAN saturada

Usuarios describen «Internet lento». Gateway RTT sube al mismo tiempo que la subida de WAN alcanza su capacidad. CPU y estados permanecen normales. El alumno debe distinguir congestión de fallo del firewall y proponer medición/traffic shaping como siguiente investigación.

85.6. Incidente E: regla cambiada, estado antiguo

Se endurece una regla, pero una sesión existente continúa. El alumno consulta Diagnostics > States, identifica el estado creado antes del cambio y aprende a eliminar únicamente ese estado si se necesita una aplicación inmediata de la nueva política.

85.7. Runbook operativo

Paso	Acción	Evidencia a conservar
1	Registrar hora, alcance y síntoma exacto.	Ticket/línea temporal.
2	Comprobar cambios recientes.	Audit/config backup/change log.
3	Estado del sistema y gateways.	Captura/dashboard/valores.
4	Rutas, vecinos y servicio relevante.	Routes/ARP/NDP/status.
5	Firewall log y estados.	Entradas filtradas.
6	Packet capture en puntos clave.	PCAP limitado.
7	Aplicar cambio mínimo o rollback.	Qué cambió y por qué.
8	Validar servicio y efectos laterales.	Matriz de pruebas.
9	Identificar causa raíz.	Explicación técnica.
10	Definir prevención/monitorización.	Acción posterior.

Resultado del laboratorio

El objetivo no es resolver cinco averías. Es adquirir una disciplina: observar, delimitar, demostrar, corregir y verificar. Esa disciplina funciona igual para un firewall doméstico, una pyme o una infraestructura crítica.

85.8. Hoja rápida de diagnóstico

```
¿ENLACE?     → status NIC / switch
¿IP?         → cliente + interfaz
¿VECINO?     → ARP / NDP
¿RUTA?       → Diagnostics Routes / route -n get
¿GATEWAY?    → Status Gateways / dpinger log
¿PF?         → firewall log + states + pfTop
¿NAT?        → states + pfctl -sn + captura ambos lados
¿DNS?        → DNS Lookup / dig/nslookup
¿PAQUETE?    → Packet Capture / tcpdump
¿SERVICIO?   → Test Port / sockets / logs del daemon
```

Glosario de la Parte X

Término	Definición
Observabilidad	Capacidad de inferir el estado del sistema mediante métricas, logs, estados y trazas.
RRD	Round-Robin Database utilizada para conservar series temporales de tamaño acotado.
State table	Tabla de conexiones/estados mantenida por PF.
pfTop	Visor dinámico de estados, reglas y tasas de tráfico.
pfInfo	Estadísticas y contadores internos de PF.
PCAP	Archivo que contiene paquetes capturados para análisis.
tcpdump	Herramienta de captura de paquetes en línea de comandos.
ARP	Resolución de vecinos IPv4 en una red local.
NDP	Descubrimiento de vecinos y funciones asociadas de IPv6.
Syslog	Mecanismo de transporte/registro de eventos hacia un colector.
dpinger	Daemon utilizado por pfSense para monitorización de gateways.
Root cause	Causa técnica subyacente que explica el incidente, no solo el síntoma.
Baseline	Comportamiento normal de referencia con el que comparar anomalías.

Fuentes técnicas de contraste

Las páginas oficiales siguientes se han utilizado para verificar herramientas, ubicaciones y comportamiento vigente. Verificación técnica: 8 de octubre de 2026.

- **System Monitoring:** https://docs.netgate.com/pfsense/en/latest/monitoring/index.html
- **Monitoring Graphs:** https://docs.netgate.com/pfsense/en/latest/monitoring/graphs/index.html
- **System Logs:** https://docs.netgate.com/pfsense/en/latest/monitoring/logs/index.html
- **Remote Logging with Syslog:** https://docs.netgate.com/pfsense/en/latest/monitoring/logs/remote.html
- **Working with Log Files:** https://docs.netgate.com/pfsense/en/latest/monitoring/logs/manage.html
- **Firewall States:** https://docs.netgate.com/pfsense/en/latest/monitoring/status/firewall-states.html

- **pfTop:** https://docs.netgate.com/pfsense/en/latest/monitoring/status/pftop.html
- **pfInfo:** https://docs.netgate.com/pfsense/en/latest/monitoring/status/pfinfo.html
- **Packet Capturing:** https://docs.netgate.com/pfsense/en/latest/diagnostics/packetcapture/index.html
- **Using tcpdump:** https://docs.netgate.com/pfsense/en/latest/diagnostics/packetcapture/tcpdump.html
- **Selecting the Proper Interface:** https://docs.netgate.com/pfsense/en/latest/diagnostics/packetcapture/interface.html
- **Route Table Contents:** https://docs.netgate.com/pfsense/en/latest/monitoring/status/routes.html
- **Troubleshooting Routes:** https://docs.netgate.com/pfsense/en/latest/troubleshooting/routes.html
- **ARP Table:** https://docs.netgate.com/pfsense/en/latest/monitoring/status/arp.html
- **NDP Table:** https://docs.netgate.com/pfsense/en/latest/monitoring/status/ndp.html
- **DNS Lookup:** https://docs.netgate.com/pfsense/en/latest/diagnostics/dns.html
- **Ping Host:** https://docs.netgate.com/pfsense/en/latest/diagnostics/ping.html
- **Traceroute:** https://docs.netgate.com/pfsense/en/latest/diagnostics/traceroute.html
- **Troubleshooting Network Connectivity:** https://docs.netgate.com/pfsense/en/latest/troubleshooting/connectivity.html
- **Troubleshooting Firewall Rules:** https://docs.netgate.com/pfsense/en/latest/troubleshooting/firewall.html
- **Diagnostics:** https://docs.netgate.com/pfsense/en/latest/menuguide/diagnostics.html

Cierre de la Parte X

Al terminar esta parte, el lector debería ser capaz de investigar un fallo con pruebas reproducibles y distinguir dónde deja de funcionar un flujo. La siguiente parte cambiará de enfoque: veremos pfSense dentro de hipervisores y plataformas virtuales, incluyendo Proxmox, VMware y Hyper-V, y analizaremos rendimiento, bridges, VLAN, VirtIO y passthrough.

pfSense® software

REDES, FIREWALL Y SEGURIDAD

Arquitectura, administración y laboratorios prácticos

PARTE XI

Virtualización y despliegue avanzado

Oscar de la Cuesta

palentino.es



Primera edición · octubre de 2026

Apertura de la Parte XI

Virtualizar un servidor suele significar abstraer CPU, memoria, disco y red para administrarlos con más flexibilidad. Virtualizar el firewall añade una condición especial: la propia conectividad del hipervisor, de otras máquinas virtuales e incluso de la consola de administración puede depender de la VM que estamos ejecutando sobre ese mismo host.

Esta parte no pretende convertir pfSense en una receta de Proxmox, VMware o Hyper-V. El objetivo es comprender las capas adicionales que aparecen cuando el firewall deja de poseer directamente todas sus NIC y pasa a recibir interfaces virtuales, bridges, vSwitches, VLAN y recursos gestionados por un hipervisor.

Pregunta central
¿Qué ocurre con la seguridad y la disponibilidad cuando el dispositivo que separa WAN y LAN es, en realidad, un proceso virtual que comparte CPU, memoria, almacenamiento y switching con otras cargas?

Mapa de capítulos

Capítulo	Tema
86	Cuándo virtualizar un firewall y cuándo mantenerlo físico.
87	Modelo de capas: NIC, vSwitch/bridge, vNIC, FreeBSD y pfSense.
88	Proxmox VE: diseño de red, VirtIO, bridges y VLAN-aware.
89	Passthrough PCI/SR-IOV y acceso casi directo al hardware.
90	VMware vSphere/ESXi: vSwitch, port groups y compatibilidad.
91	Microsoft Hyper-V: virtual switches y adaptadores sintéticos.
92	Rendimiento, offloading, MTU, CPU, NUMA y almacenamiento.
93	Seguridad del hipervisor y dependencia circular.
94	Alta disponibilidad, migración, backup y recuperación.
95	Laboratorios y arquitecturas de referencia.

Capítulo 86. ¿Debe el firewall ser una máquina virtual?

La virtualización aporta consolidación, snapshots del entorno, automatización, administración remota y rapidez de despliegue. Pero un firewall perimetral no es una carga cualquiera: si falla, puede perderse el acceso remoto al propio hipervisor que debería ayudarnos a repararlo.

86.1. Ventajas reales

- Aprovechar un clúster o servidor ya existente sin adquirir otra plataforma.
- Crear laboratorios y clones con rapidez.
- Separar redes mediante bridges y port groups sin recablear físicamente cada prueba.
- Automatizar backup de disco y configuración del entorno virtual.
- Escalar CPU y RAM con mayor facilidad que en appliances cerrados.
- Integrar la VM en estrategias de monitorización y gestión del hipervisor.

86.2. Costes que no deben ocultarse

- El firewall hereda fallos del host, del almacenamiento y de la capa de switching virtual.
- Una actualización o reinicio del hipervisor puede cortar Internet y VPN.
- La configuración de bridges/vSwitch puede crear exposiciones que pfSense no puede ver ni impedir.
- Un administrador del hipervisor tiene poder indirecto sobre las NIC y discos del firewall.
- La recuperación puede requerir acceso local o gestión fuera de banda cuando la propia VM está caída.

Criterio profesional

Para laboratorios y muchos entornos empresariales, virtualizar pfSense es perfectamente viable. Para un perímetro crítico, la decisión debe comparar el beneficio operativo con el aumento de dependencias. La propia documentación oficial recomienda hipervisores tipo 1 en producción y advierte que un firewall perimetral puede justificar hardware dedicado.

