pfSense: The Definitive Guide

La guía definitiva para el Abierto de pfSense Fuente firewall y router de distribución

Christopher M. Buechler
Jim Pingle

pfSense: The Definitive Guide: La guía definitiva para el Abierto de pfSense Fuente firewall y router de distribución

por Christopher M. Buechler y Pingle Jim

Sobre la base de pfSense Versión 1.2.3

Fecha de publicación 2009

Resumen

La guía oficial para la distribución de pfSense abrir cortafuegos de origen.

Tabla de contenidos

Lista de figuras

Lista de cuadros

Prefacio

Mis amigos y compañeros de trabajo saben que voy a construir cortafuegos. Por lo menos una vez al mes alguien dice "Mi empresa necesita un servidor de seguridad con X e Y, y el precio citas que he recibido decenas de miles de dólares. ¿Nos puede ayudar a cabo? "

Cualquier persona que construye cortafuegos sabe esta pregunta podría ser más realista enunciado como "¿Podría usted por favor, venir una noche y bofetada a unos equipo para mí, entonces me dejó al azar se interrumpe durante los próximos tres a cinco años para tener que instalar nuevas características, los problemas de depuración, configurar las funciones Yo no sabía lo suficiente para solicitar, asistir a las reuniones para resolver los problemas que no puede posiblemente ser problemas de firewall, pero alguien piensa que puede ser el servidor de seguridad, y identificar soluciones para mis necesidades innumerables desconocidos? Ah, y asegúrese para probar cada caso de uso posible antes de implementar cualquier cosa. " Rechazar estas peticiones me hace parecer grosero. La aceptación de estas solicitudes ruinas de mi comportamiento alegre. Durante mucho tiempo, yo no construir cortafuegos, excepto para mi empleador.

pfSense me permite ser una persona más agradable sin tener que trabajar realmente en ello.

Con pfSense puedo implementar un servidor de seguridad en tan sólo unas horas - y la mayoría de que es la instalación de cables y explicar la diferencia entre "dentro" y

"Afuera". extensa documentación pfSense y comunidad de usuarios me ofrece una respuesta fácil a las preguntas - "¿Has mirado eso?" Si pfSense no admite una característica, lo más probable es que no podía apoyar bien. Pero pfSense apoya todo lo que podía pedir, y con una interfaz amigable para arrancar. La gama base de usuarios significa que las características son probados en diferentes ambientes y en general, "sólo trabajo", aun cuando interactúan con Windows hijos del CEO ME PC conectado a Internet por Ethernet sobre ATM a través de palomas mensajeras. Lo mejor de todo, pfSense se basa en gran parte del software mismo me había uso. Confío el sistema operativo FreeBSD subyacentes para ser seguro, estable y eficiente. Actualizaciones de seguridad? Basta con hacer clic en un botón y reiniciar el sistema.

Su necesidad de nuevas características? Sólo tienes que activar. pfSense maneja la agrupación, el tráfico la formación, el equilibrio de carga, la integración con su equipo existente a través de RADIUS, IPSec, PPTP, el seguimiento, DNS dinámico, y más.

proveedores de renombre de la industria de carga honorarios indignantes para apoyar lo que pfSense proporciona libremente. Si su empleador insiste en pagar por contratos de apoyo, o si simplemente te sientes más seguro sabiendo que puede levantar el teléfono y el grito de ayuda, usted puede conseguir acuerdos pfSense apoyo muy razonable. Si usted no necesidad de un contrato de soporte, me he enterado de que Chris, Jim, o cualquier otra persona con pfSense cometer un poco dejará agradecido pfSense usuarios a comprar una cerveza o seis. Personalmente, no construyen cortafuegos de la nada más. Cuando necesito un firewall, yo uso pfSense.

-Michael Lucas W.

Prólogo

Bienvenido a la guía definitiva de pfSense. Escrito por pfSense Buechler cofundador Chris pfSense y consultor Jim Pingle, este libro cubre la instalación y configuración básica a través de redes avanzadas y cortafuegos con el firewall de fuente abierta popular y el router de distribución.