86.3. Tres patrones de despliegue

Patrón	Fortaleza	Debilidad
Appliance físico dedicado	Aislamiento de fallos y cableado directo.	Otro equipo que adquirir, alimentar y mantener.
pfSense VM en host único	Flexibilidad y coste bajo.	El host se convierte en punto único de fallo.
pfSense VM en clúster	Recuperación y orquestación superiores.	Mayor complejidad; la red del clúster debe sobrevivir al fallo del firewall.

86.4. Firewall virtual no significa firewall menos real

Las reglas PF, estados, NAT, VPN y servicios operan igual desde el punto de vista lógico. Lo que cambia es cómo llegan los paquetes a las interfaces. La VM ya no controla necesariamente el puerto físico; recibe frames que el hipervisor decidió entregarle.

Capítulo 87. La cadena virtual: del cable a vtnet0

En un firewall físico podemos dibujar cable → NIC → driver → interfaz. En una VM aparecen varias capas intermedias. Comprenderlas es imprescindible para localizar un fallo.

```
Cable WAN
  ↓
NIC física del host
  ↓
bridge / vSwitch / port group
  ↓
vNIC de la VM
  ↓
driver virtual en FreeBSD
  ↓
vtnet0 / vmx0 / hn0
  ↓
pfSense: WAN
```

87.1. Bridge o vSwitch

Un bridge de Linux, un vSwitch de VMware o un Virtual Switch de Hyper-V realiza switching Ethernet dentro del host. Puede conectar una NIC física, varias vNIC, VLAN y redes completamente internas. En esta capa pueden existir errores aunque pfSense muestre su interfaz como UP.

87.2. vNIC

La VM ve una tarjeta virtual. Puede ser emulada —imitando hardware conocido— o paravirtualizada, diseñada específicamente para el entorno virtual. VirtIO es el ejemplo típico en KVM/Proxmox. FreeBSD incorpora los drivers VirtIO utilizados por pfSense, por lo que no requiere instalar un paquete de drivers adicional.

87.3. MAC y persistencia

La MAC de una vNIC es una pieza de identidad importante. Cambiarla puede afectar a reservas DHCP, upstream que memoriza la CPE, reglas, DHCP estático o licencias de terceros. Durante migraciones y restauraciones conviene conservar o documentar las MAC.

87.4. Red interna sin NIC física

Un bridge puede no tener ningún puerto físico. Esto permite crear segmentos que existen solo entre VM, por ejemplo una DMZ de laboratorio. El tráfico entre dos máquinas del mismo bridge puede no abandonar nunca el host físico.

Qué ocurre realmente
Si una VM de servidor y pfSense comparten un bridge interno, el paquete puede recorrer RAM y estructuras del kernel del hipervisor sin llegar a un switch físico. Capturar en el switch de rack no mostraría ese flujo.

Capítulo 88. Proxmox VE: pfSense sobre KVM

Proxmox VE utiliza KVM para virtualización completa y Linux Bridge u OVS para networking según el diseño. En un esquema sencillo, pfSense recibe al menos una vNIC WAN y una vNIC LAN conectadas a bridges diferentes.

88.1. Separar gestión, WAN y LAN

```
NIC 1 ── vmbr0 ── Gestión Proxmox
NIC 2 ── vmbr1 ── vNIC WAN de pfSense
NIC 3 ── vmbr2 ── vNIC LAN de pfSense
                    ↓
              switch / trunk interno
```

Esta separación física es muy clara, aunque consume puertos. En plataformas con menos NIC se puede transportar varias VLAN por un trunk y mantener la gestión del host en una VLAN independiente.

88.2. VirtIO frente a emulación

VirtIO reduce la emulación de hardware y suele ofrecer mejor rendimiento. pfSense identifica estas interfaces como vtnet. La documentación vigente recomienda VirtIO y advierte de comprobar el hardware checksum offload: en Proxmox/KVM debe estar desactivado para evitar tráfico corrupto o rendimiento anómalo; las versiones actuales intentan hacerlo automáticamente para vtnet, pero conviene verificarlo.

Ajuste importante
Con VirtIO/KVM, comprueba System > Advanced > Networking > Disable hardware checksum offload. Si aparecen problemas persistentes, también puede ser necesario revisar offloading en el host.

88.3. VLAN-aware bridge

Un bridge VLAN-aware puede transportar múltiples VLAN hasta la VM. Hay dos modelos válidos, pero deben elegirse conscientemente:

Modelo	Dónde se separan VLAN	Ventaja
Trunk hasta pfSense	pfSense crea VLAN sobre una única vNIC.	La política de VLAN queda visible en el firewall.
Una vNIC por VLAN	Proxmox filtra/taggea y entrega una red por vNIC.	Interfaz pfSense muy simple; más vNIC y dependencia del host.

Mezclar ambos modelos sin documentación suele producir dobles tags, VLAN desaparecidas o tráfico entregado a la interfaz equivocada.

88.4. UEFI y tipo de máquina

pfSense puede arrancar con UEFI en Proxmox. En el procedimiento oficial actual se documenta q35 + OVMF con disco EFI y Secure Boot desactivado. No es obligatorio convertir una VM que ya funciona en BIOS tradicional; hacerlo solo por estética introduce un cambio sin beneficio operativo inmediato.

88.5. La gestión no debe depender de la misma VM

Si el host Proxmox solo es alcanzable a través de pfSense y esa VM no arranca, la administración remota puede desaparecer. Es preferible disponer de una red de gestión independiente, IPMI/iDRAC/iLO u otra vía fuera de banda.

El problema del huevo y la gallina

Necesitas Proxmox para arrancar pfSense, pero necesitas pfSense para llegar a Proxmox. Si el diseño crea esta dependencia circular, documenta una ruta de recuperación que no dependa del firewall virtual.

88.6. No confundir VLAN-aware con seguridad

Marcar un bridge como VLAN-aware permite transportar etiquetas; no reemplaza las reglas de firewall ni garantiza que cada VM esté correctamente aislada. La configuración del host determina qué VLAN puede llegar a cada vNIC antes de que pfSense tenga oportunidad de filtrarla.

Capítulo 89. PCI passthrough y SR-IOV

La alternativa a entregar una vNIC es asignar una NIC física, o una función virtual de hardware, casi directamente a la VM. Esto reduce capas y puede mejorar previsibilidad, pero sacrifica parte de la flexibilidad del hipervisor.

89.1. PCI passthrough

Con IOMMU/VT-d/AMD-Vi, una tarjeta PCIe puede asignarse a pfSense. El host deja de utilizarla de forma ordinaria y la VM accede al dispositivo con su driver FreeBSD.

Ventaja	Consecuencia
Acceso más directo a la NIC	Menor dependencia del bridge virtual para ese puerto.
Driver nativo de FreeBSD	Hay que asegurar compatibilidad de la NIC con pfSense/FreeBSD.
Aislamiento de WAN	El host puede quedar sin presencia lógica en esa red.
Menos abstracción	Live migration suele complicarse o dejar de ser posible.

89.2. Grupos IOMMU

El aislamiento real de dispositivos depende de los grupos IOMMU de la plataforma. Dos funciones inseparables en el mismo grupo pueden impedir asignar una sin afectar a la otra. La placa base y el firmware son tan importantes como el hipervisor.

89.3. SR-IOV

SR-IOV permite que una NIC cree Virtual Functions que pueden asignarse a VM. Ofrece alto rendimiento y menor intervención del switch virtual, pero exige soporte de NIC, firmware, plataforma, hipervisor y driver invitado. No debe asumirse como una mejora universal.

Decisión

Passthrough es útil cuando el aislamiento o el rendimiento justifican perder movilidad. Para un clúster que dependa de live migration, una vNIC paravirtualizada puede ofrecer mejor equilibrio operativo.

Capítulo 90. VMware vSphere / ESXi

En VMware, las piezas equivalentes son vSwitch o Distributed Switch, port groups y adaptadores virtuales. La lógica sigue siendo la misma: una red WAN del hipervisor debe terminar en la vNIC WAN de pfSense sin mezclarse accidentalmente con redes internas.

90.1. Port groups

Un port group agrupa configuración de conectividad para vNIC. Puede representar WAN, LAN o un trunk VLAN. En entornos con Distributed Switch, la política puede mantenerse a escala de varios hosts, pero también aumenta la importancia de controlar quién puede modificarla.

90.2. Tipo de adaptador

VMXNET3 es un adaptador paravirtualizado habitual en VMware moderno. La compatibilidad final depende de la versión base de FreeBSD utilizada por la versión de pfSense y de la versión de ESXi/virtual hardware. La documentación actual advierte expresamente de comprobar esa matriz, especialmente al cambiar de ramas de FreeBSD.

90.3. Promiscuous mode y seguridad del vSwitch

No debe habilitarse promiscuous mode por reflejo. Solo ciertos diseños, appliances o funciones lo requieren. Las opciones MAC address changes y forged transmits también deben entenderse antes de modificarlas, especialmente en HA o configuraciones con direcciones virtuales.

90.4. Snapshot no es backup del firewall

Un snapshot de VM es una herramienta de reversión del disco virtual. No sustituye un backup de config.xml, ni una copia externa, ni una prueba de restauración. Mantener snapshots durante demasiado tiempo puede penalizar almacenamiento y complicar operaciones.

Capítulo 91. Microsoft Hyper-V

Hyper-V utiliza Virtual Switches y adaptadores sintéticos para conectar las VM. Puede desplegar pfSense en Windows Server o en plataformas con el rol Hyper-V, pero el firewall hereda la disponibilidad y mantenimiento del host Windows.

91.1. Tipos de Virtual Switch

Tipo	Conectividad
External	Conecta VM con una NIC física y el exterior.
Internal	Conecta VM y host, sin salida física directa.
Private	Conecta únicamente VM entre sí.

Un diseño común usa un External Switch para WAN y otro para LAN, o bien LAN sobre un switch virtual enlazado a una NIC/trunk. La gestión del host debe diseñarse aparte para evitar depender de la VM.

91.2. Adaptadores sintéticos

FreeBSD dispone de drivers para los dispositivos virtuales de Hyper-V utilizados por pfSense. Como en cualquier hipervisor, el nombre que ve pfSense identifica el driver invitado, no el puerto físico real.

91.3. MAC dinámica o estática

Para firewalls, HA y restauraciones, una MAC estable simplifica la operación. Cambios automáticos de MAC pueden tener efectos aguas arriba. Documentar las MAC es parte del backup lógico del entorno virtual.

Contexto de seguridad

La documentación de pfSense recuerda que, para un firewall perimetral donde se busque minimizar superficie de ataque, el hardware independiente puede seguir siendo la mejor práctica. Virtualizar es una decisión de arquitectura, no un requisito.

Capítulo 92. Rendimiento y detalles que solo aparecen en virtualización

92.1. Checksum offload

El checksum offload puede causar síntomas engañosos en entornos virtuales: tráfico que parece corrupto, bajo throughput o problemas entre VM del mismo host. En Xen/KVM/VirtIO es un punto de diagnóstico prioritario. Además, una captura realizada antes de que el hardware calcule el checksum puede mostrarlo como incorrecto aunque el paquete final sea válido.

92.2. TSO y LRO

TCP Segmentation Offload y Large Receive Offload agrupan o segmentan trabajo alrededor de la NIC. En un endpoint pueden mejorar rendimiento; en un router/firewall pueden interferir con la inspección y modificación del tráfico. pfSense los mantiene desactivados por defecto en el rol de firewall y no conviene activarlos sin un motivo demostrado.

92.3. CPU virtual

Añadir vCPU no garantiza una mejora lineal. El scheduler del hipervisor necesita encontrar tiempo físico para ejecutarlas. Una VM con demasiadas vCPU puede esperar más que una VM correctamente dimensionada. Para VPN, IDS/IPS y alto PPS importan arquitectura, frecuencia, SIMD y disponibilidad real de CPU.

92.4. CPU type y flags

En KVM/Proxmox, exponer un tipo de CPU próximo al host puede ofrecer instrucciones modernas y mejor rendimiento, pero reduce portabilidad entre nodos heterogéneos. Un modelo genérico facilita migración, a cambio de ocultar algunas extensiones. La elección debe alinearse con la estrategia de clúster.

92.5. NUMA

En hosts con varias regiones NUMA, CPU y memoria no tienen la misma latencia desde todos los sockets. Un firewall de alto rendimiento puede beneficiarse de afinidad y localidad, pero estos ajustes solo deben introducirse después de medir un cuello de botella real.

92.6. Disco

El firewall no suele ser una carga intensiva de almacenamiento, salvo por logs, paquetes, IDS/IPS o proxy. Un almacenamiento lento puede hacer que la GUI parezca torpe, retrasar actualizaciones o agravar una tormenta de logs. El disco virtual debe residir en almacenamiento fiable, con backup independiente de config.xml.

92.7. MTU

Una red virtual puede añadir VLAN, VXLAN, túneles del datacenter u otras encapsulaciones antes de que pfSense vea el paquete. Una MTU inconsistente entre host, vSwitch, NIC y red física puede generar síntomas que parecen un fallo VPN o TCP.

```
Aplicación → TCP/IP invitado → vNIC → bridge/vSwitch → NIC física → switch → red
        MTU 1500     ?        ?           ?
```

Método

Antes de “optimizar” una VM de firewall, crea una línea base: PPS, throughput, latencia, CPU ready/steal, drops, errores de interfaz y uso de estados. Cambia una variable cada vez.

Capítulo 93. El hipervisor se convierte en parte del perímetro

En un firewall físico, comprometer un servidor interno no concede automáticamente control sobre la NIC WAN del firewall. En virtualización, una cuenta administrativa del hipervisor puede reconfigurar bridges, clonar discos, capturar memoria, cambiar una vNIC o apagar la VM. Por tanto, el plano de gestión del hipervisor pasa a formar parte del modelo de amenazas.

93.1. Separar gestión

- VLAN o NIC de gestión independiente.
- Acceso solo desde estaciones administrativas o VPN de gestión.
- MFA en el hipervisor cuando esté disponible.
- No publicar la GUI del hipervisor directamente a Internet.
- Syslog/auditoría remota para cambios administrativos.
- Acceso fuera de banda para recuperación.

93.2. WAN en el host

Si un bridge WAN tiene una IP del host sin necesidad, el propio hipervisor queda presente en la red exterior. Un patrón más limpio es que el bridge de WAN transporte tráfico a la VM sin asignar al host una dirección IP en ese segmento, salvo que exista un requisito explícito y protegido.

93.3. Copias y secretos

Un backup de la VM puede contener config.xml, certificados, claves privadas y PSK. La plataforma de backup del hipervisor debe tratar esas copias como material sensible, cifrarlas cuando corresponda y controlar el acceso a operadores.

93.4. Actualizar el host sin derribar el negocio

El calendario de mantenimiento del hipervisor se convierte en calendario del firewall. Si no existe migración o nodo redundante, cada parche del host puede exigir una ventana de indisponibilidad. Esto debe aceptarse en el diseño, no descubrirse el día de la actualización.

Principio
Virtualizar no elimina hardware: cambia quién lo administra. CPU, RAM, NIC, switch y almacenamiento siguen existiendo, pero ahora hay una capa de software capaz de reconfigurarlos antes de que pfSense vea nada.

Capítulo 94. Alta disponibilidad, migración y recuperación

94.1. Live migration no equivale a HA de firewall

Migrar una VM encendida entre hosts puede reducir indisponibilidad durante mantenimiento. Sin embargo, no sustituye un par pfSense HA: si la propia VM se bloquea, si el guest falla o si el problema está en su configuración, moverla de host conserva el mismo fallo.

94.2. Dos modelos de redundancia

Modelo	Protege principalmente
Una VM + HA del hipervisor	Fallo de host: la VM reinicia en otro nodo.
Live migration	Mantenimiento planificado del host.
Dos pfSense + CARP/pfsync/XMLRPC	Fallo del nodo firewall y continuidad de IP/estados.
Dos pfSense en hosts distintos + HA pfSense	Combina aislamiento de host y de firewall.

94.3. Evitar anti-patrones de clúster

Dos pfSense virtuales sobre el mismo host no protegen frente al fallo de ese host. Para HA real, los nodos deberían residir en hosts distintos y sus redes WAN/LAN/SYNC deben mantener conectividad de capa 2 o el diseño equivalente requerido.

94.4. Backup de VM frente a backup de configuración

El backup de VM conserva sistema, disco y entorno virtual. El backup de config.xml conserva la configuración lógica de pfSense y es mucho más portable. La estrategia correcta usa ambos en niveles diferentes.

94.5. Restaurar en otro hipervisor

Un config.xml puede restaurarse en hardware o VM diferente, pero los nombres de interfaces pueden cambiar. La recuperación debe incluir un mapa de roles, MAC y redes para reasignar WAN, LAN, VLAN y OPT sin depender del nombre antiguo del driver.

94.6. Boot order

Si el firewall proporciona DNS, routing o acceso de red para otras VM, debe arrancar suficientemente pronto. En clústeres, las dependencias entre storage, DNS, autenticación y firewall deben analizarse: un servicio necesario para arrancar pfSense no puede depender exclusivamente de pfSense.

Prueba de desastre

Apagar el host que contiene el firewall en una ventana de laboratorio enseña más que diez diagramas. La pregunta es: ¿puedes seguir administrando el clúster y recuperar Internet sin acceso previo a esa VM?

Capítulo 95. Laboratorios y arquitecturas de referencia

95.1. Laboratorio A: pfSense en Proxmox con tres redes

Elemento	Diseño
Host	Proxmox VE con 3 NIC físicas.
vmbr0	Gestión Proxmox, IP solo del host.
vmbr1	WAN, sin IP del host.
vmbr2	LAN/trunk interno.
pfSense WAN	VirtIO → vmbr1.
pfSense LAN	VirtIO → vmbr2.
CPU/RAM	2-4 vCPU, 4 GB iniciales para laboratorio; ajustar por carga.
Disco	VirtIO/SCSI virtual en almacenamiento fiable.

1. Crear los tres bridges y verificar qué NIC física pertenece a cada uno.
2. Comprobar que vmbr1 no expone una IP de gestión del host hacia WAN.
3. Crear la VM pfSense y asignar dos vNIC VirtIO.
4. Instalar y asignar vtnet0/vtnet1 mediante MAC y bridge, no por suposición.
5. Verificar y desactivar checksum offloading según el diseño VirtIO/KVM.
6. Acceder desde LAN y ejecutar pruebas de throughput, ping y captura.
7. Documentar MAC, bridge, VLAN, tipo de CPU, storage y orden de arranque.

95.2. Laboratorio B: trunk VLAN-aware

```
Switch físico trunk 802.1Q
        ↓
NIC LAN del host
        ↓
vmbr2 VLAN-aware
        ↓
vNIC pfSense (trunk)
        ↓
VLAN 10 MGMT / 20 USERS / 30 SERVERS / 40 IOT
```

1. Configurar el switch físico con un trunk conocido.
2. Permitir únicamente las VLAN necesarias en el bridge/puerto según política.