Este libro está diseñado para ser un amistoso guía paso-a-paso para la creación de redes y de seguridad común tareas, además de una referencia completa de las capacidades de pfSense. La guía definitiva para pfSense cubre los siguientes temas:

- Una introducción a pfSense y sus características.
- Hardware y planificación del sistema.
- Instalación y actualización pfSense.
- Utilizar la interfaz de configuración basada en web.
- Copia de seguridad y restauración.
- Cortafuegos fundamentos y las normas de la definición y solución de problemas.
- El reenvío de puertos y traducción de direcciones de red.
- General de redes y configuración de enrutamiento.
- Reducir, LAN virtuales (VLAN), y Multi-WAN.
- Redes privadas virtuales con IPSec, PPTP, y OpenVPN.
- Control del tráfico y balanceo de carga.
- Redes inalámbricas y cautivos configuraciones del portal.
- servidores de seguridad redundantes y de alta disponibilidad.
- Servicios relacionados con la red de Varios.
- Sistema de monitoreo, registro, análisis de tráfico, aspirados, captura de paquetes, y solución de problemas.
- Paquetes de software y las instalaciones de software de terceros y actualizaciones.

Al final de este libro, usted encontrará una guía de menú con las opciones del menú estándar disponibles en pfSense y un índice detallado.

1. Autores

1.1. Chris Buechler

Chris es uno de los fundadores del proyecto pfSense, y uno de sus promotores más activos.

Él ha estado trabajando en la industria de TI durante más de una década, trabajando extensamente con los cortafuegos y FreeBSD para la mayoría de ese tiempo. Él ha proporcionado seguridad, red y servicios relacionados para las organizaciones en el sector público y privado, que van desde pequeñas organizaciones de Fortune 500 empresas y grandes organizaciones del sector público. Actualmente se gana la vida ayudando a organizaciones con necesidades relacionadas con pfSense incluyendo el diseño de redes, la planificación de implementación,
asistencia para la configuración, la conversión de los cortafuegos existentes, el desarrollo y mucho más. Él se basa en Louisville, Kentucky, EE.UU. y proporciona servicios a clientes de todo el mundo. Tiene numerosas certificaciones de la industria incluyendo el CISSP, SSCP, MCSE, CCNA y entre otros.
Su página web personal se puede encontrar en http://chrisbuechler.com.

1.2. Jim Pingle

Jim ha estado trabajando con FreeBSD desde hace más de diez años, profesional durante los últimos seis años.
En la actualidad como un administrador de sistemas de HPC Servicios de Internet, un ISP local en Bedford, New York, EE.UU. trabaja con los servidores de FreeBSD, diversos equipos de enrutamiento y circuitos, y por supuesto cortafuegos pfSense basado tanto a nivel interno y para muchos clientes. Jim tiene un título de licenciatura en Sistemas de Información de Indiana-Purdue Fort Wayne, y se graduó en 2002. También contribuye a varios proyectos de código abierto, además de pfSense, sobre todo RoundCube Webmail y glTail.
Cuando lejos de la computadora, Jim también le gusta pasar tiempo con su familia, leer, tomar imágenes, y ser un adicto a la televisión. Su página web personal se puede encontrar en http://pingle.org.

2. Agradecimientos

Este libro, y pfSense en sí misma no sería posible sin un gran equipo de desarrolladores, colaboradores, patrocinadores corporativos, y una comunidad maravillosa. El proyecto ha recibido el código contribuciones de más de 100 personas, con 29 personas que han contribuido considerablemente suficiente para obtener acceso de confirmación. Cientos de personas han contribuido financieramente, con el hardware, y otros recursos necesarios. Miles más han hecho su parte para apoyar el proyecto, ayudando a

otros en la lista de correo, foro, y el IRC. Nuestro agradecimiento a todos los que han hecho su parte para que el proyecto del gran éxito se ha convertido.

2.1. Libro de Diseño de Portada

Gracias a Holger Bauer para el diseño de la cubierta. Holger fue uno de los colaboradores primera
al proyecto, después de haber hecho gran parte del trabajo de tematización, gráficos, y es el creador de la
antecedentes que hemos utilizado en nuestras presentaciones a las seis conferencias BSD en los últimos cinco años.

2.2. Los desarrolladores pfSense

El actual equipo activo de desarrollo pfSense, enumerados por orden de antigüedad.