3. Entregar el trunk a pfSense por una única vNIC.
4. Crear VLAN en pfSense sobre la interfaz padre.
5. Asignarlas y aplicar direccionamiento/reglas.
6. Capturar tráfico etiquetado en el host y tráfico lógico en pfSense para comprobar dónde se elimina el tag.

95.3. Laboratorio C: passthrough de WAN

1. Activar IOMMU en firmware y host.
2. Identificar grupo IOMMU de la NIC WAN.
3. Reservar la NIC para passthrough.
4. Asignarla a pfSense y dejar el host sin IP en WAN.
5. Verificar compatibilidad del driver FreeBSD.
6. Comparar rendimiento, capacidad de migración y facilidad de recuperación frente a VirtIO.

95.4. Laboratorio D: fallo del host

Escenario: pfSense está virtualizado y proporciona salida a Internet. Se simula una caída completa del host.

1. Confirmar que existe consola fuera de banda o acceso local.
2. Apagar el host de forma controlada.
3. Observar qué servicios de gestión permanecen accesibles.
4. Si hay clúster, medir el tiempo hasta el reinicio de la VM en otro nodo.
5. Validar WAN, LAN, DNS, VPN y rutas tras recuperación.
6. Repetir con dos nodos pfSense HA en hosts distintos y comparar continuidad.

95.5. Matriz de decisión final

Necesidad	Diseño que suele encajar
Laboratorio/formación	Una VM con bridges virtuales.
Pyme con host robusto y ventana de mantenimiento	pfSense VM + backup + gestión fuera de banda.
Perímetro crítico sin clúster	Hardware dedicado o dos appliances HA.
Datacenter virtualizado	Dos VM pfSense en hosts distintos + HA pfSense.
Máximo aislamiento WAN	NIC dedicada o passthrough cuando compense la pérdida de movilidad.
Movilidad/live migration prioritaria	VirtIO/vNIC sobre switching virtual bien diseñado.

Resultado esperado

El lector debe poder mirar un diagrama de virtualización y señalar qué capa puede bloquear, etiquetar, traducir o perder un paquete antes de llegar a pfSense. También debe ser capaz de recuperar el firewall sin depender de la conectividad que ese mismo firewall proporciona.

Checklist de troubleshooting virtual

Síntoma	Primera comprobación
pfSense ve vNIC UP pero no hay tráfico	Bridge/vSwitch, port group, VLAN y NIC física.
Solo fallan otras VM del mismo host	Checksum/offloading y switching virtual.
WAN funciona tras migrar pero LAN no	Asociación de bridges/port groups en host destino.
Rendimiento irregular	CPU ready/steal, vCPU sobredimensionadas, offload, drops, MTU.
HA no cambia correctamente	MAC/VIP, switch virtual, anti-spoofing y ubicación de nodos.
Host inaccesible cuando pfSense cae	Dependencia circular de la red de gestión.
Tras restauración cambian interfaces	MAC, driver virtual y reasignación WAN/LAN.
Captura en pfSense no muestra paquete	Capturar antes en bridge/vSwitch/NIC física.

Glosario de la Parte XI

Término	Definición
Hipervisor tipo 1	Capa de virtualización ejecutada directamente sobre el hardware/OS especializado del host.
vNIC	Interfaz de red virtual entregada a una VM.
Bridge/vSwitch	Conmutador virtual que conecta vNIC, NIC físicas y redes internas.
VirtIO	Familia de dispositivos paravirtualizados usada en KVM.
vtnet	Nombre habitual del driver/interfaz VirtIO en FreeBSD/pfSense.
VLAN-aware	Bridge capaz de tratar etiquetas 802.1Q de forma explícita.
PCI passthrough	Asignación casi directa de un dispositivo PCI a una VM mediante IOMMU.

Término	Definición
SR-IOV	Tecnología que crea funciones virtuales hardware de una NIC para VM.
IOMMU	Mecanismo que traduce/aisla acceso DMA de dispositivos para virtualización.
Live migration	Traslado de una VM en ejecución entre hosts compatibles.
CPU ready/steal	Tiempo en que la VM desea ejecutar CPU pero el host no la programa inmediatamente.
OVMF	Firmware UEFI para máquinas virtuales QEMU/KVM.
Port group	Agrupación lógica de puertos/configuración de red en VMware.
Virtual Switch	Conmutador software de Hyper-V.

Fuentes técnicas de contraste

Las siguientes fuentes oficiales se han utilizado para contrastar compatibilidad, comportamiento actual de virtualización y recomendaciones técnicas. Verificación técnica: 8 de octubre de 2026.

- **Virtualization overview:** https://docs.netgate.com/pfsense/en/latest/virtualization/index.html
- **VirtIO Drivers:** https://docs.netgate.com/pfsense/en/latest/virtualization/virtio.html
- **Virtualizing with Proxmox VE:** https://docs.netgate.com/pfsense/en/latest/recipes/virtualize-proxmox-ve.html
- **Virtualizing with VMware vSphere / ESXi:** https://docs.netgate.com/pfsense/en/latest/recipes/virtualize-esxi.html
- **Virtualizing with Hyper-V:** https://docs.netgate.com/pfsense/en/latest/recipes/virtualize-hyper-v.html
- **Advanced Networking / NIC offloading:** https://docs.netgate.com/pfsense/en/latest/config/advanced-networking.html
- **Troubleshooting Low Interface Throughput:** https://docs.netgate.com/pfsense/en/latest/troubleshooting/low-throughput.html
- **Versions of pfSense and FreeBSD:** https://docs.netgate.com/pfsense/en/latest/releases/versions.html
- **Hardware Selection:** https://docs.netgate.com/pfsense/en/latest/hardware/selection.html
- **VLANs:** https://docs.netgate.com/pfsense/en/latest/vlan/index.html

Cierre de la Parte XI

Virtualizar pfSense no cambia los fundamentos del firewall, pero sí cambia el terreno sobre el que se apoya. La red física ya no llega directamente a todas sus interfaces; antes atraviesa una capa de virtualización que también debe diseñarse, protegerse, documentarse y monitorizarse.

pfSense® software

REDES, FIREWALL Y SEGURIDAD

Arquitectura, administración y laboratorios prácticos

PARTE XII

Laboratorios integrales, recuperación y anexos de referencia

Oscar de la Cuesta

palentino.es



Primera edición · octubre de 2026

Apertura de la Parte XII

Las once partes anteriores construyeron el conocimiento por capas: hardware, interfaces, direccionamiento, routing, PF, NAT, servicios, VPN, seguridad, alta disponibilidad, diagnóstico y virtualización. Esta Parte XII cambia el enfoque. Ya no estudia una función aislada: obliga a combinar varias de ellas en escenarios que se parecen a una red real.

El objetivo es entrenar una forma de pensar. Cada laboratorio parte de requisitos de negocio, los transforma en zonas y flujos, implementa controles, define pruebas de aceptación y termina con una estrategia de recuperación. El lector debe ser capaz de explicar no solo qué ha configurado, sino qué riesgo reduce y cómo demostrará que funciona.

Regla de los laboratorios

Un laboratorio termina cuando existe evidencia de que el diseño cumple su objetivo, no cuando la WebGUI deja de mostrar errores. Cada escenario incluye criterios de aceptación, pruebas negativas y un punto de restauración.

Mapa de la Parte XII

Capítulo	Escenario principal
96	Método común para diseñar y documentar laboratorios.
97	Hogar avanzado con IoT, invitados y teletrabajo.
98	Pyme segmentada con servidores, voz, Wi-Fi y administración.
99	DMZ y publicación controlada de servicios.
100	Empresa multisede con VPN, DNS y continuidad.
101	Alta disponibilidad, Multi-WAN y pruebas de desastre.
102	Recuperación: config.xml, AutoConfigBackup y reconstrucción.
103	Auditoría técnica y revisión periódica de seguridad.
104	Operación, cambios, actualizaciones y documentación viva.
105	Anexos rápidos: matrices, checklists y hoja de diagnóstico.

Capítulo 96. Método común: de requisito a evidencia

El error más frecuente en un laboratorio de firewall es empezar por las reglas. Antes de escribir una regla debe existir una necesidad comprensible: quién necesita comunicarse, con qué servicio, en qué dirección, bajo qué identidad y qué debería ocurrir si la comunicación no está autorizada.

96.1. Cadena de diseño

```
REQUISITO → ZONA → FLUJO → CONTROL → CONFIGURACIÓN → PRUEBA → EVIDENCIA → BACKUP
```

Esta cadena evita confundir la configuración con el objetivo. Dos organizaciones pueden utilizar exactamente la misma regla técnica y perseguir resultados distintos; el contexto de negocio es el que da sentido a la política.

96.2. Ficha mínima de un flujo

Campo	Ejemplo
Origen	USERS 10.20.0.0/24
Destino	ERP 10.30.0.20
Servicio	HTTPS/TCP 443
Dirección	USERS → SERVERS
Necesidad	Acceso al ERP corporativo
Identidad	Usuarios corporativos; control adicional en la aplicación
Registro	Log de bloqueos; acceso exitoso visible en aplicación
Prueba negativa	USERS no alcanza SSH/22 del ERP

96.3. Criterios de aceptación

Un criterio de aceptación es una frase verificable. “La VLAN de invitados está aislada” es demasiado amplia. “Un cliente GUEST obtiene IP, resuelve DNS, navega a Internet y no puede abrir TCP 443 contra 10.20.0.0/16” es una condición comprobable.

Prueba negativa
Probar solo que algo funciona demuestra disponibilidad. Probar también que aquello que debe estar prohibido permanece bloqueado demuestra control.

96.4. Evidencia y reversibilidad

- Captura o registro del estado antes del cambio.
- Backup completo de configuración.
- Lista de comandos/pruebas que demuestran el resultado.
- Registro de reglas o aliases modificados.
- Criterio de rollback: qué síntoma obliga a revertir.
- Copia posterior al cambio una vez validado.

Capítulo 97. Laboratorio integral: hogar avanzado

Un hogar moderno puede contener ordenadores, teléfonos, televisores, asistentes, cámaras, consolas, NAS, domótica y dispositivos que reciben pocas actualizaciones. El objetivo del laboratorio es separar el riesgo sin convertir la red doméstica en un entorno imposible de usar.

97.1. Requisitos

Zona	Objetivo
TRUSTED	PC, móviles y equipos personales de confianza.
IOT	TV, asistentes, cámaras y domótica.
GUEST	Visitas: solo Internet.
SERVICES	NAS, Home Assistant u otros servicios locales.
MGMT	Gestión de firewall, switch y AP.

97.2. Plan de red

VLAN	Red	DHCP	Política base
10 MGMT	10.10.10.0/24	Reservas/limitado	Solo administración.
20 TRUSTED	10.10.20.0/24	Sí	Internet + servicios internos autorizados.
30 IOT	10.10.30.0/24	Sí	Internet limitado + destinos locales concretos.
40 GUEST	10.10.40.0/24	Sí, lease corto	Internet; bloqueadas redes privadas.
50 SERVICES	10.10.50.0/24	Preferencia estáticos/reservas	Solo puertos necesarios desde TRUSTED.

97.3. Flujo IoT controlado

En lugar de permitir IOT → LAN, se crea una política explícita. Por ejemplo, una cámara necesita NTP, DNS y comunicación con un NVR concreto. El resto de redes privadas permanece bloqueado.

```
CAMARA_IOT → DNS_LOCAL : 53
CAMARA_IOT → NTP_LOCAL : 123
CAMARA_IOT → NVR : puerto requerido
CAMARA_IOT → RFC1918 : BLOCK
CAMARA_IOT → Internet : solo si el dispositivo lo necesita
```

97.4. mDNS y descubrimiento

Separar VLAN rompe algunos mecanismos de descubrimiento basados en multicast/broadcast. La solución profesional no es unir todas las redes otra vez. Debe decidirse si el servicio necesita reflexión/proxy de mDNS, una configuración manual o un controlador que conozca ambos segmentos.

97.5. Acceso remoto

El propietario accede al NAS o Home Assistant mediante VPN. No se publica la administración de pfSense ni del NAS directamente en WAN. Un perfil de acceso remoto recibe únicamente rutas hacia los servicios domésticos necesarios.

97.6. Pruebas de aceptación

Prueba	Resultado
GUEST → 10.10.20.10	Bloqueado.
GUEST → Internet	Permitido.
IOT → firewall WebGUI	Bloqueado.
TRUSTED → NAS HTTPS	Permitido.
VPN → Home Assistant	Permitido.
VPN → MGMT	Bloqueado salvo perfil administrativo.
Cámara → NVR	Permitido.

Resultado

El hogar sigue siendo cómodo, pero un televisor vulnerable no comparte el mismo nivel de confianza que el portátil donde se gestiona banca o documentación.

Capítulo 98. Laboratorio integral: pyme segmentada

Este laboratorio consolida la topología que el libro ha utilizado en capítulos anteriores. La pyme dispone de unos 70 usuarios, servidores locales, telefonía IP, Wi-Fi corporativa, invitados e IoT. El firewall debe permitir trabajar sin convertir la red interna en una superficie plana.

98.1. Zonas y servicios

Zona	Ejemplos	Acceso esperado
MGMT	Switch, AP, Proxmox, pfSense	Solo administradores.
USERS	Puestos de trabajo	ERP, DNS, impresión, Internet.
SERVERS	ERP, ficheros, AD/DNS	Exposición mínima por servicio.
VOICE	Teléfonos IP	PBX, NTP, DNS, proveedor.
IOT	Control horario, TV, sensores	Servicios concretos; sin lateralidad.
GUEST	Wi-Fi visitas	Internet únicamente.
BACKUP	Repositorio/copias	Solo orígenes y puertos de backup.

98.2. Administración separada

El mayor cambio frente a una red pequeña es que la administración deja de ser “desde cualquier PC de IT”. MGMT se trata como una zona privilegiada. Los técnicos acceden desde equipos administrados o mediante un jump host, y la WebGUI escucha únicamente donde es necesario.

98.3. DNS y Active Directory

Los clientes de dominio consultan a los DNS de Active Directory; estos resuelven las zonas corporativas y reenvían el resto hacia un resolver aprobado. pfSense continúa aplicando routing y filtrado sin romper la lógica de descubrimiento del dominio.

98.4. Regla por intención, no por comodidad

```
USERS → ERP_HTTPS          PASS
USERS → FILESERVER_SMB     PASS
USERS → DOMAIN_CONTROLLERS  puertos AD requeridos
USERS → MGMT_NET           BLOCK
IOT   → RFC1918            BLOCK (salvo excepciones)
GUEST → RFC1918/ULA        BLOCK
MGMT  → infraestructura    PASS según administración
```

98.5. Impresión y dispositivos heredados

Las impresoras suelen forzar aperturas amplias por desconocimiento. El laboratorio obliga a identificar el protocolo real —IPP, RAW 9100, LPR u otro— y permitir únicamente ese tráfico desde la red de usuarios hacia las IP de impresión.

98.6. Backup como zona

El repositorio de copias merece su propia política. Los servidores pueden enviar copias al repositorio, pero los puestos de usuario no necesitan explorar el almacenamiento de backup. Esta separación reduce el alcance de ransomware y errores administrativos.

98.7. Criterios de aceptación

Prueba	Esperado
USERS → ERP 443	PASS
USERS → Proxmox 8006	BLOCK
IOT → DC	BLOCK
GUEST → ERP	BLOCK
Servidor → backup	PASS solo puertos definidos
USERS → impresora 9100	PASS si es protocolo elegido
MGMT → pfSense HTTPS	PASS
Equipo no MGMT → pfSense HTTPS	BLOCK

Capítulo 99. Laboratorio integral: DMZ y publicación controlada

Publicar un servicio implica aceptar tráfico originado fuera de la organización. La DMZ no convierte un servidor en seguro por sí sola; limita lo que puede alcanzar si ese servidor es comprometido y obliga a documentar los flujos estrictamente necesarios.

99.1. Escenario

La empresa publica un portal HTTPS que necesita consultar una API interna y escribir eventos en un sistema de logs. El servidor web vive en DMZ, la API en SERVERS y la base de datos no se expone directamente a la DMZ.

Componente	Red	Flujo
Portal	10.70.0.10 DMZ	Internet → 443
API	10.30.0.25 SERVERS	Portal → 8443
Syslog	10.30.0.40 SERVERS	Portal → 6514/TLS
DB	10.30.0.30 SERVERS	Solo API → DB; nunca portal directo

99.2. Publicación

El port forward o reverse proxy publica únicamente el servicio requerido. La regla WAN no se amplía a “any”. El acceso de administración del portal se realiza desde MGMT o VPN, nunca mediante el mismo puerto de gestión expuesto a Internet.

99.3. Egress de la DMZ

Una DMZ segura también controla salida. Un servidor comprometido no debería disponer de Internet sin límites. Actualizaciones, DNS, NTP y repositorios se permiten según necesidad. Conexiones hacia USERS se bloquean de forma predeterminada.

Qué protege la DMZ
La DMZ no evita que el portal tenga una vulnerabilidad. Reduce el salto posterior: el atacante no debería poder pivotar desde el servidor publicado hacia estaciones, hipervisores o administración.

99.4. Split DNS y hairpin

Los usuarios internos resuelven portal.ejemplo.es hacia la dirección interna apropiada mediante split DNS. Esto evita depender de NAT reflection cuando la arquitectura DNS puede resolver el problema de forma limpia.

99.5. Pruebas

Prueba	Resultado
Internet → portal 443	PASS
Internet → portal SSH	BLOCK
Portal → API 8443	PASS
Portal → DB	BLOCK
Portal → USERS	BLOCK
MGMT → portal SSH/administración	PASS según política
USERS → nombre portal	Resuelve hacia ruta interna prevista

Capítulo 100. Laboratorio integral: empresa multisede

Una organización con dos sedes necesita mucho más que un túnel. Debe decidir qué redes se anuncian, cómo se resuelve DNS, qué ocurre si cambia la WAN, cómo se monitoriza el túnel y qué servicios pueden cruzarlo.

100.1. Topología

Sede A	Sede B
USERS 10.20.0.0/24	USERS 10.80.0.0/24
SERVERS 10.30.0.0/24	SERVERS 10.90.0.0/24
MGMT 10.10.0.0/24	MGMT 10.70.0.0/24
WAN1 + WAN2	WAN1
DNS/AD principal	DNS/AD secundario o réplica según diseño

100.2. VPN y rutas

Puede utilizarse IPsec VTI, WireGuard o un diseño OpenVPN site-to-site. El laboratorio se centra en el resultado: rutas coherentes, retorno simétrico y política por redes. La elección concreta se realiza con los criterios de la Parte VII.

100.3. DNS entre sedes

El nombre de un servidor remoto debe resolver hacia una dirección alcanzable por VPN. Los resolvers/AD deben conocer las zonas necesarias y el firewall debe permitir ese flujo. “La VPN levanta” no valida DNS.

100.4. Fallo de WAN principal

Si la sede A tiene Multi-WAN, el diseño define si la VPN debe reestablecerse por WAN2. Se prueban endpoint, Dynamic DNS si existe, rutas y estados. La conmutación de Internet y la conmutación del túnel son problemas relacionados, pero no idénticos.

100.5. Aplicación central

```
PC sede B → DNS local → nombre ERP
        ↓
   ruta VPN a 10.30.0.20
        ↓
  firewall B → túnel → firewall A
        ↓
    ERP 443
        ↑ ruta de retorno por VPN
```

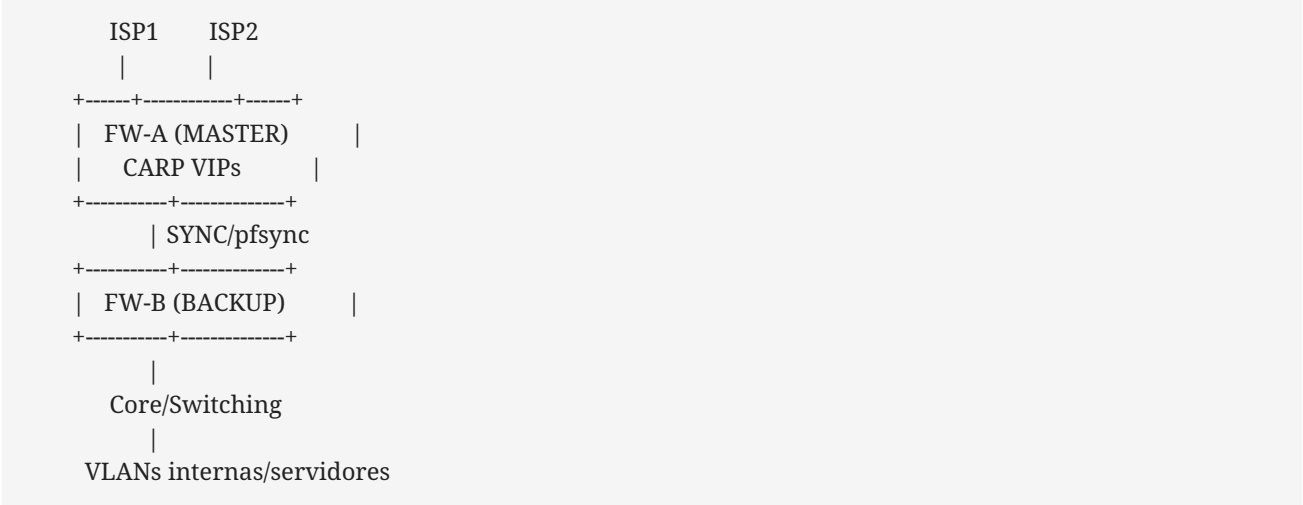
100.6. Pruebas de continuidad

Evento	Prueba
WAN1 A cae	ERP desde B vuelve a funcionar por ruta/túnel alternativo si el diseño lo contempla.
DNS principal no responde	Resolver secundario mantiene nombres críticos.
Túnel se reinicia	Monitor detecta caída y recuperación.
Nueva VLAN en B	No se considera operativa hasta incorporar routing, VPN y política.
Redes solapadas	El laboratorio debe detectarlo antes de desplegar, no después.

Capítulo 101. Laboratorio de continuidad: HA + Multi-WAN + fallo real

Este escenario combina dos firewalls, dos proveedores y una red SYNC. El objetivo no es presumir de redundancia, sino demostrar qué fallos soporta y cuáles siguen siendo puntos únicos.

101.1. Arquitectura



CARP aporta IP virtual, pfsync comparte estados y XMLRPC replica áreas compatibles de configuración. La red SYNC debe ser fiable y, preferiblemente, dedicada. La sincronización XMLRPC se configura solo desde el nodo primario.

101.2. Escenarios de fallo

Fallo	Qué debe ocurrir
ISP1	Tráfico elegible usa ISP2 según Gateway Group.
FW-A apagado	FW-B adopta VIP CARP.
SYNC interrumpido	Puede existir failover de VIP, pero estados no se sincronizan correctamente.
Switch único caído	Si solo existe uno, toda la HA del firewall resulta irrelevante.
Alimentación común	Ambos nodos pueden caer simultáneamente.
Error de configuración sincronizado	La redundancia replica el error; HA no es backup.

101.3. Prueba controlada de nodo

1. Abrir varias sesiones largas a través del clúster.
2. Registrar qué nodo es MASTER y el estado de pfsync.
3. Apagar o aislar FW-A de forma controlada.
4. Medir pérdida y tiempo de recuperación.
5. Comprobar continuidad de sesiones existentes.
6. Verificar que FW-B asume las VIP.
7. Recuperar FW-A y observar el comportamiento previsto de retorno/preemption.
8. Documentar la evidencia.

101.4. Prueba de error sincronizado

Se realiza en laboratorio, nunca improvisando en producción. Se introduce una modificación reversible que se sincroniza al secundario y se demuestra que HA no protege frente a una mala política. La conclusión es operativa: redundancia y backup resuelven problemas diferentes.

Idea esencial

Dos firewalls idénticos con una configuración equivocada proporcionan alta disponibilidad del error. La continuidad necesita redundancia, control de cambios y recuperación.

Capítulo 102. Recuperación: de config.xml a una reconstrucción completa

La recuperación debe ensayarse antes del desastre. pfSense concentra su configuración principal en config.xml y ofrece mecanismos locales y remotos de copia. Esto permite reconstruir un firewall con rapidez, pero únicamente si las copias, contraseñas y dependencias están disponibles.

102.1. Niveles de recuperación

Nivel	Ejemplo	Objetivo
Revertir cambio	Historial de configuración	Deshacer una modificación reciente.
Restaurar XML	Backup manual	Recuperar configuración en el mismo equipo.
AutoConfigBackup	Copia remota cifrada	Recuperar versiones off-site.
Reinstalar + restaurar	Disco averiado o sistema dañado	Reconstruir sistema base.
Migrar hardware	Equipo nuevo	Restaurar y reasignar interfaces si es necesario.

102.2. Copias manuales y ACB

AutoConfigBackup es un servicio remoto cifrado incluido para usuarios de pfSense Plus y CE. Puede crear copias ante cambios significativos o según una programación. La clave/dispositivo de cifrado y las credenciales necesarias deben formar parte del plan de recuperación.

No confundir

El historial local es cómodo, pero comparte destino físico con el firewall. Una estrategia de desastre necesita al menos una copia fuera del dispositivo.

102.3. Antes de una actualización

- Backup completo “All”.
- Copia segura en ubicación independiente.
- Acceso a consola o gestión fuera de banda.
- Medio/instalador disponible cuando sea razonable.
- Inventario de paquetes y funciones críticas.
- Ventana y criterio de rollback.
- Pruebas posteriores definidas antes de actualizar.

102.4. Prueba de reconstrucción

1. Crear una VM aislada o utilizar hardware de laboratorio.
2. Instalar una versión compatible.
3. Restaurar una copia completa.
4. Reasignar interfaces si los nombres han cambiado.
5. Mantener las NIC desconectadas de producción hasta revisar IP/VIP/HA.
6. Validar servicios, paquetes y certificados.
7. Conectar a redes de prueba y ejecutar la matriz de aceptación.

102.5. Editar config.xml: excepción, no rutina

La configuración XML puede editarse, pero un error de sintaxis o de estructura puede provocar consecuencias severas. Cuando sea imprescindible, el método más seguro es editar una copia y restaurarla, conservando siempre el original. La administración normal debe realizarse desde la GUI y herramientas soportadas.

Capítulo 103. Auditoría técnica de pfSense

Una auditoría útil no consiste en contar reglas. Debe encontrar exposición innecesaria, objetos obsoletos, dependencias no documentadas y diferencias entre la política declarada y el comportamiento real.

103.1. Inventario

Área	Preguntas
Interfaces/VLAN	¿Todas siguen en uso? ¿Existe descripción y propietario?
Reglas	¿Cada excepción tiene propósito? ¿Hay any/any heredados?
Aliases	¿Contienen IP antiguas o nombres ambiguos?
NAT	¿Se siguen publicando todos los servicios?
VPN	¿Peers/usuarios siguen autorizados?
Certificados	¿Caducan pronto? ¿Hay CRL y claves innecesarias?
Paquetes	¿Se utilizan y están actualizados?
Usuarios	¿Persisten cuentas compartidas o bajas?
Logs	¿Se conservan fuera del firewall cuando es necesario?
Backups	¿Se prueban y protegen?

103.2. Revisar desde WAN hacia dentro

Se comienza por la superficie externa: VIP, port forwards, servicios administrativos, VPN y cualquier paquete que escuche en WAN. Después se sigue cada publicación hasta el host interno y se confirma que el flujo sigue siendo necesario.

103.3. Revisar lateralidad interna

Una red segmentada puede degradarse con los años si cada necesidad se resuelve añadiendo excepciones amplias. La auditoría compara la matriz de flujos original con las reglas actuales y pregunta si cada nueva apertura podría limitarse por origen, destino, protocolo o identidad.

103.4. Auditoría de administración

- WebGUI accesible solo desde zonas autorizadas.
- SSH deshabilitado si no se utiliza; si se usa, limitado y autenticado de forma robusta.
- Usuarios nominales y privilegios mínimos.
- MFA donde la arquitectura de identidad lo permita.
- Certificado administrativo válido y gestión coherente de PKI.

- Consola y recuperación fuera de banda documentadas.

103.5. Evidencia de auditoría

Cada hallazgo debe expresar riesgo, evidencia, impacto, corrección propuesta, responsable y fecha. “Hay una regla any” es una observación; “GUEST puede alcanzar MGMT por any/any y abrir la WebGUI” es un hallazgo verificable.

Capítulo 104. Operación: cambios, actualizaciones y documentación viva

Un firewall que no cambia se queda obsoleto; uno que cambia sin disciplina se vuelve impredecible. La operación madura busca equilibrio: cambios pequeños, reversibles, documentados y comprobables.

104.1. Ciclo de cambio

```
Solicitud → análisis de impacto → backup → cambio → pruebas → observación → cierre
                                                  (rollback si falla)
```

104.2. Actualizaciones

Las actualizaciones requieren notas de versión, backup y consola disponible. En las versiones actuales, System Patches está instalado por defecto en pfSense Plus 26.03 y CE 2.9.0 o posteriores. Los parches recomendados pueden resolver problemas entre releases, pero el paquete en sí debe mantenerse actualizado para recibir nuevos parches.

104.3. Cambios de paquetes

Un paquete amplía funcionalidad y superficie. Antes de instalarlo se registra el propósito, dependencia, impacto de CPU/RAM/almacenamiento y procedimiento de retirada. Un paquete “por probar” no debería permanecer indefinidamente en producción.

104.4. Documentación viva

Documento	Debe contener
Mapa lógico	VLAN, subredes, gateways, VPN.
Matriz de flujos	Origen/destino/servicio/justificación.
Inventario	Hardware, interfaces, MAC, ISP, licencias/soporte.
Runbook	Reinicio, failover, recuperación, contactos.
Cambios	Fecha, motivo, responsable, pruebas.
Backups	Ubicaciones, cifrado, restauración probada.

104.5. Cadencia sugerida

La frecuencia real depende de criticidad, regulación y ritmo de cambio, pero el principio es estable: los objetos que expiran o cambian —certificados, cuentas, peers, reglas temporales, backups— necesitan revisiones programadas. Una revisión anual puede ser insuficiente para una red que cambia semanalmente.

Operación profesional

La documentación no debe describir el firewall ideal; debe describir el firewall que realmente existe y cómo recuperarlo.

Capítulo 105. Anexos rápidos de referencia

Estos anexos no sustituyen los capítulos. Funcionan como hojas de trabajo para operación, auditoría y diagnóstico. Pueden imprimirse o copiarse a la documentación interna de un entorno concreto.

105.1. Checklist de puesta en producción

Área	Comprobación
Hardware/VM	Recursos, NIC/vNIC y consola verificados.
Interfaces	WAN/LAN/VLAN etiquetadas y documentadas.
Direcciones	Sin solapamientos; gateways correctos.
DNS/NTP	Resolución y hora verificadas.
Reglas	Mínimo privilegio y pruebas negativas.
NAT	Solo traducciones necesarias.
Administración	WebGUI/SSH limitados a zonas autorizadas.
VPN	Identidad, rutas, DNS y revocación probadas.
HA/Multi-WAN	Pruebas de caída realizadas si aplican.
Logs	Retención y syslog remoto según necesidad.
Backup	Copia externa reciente y restauración conocida.
Documentación	Mapa, flujos y rollback actualizados.

105.2. Hoja de diagnóstico de 60 segundos

1. ¿Hay enlace físico/virtual?
2. ¿La interfaz tiene la IP/prefijo esperados?
3. ¿ARP/NDP resuelve el siguiente salto?
4. ¿La tabla de rutas elige el camino correcto?
5. ¿El gateway/monitor está UP?
6. ¿PF permite o bloquea?
7. ¿Existe un estado anterior que cambie el resultado?
8. ¿NAT modifica el flujo como esperamos?
9. ¿DNS resuelve hacia la IP correcta?
10. ¿El servicio destino escucha y responde?

105.3. Matriz de flujo reutilizable

ID	Origen	Destino	Servicio	Acción	Justificación	Log
F-001	USERS	ERP	TCP 443	PASS	Aplicación corporativa	Sí
F-002	GUEST	RFC1918	Any	BLOCK	Aislamiento invitados	Solo bloqueos
F-003	MGMT	pfSense	HTTPS	PASS	Gestión	Sí

105.4. Plantilla de regla temporal

- Propietario de la solicitud.
- Motivo y ticket/cambio asociado.
- Origen y destino más específicos posibles.
- Puerto/protocolo exactos.
- Fecha de expiración.
- Prueba de retirada programada.

105.5. Checklist de VPN

Plano	Validación
Underlay	Endpoint alcanzable; DNS/puerto/NAT upstream correctos.
Identidad	Certificado/clave/usuario válidos y revocables.
Negociación	Handshake/SA estable.
Routing	Prefijos y retorno por túnel.
Firewall	Tráfico interior autorizado por mínimo privilegio.
DNS	Nombres internos resolubles si son necesarios.
MTU	Sin síntomas de fragmentación/PMTUD.
Operación	Logs, monitorización y procedimiento de baja.

105.6. Checklist HA

Elemento	Validación
CARP	VIP y estados MASTER/BACKUP correctos.
pfsync	Estados sincronizados por SYNC.

Elemento	Validación
XMLRPC	Solo primario sincroniza configuración.
Interfaces	Asignaciones y orden coherentes.
NAT	Traducciones utilizan VIP cuando corresponde.
Switching	No existe un único punto de fallo no previsto.
Energía	Fuentes/UPS distribuidas según criticidad.
Prueba	Failover real medido y documentado.

105.7. Mapa mental final

```
PAQUETE
  ↓
INTERFAZ → DIRECCIÓN → RUTA/GATEWAY
  ↓
PF / ESTADO
  ↓
NAT (si aplica)
  ↓
VPN / SERVICIO / INTERNET
  ↓
RETORNO

Alrededor del flujo:
DNS · DHCP · NTP · LOGS · HA · BACKUP · MONITORIZACIÓN · IDENTIDAD
```

Cierre conceptual

Aprender pfSense no consiste en aprender una WebGUI. Consiste en entender redes, estados, rutas, traducciones, servicios, identidad y recuperación; pfSense es la plataforma donde todas esas decisiones se encuentran.

Fuentes técnicas de contraste

Las siguientes fuentes oficiales se han utilizado para verificar mecanismos de recuperación, alta disponibilidad y mantenimiento vigentes en octubre de 2026.

- **Automatic Configuration Backup Service:** https://docs.netgate.com/pfsense/en/latest/backup/acb.html
- **Backup and Recovery / pre-upgrade tasks:** https://docs.netgate.com/pfsense/en/latest/install/upgrade-guide-prepare.html
- **XML Configuration File:** https://docs.netgate.com/pfsense/en/latest/config/xml-configuration-file.html

- **High Availability Configuration Example:** https://docs.netgate.com/pfsense/en/latest/recipes/high-availability.html
- **State Synchronization (pfsync):** https://docs.netgate.com/pfsense/en/latest/highavailability/pfsync.html
- **HA Synchronization Settings:** https://docs.netgate.com/pfsense/en/latest/highavailability/settings.html
- **Troubleshooting High Availability:** https://docs.netgate.com/pfsense/en/latest/troubleshooting/high-availability.html
- **System Patches Package:** https://docs.netgate.com/pfsense/en/latest/development/system-patches.html
- **pfSense Plus 26.03 release notes:** https://docs.netgate.com/pfsense/en/latest/releases/26-03.html
- **Diagnostics overview:** https://docs.netgate.com/pfsense/en/latest/menuguide/diagnostics.html

Cierre de la Parte XII

Con esta Parte XII concluye el recorrido principal de la obra. El objetivo final no es que el lector memorice una interfaz, sino que pueda diseñar, operar, proteger y diagnosticar una arquitectura de red con criterio. Las versiones de pfSense evolucionarán; los modelos mentales, las pruebas y la metodología de diagnóstico desarrollados a lo largo del libro están concebidos para seguir siendo útiles más allá de una pantalla concreta.

Bibliografía y referencias técnicas consolidadas

Esta bibliografía reúne las fuentes marco utilizadas para contrastar la obra. Las referencias específicas de cada tema se conservan al final de la parte correspondiente. La consulta de estas fuentes no implica reproducción de su estructura, redacción, capturas o material gráfico.

pfSense® software, Netgate® y documentación primaria

- **Documentación de pfSense® software:** https://docs.netgate.com/pfsense/en/latest/
- **Versiones de pfSense software y FreeBSD:** https://docs.netgate.com/pfsense/en/latest/releases/versions.html
- **Instalación y actualización:** https://docs.netgate.com/pfsense/en/latest/install/
- **Netgate Installer:** https://docs.netgate.com/pfsense/en/latest/install/netinstaller.html
- **Firewall:** https://docs.netgate.com/pfsense/en/latest/firewall/
- **NAT:** https://docs.netgate.com/pfsense/en/latest/nat/
- **Routing:** https://docs.netgate.com/pfsense/en/latest/routing/
- **Servicios DHCP:** https://docs.netgate.com/pfsense/en/latest/services/dhcp/
- **DNS:** https://docs.netgate.com/pfsense/en/latest/services/dns/
- **Selección de VPN:** https://docs.netgate.com/pfsense/en/latest/vpn/selection.html
- **Multi-WAN:** https://docs.netgate.com/pfsense/en/latest/multiwan/
- **Alta disponibilidad:** https://docs.netgate.com/pfsense/en/latest/highavailability/
- **Monitorización:** https://docs.netgate.com/pfsense/en/latest/monitoring/
- **Virtualización:** https://docs.netgate.com/pfsense/en/latest/virtualization/
- **Paquetes:** https://docs.netgate.com/pfsense/en/latest/packages/
- **Licencias de componentes:** https://docs.netgate.com/pfsense/en/latest/licensing/
- **Política de marcas de Netgate:** https://www.netgate.com/company/legal/trademarks

FreeBSD

- **FreeBSD Handbook:** https://docs.freebsd.org/en/books/handbook/
- **Network — FreeBSD Handbook:** https://docs.freebsd.org/en/books/handbook/network/
- **Advanced Networking — FreeBSD Handbook:** https://docs.freebsd.org/en/books/handbook/advanced-networking/

Estándares de Internet

- **RFC Editor — repositorio oficial de RFC:** https://www.rfc-editor.org/
- **RFC Index:** https://www.rfc-editor.org/rfc-index/

VPN y seguridad

- **WireGuard — Quick Start:** https://www.wireguard.com/quickstart/
- **WireGuard — Protocol & Cryptography:** https://www.wireguard.com/protocol/
- **OpenVPN Community Documentation:** https://openvpn.net/community-docs/
- **OpenVPN 2.7 Manual:** https://openvpn.net/community-docs/community-articles/openvpn-2-7-manual.html
- **Suricata User Guide:** https://docs.suricata.io/en/suricata-8.0.7/
- **Snort 3 — documentación y descargas:** https://snort.org/snort3

Fecha general de consulta técnica: 8 de octubre de 2026. Para una reedición deben revisarse especialmente las páginas de versiones, licencias, marcas, soporte y funciones exclusivas de edición.

Diagnóstico rápido: del síntoma a la evidencia

Guía de orientación. Antes de cambiar nada, confirma impacto y acceso de recuperación.

1 · No hay conectividad

Comprueba enlace, IP, máscara/prefijo, gateway y ruta de retorno. Después revisa los estados y las reglas.

Capítulos 18 / 23 / 31 / 80

2 · Resuelve mal los nombres

Separa fallo DNS de fallo IP. Comprueba el resolver, consultas, interfaces y servidores de destino.

Capítulos 40 / 41 / 45

3 · El NAT o Port Forward no funciona

Identifica interfaz de entrada, traducción, regla de paso, destino real y respuesta de vuelta.

Capítulos 32 / 33 / 35

4 · La VPN conecta, pero no pasa tráfico

Verifica direcciones de túnel, rutas, políticas, DNS y filtrado en ambos extremos.

Capítulos 49 / 50 / 51 / 55

5 · Falla la alta disponibilidad o Multi-WAN

Distingue caída del gateway, failover, VIP, estados, NAT y asimetría de las rutas.

Capítulos 66 / 68 / 71 / 75

6 · Una incidencia sigue sin explicación

Recoge logs y captura en el punto correcto; formula una hipótesis y cambia una variable cada vez.

Capítulos 77 / 79 / 83 / 85

Método transversal: síntomas → alcance → evidencias → hipótesis → cambio único → comprobación.

Conceptos y capítulos de referencia · 1/2

Las páginas enlazan al inicio del capítulo relacionado; pueden contener más referencias en el texto.

Aliases
Pág. 123

Alta disponibilidad
Pág. 219, 231, 292

Backups y restauración
Pág. 83, 294

Bridges y LAGG
Pág. 107

CARP
Pág. 228

Certificados y PKI
Pág. 170

CLI y pfctl
Pág. 249

Conectividad y diagnóstico
Pág. 87, 247, 255

DHCP
Pág. 143

DHCP Relay
Pág. 148

DHCPv6 y SLAAC
Pág. 149

DMZ y publicación
Pág. 288

DNS interno
Pág. 151, 153

DNSBL y pfBlockerNG
Pág. 204

Dynamic DNS
Pág. 155

Egress filtering
Pág. 206

Firewall con estado
Pág. 117

Floating Rules
Pág. 121

FreeBSD y PF
Pág. 28

Gateway Groups
Pág. 223

Hardening
Pág. 195

Hardware Netgate
Pág. 31, 45

Hipervisor y perímetro
Pág. 273

Hyper-V
Pág. 270

IDS/IPS
Pág. 197, 202

IPsec
Pág. 178

IPv4 y subnetting
Pág. 94

IPv6
Pág. 97, 149

Kea DHCP
Pág. 146

LDAP y RADIUS
Pág. 180

Conceptos y capítulos de referencia · 2/2

Las páginas enlazan al inicio del capítulo relacionado; pueden contener más referencias en el texto.

Logs y auditoría
Pág. 241, 296

Monitorización
Pág. 239, 251

MTU
Pág. 107

Multi-WAN
Pág. 219, 227

NAT
Pág. 127

NAT 1:1 y Outbound
Pág. 131

NTP
Pág. 155

OpenVPN
Pág. 176

Packet capture y tcpdump
Pág. 245

PCI passthrough y SR-IOV
Pág. 268

pfInfo y pfTop
Pág. 243

pfsync
Pág. 229

Policy routing
Pág. 225

Port Forward
Pág. 129

Proxmox VE
Pág. 266

Recuperación desde config.xml
Pág. 294

Redes multisede
Pág. 290

Reglas de firewall
Pág. 119, 121

Rendimiento
Pág. 251, 271

Routing y gateways
Pág. 102

Segmentación y VLAN
Pág. 104, 206

Snort
Pág. 201

Suricata
Pág. 199

Trazas y evidencias
Pág. 245, 257

VMware / ESXi
Pág. 269

VPN sitio a sitio
Pág. 182

VPN y acceso remoto
Pág. 168, 180

WireGuard
Pág. 174

XMLRPC
Pág. 230

Nota de edición, fuentes y erratas

Cómo citar, comprobar versiones y proponer correcciones al autor.

Identificación de esta edición

Oscar de la Cuesta Campillo. pfSense® software: Redes, Firewall y Seguridad. Primera edición, octubre de 2026. Publicación técnica independiente.

Uso y licencia

La aportación editorial original se distribuye con licencia CC BY-NC-ND 4.0: atribución obligatoria, uso no comercial y sin distribución de adaptaciones. La copia de pequeños comandos y configuraciones de laboratorio se permite según los créditos del libro.

Versiones y vigencia

Las referencias de pfSense CE, pfSense Plus, paquetes, dispositivos Netgate y capturas corresponden al estado de consulta indicado en el libro. Para aplicar procedimientos, comprueba siempre la documentación de tu versión. La existencia de un manual para un modelo no garantiza su disponibilidad comercial.

Comunicación de erratas

Para remitir errores, matices o ejemplos reproducibles, contacta con el autor mediante palentino.es. Identifica la página, el capítulo, la versión afectada y el comportamiento observado. Consulta el blog para nuevas publicaciones y posibles revisiones; no se presupone un registro de erratas público ya creado.

palentino.es/blog

Licencia oficial CC BY-NC-ND 4.0

Criterio editorial

Mi propósito es enseñar a decidir y verificar, no limitar el aprendizaje a los menús de una versión concreta. Las ilustraciones de hardware son esquemáticas y deben contrastarse con las fotografías y fichas oficiales.

Créditos gráficos y alcance de las ilustraciones

Las imágenes se han integrado durante la preparación editorial, en parte con técnicas de generación digital. Los equipos Netgate se representan de forma esquemática: no son fotografías oficiales ni planos exactos. Las marcas y los materiales de terceros quedan fuera de la licencia de esta obra.

QUÉ ENCONTRARÁS EN ESTE LIBRO



UN RECORRIDO COMPLETO

Una guía técnica y práctica para comprender pfSense® software desde el diseño de redes hasta su operación diaria. Explica la arquitectura, las interfaces y el direccionamiento; profundiza en routing, VLAN, filtrado, NAT, DNS, DHCP, VPN y seguridad; y culmina con alta disponibilidad, monitorización, virtualización, diagnóstico y laboratorios reproducibles.

PRINCIPALES BLOQUES

- Fundamentos, hardware e instalación
- Direccionamiento, routing, VLAN y NAT
- Reglas, estados, servicios y VPN
- IDS/IPS y seguridad avanzada
- Multi-WAN y alta disponibilidad
- Monitorización y troubleshooting
- Virtualización y laboratorios prácticos

SOBRE EL AUTOR



Oscar de la Cuesta

Ingeniero Informático y Técnico Superior en Telecomunicaciones. Colegiado n.º 406 en el Ilustre Colegio Profesional de Ingenieros en Informática de Castilla y León (CPIICyL).

Más de 27 años de experiencia profesional en consultoría, metal, aeronáutica e industria agroalimentaria, con el foco en los objetivos, los plazos y la calidad de los resultados.

Gestiono y evoluciono tecnología, infraestructura, seguridad, sistemas, comunicaciones, automatización y continuidad, conectando la operativa IT con las necesidades del negocio. Busco soluciones sencillas, seguras, documentadas y sostenibles.

ALGUNOS HITOS Y PUBLICACIONES

- Primer Premio Internet 2005 · Trazagest · Junta de Castilla y León.
- Primer Premio Internet 2004 · Portal multimedia de la provincia de Soria.
- Otras publicaciones técnicas sobre Windows Server, Proxmox e infraestructura.

palentino.es · ctomanager.com

LICENCIA Y USO

CC BY-NC-ND 4.0. Se permite consultar y compartir gratis la obra original, completa o por partes, sin fines comerciales y con atribución. No se autoriza distribuir adaptaciones ni traducciones.
Los ejemplos breves de configuración pueden utilizarse y adaptarse en sistemas propios o autorizados.

CC BY NC ND

CC BY-NC-ND 4.0

VISITA MI BLOG

Publicación independiente · Oscar de la Cuesta · Primera edición: octubre de 2026