• Co-fundador Scott Ullrich

• Co-fundador Chris Buechler

• Proyecto de Ley de Marquette

• Bauer Holger

• Erik Kristensen

• Mos Seth

• Dale Scott

• Martin Fuchs

• Luci Ermal

• Los novios Mateo

• Grúa Marcos

• Zelaya Rob

• Renato Botelho

También nos gustaría dar las gracias a todos los desarrolladores de FreeBSD, y específicamente, los desarrolladores que han ayudado considerablemente con pfSense.

• Laier Max

• Christian S.J. Perón

• Andrew Thompson

Bjoern • A. Zeeb

2.3. Agradecimientos personales

2.3.1. De Chris

Debo dar mi agradecimiento esposa y de crédito importantes para la realización de este libro, y el éxito del proyecto en general. Este libro y el proyecto han llevado a un sinnúmero de días largos y noches y meses sin descanso de un día, y su apoyo ha sido crucial.

También me gustaría dar las gracias a las muchas empresas que han comprado nuestro apoyo y distribuidor suscripciones, lo que me permite dar el salto a trabajar a tiempo completo en el proyecto a principios de 2009.

También debo agradecer a Jim para saltar en este libro y ofrecer una ayuda considerable en la realización de que. Ya han pasado dos años en la fabricación, y trabajar mucho más de lo que había imaginado. Puede que haya sido obsoletos antes de que se termine, si no fuera por su ayuda durante los últimos meses. También gracias a Jeremy Reed, nuestro editor y el editor, por su ayuda con el libro.

Por último, mi agradecimiento a todos los que han contribuido al proyecto pfSense en cualquier forma, especialmente a los desarrolladores que han dado enormes cantidades de tiempo al proyecto durante los últimos cinco años.

2.3.2. De Jim

Me gustaría dar las gracias a mi esposa e hijo, que aguantarme a través de mi participación en el proceso de escritura. Sin ellos, habría vuelto loco hace mucho tiempo.

También me gustaría dar las gracias a mi jefe, Rick Yanez de HPC Servicios de internet, por ser de apoyo de pfSense, FreeBSD, y el software de código abierto en general.

La comunidad pfSense todo es digno de agradecimiento aún más así, es el mejor y más grupo de apoyo de los usuarios de software de código abierto y colaboradores que he encontrado.

2.4. Los revisores

Las siguientes personas proporcionaron información muy necesaria y los conocimientos para ayudar a mejorar el libro y su exactitud. Enumerados en orden alfabético por el apellido.

- Bruce Jon
- Mark Foster
- Irvine Bryan
- Midgley Warren
- Eirik Overby

3. Comentarios

El editor y autores animar a su opinión sobre este libro y la distribución de pfSense.

Por favor, envíe sus sugerencias, críticas y / o elogios por La guía definitiva para pfSense libro `<info@reedmedia.net>`. página web de la editorial para el libro está en http://www.reedmedia.net/books/pfsense/.

Para consultas generales relacionadas con el proyecto pfSense, por favor, escribir en el foro o lista de correo. Enlaces con estos recursos se pueden encontrar en http://pfsense.org/support.

4. Convenciones tipográficas

A lo largo del libro una serie de convenciones se utilizan para designar ciertos conceptos, información o acciones. La siguiente lista nos da ejemplos de cómo estos se formatean en el libro.

Selecciones de menú	Servidor de seguridad → Reglas
Interfaz gráfica de las etiquetas de artículos / Nombres	Destino
Botones	Aplicar cambios
Preguntar por la entrada	`¿Desea continuar?`
Entrada del usuario	**Regla Descripción**
Nombres de archivos	`/ Boot / loader.conf`
Los nombres de los comandos o programas	gzip
Comandos escritos en el intérprete de comandos	**#ls -l**
Los elementos que debe ser reemplazado por valores específicos a su configuración	*192.168.1.1*

Notas especiales

Nota

Cuidado con esto!

Largas colas literal en ejemplos de salida puede ser dividida con el (Hookleftarrow). Largo de shell ejemplos de línea de comandos se puede dividir utilizando la barra invertida (\) para la continuación de línea shell.

Capítulo 1. Introducción

pfSense es un gratuito, de código abierto de distribución personalizada de FreeBSD adaptado para su uso como un servidor de seguridad y el router, todo a un manejo fácil de usar interfaz web. Esta interfaz web, que se conoce como la GUI basado en web configurador, o WebGUI para abreviar. No se requieren conocimientos de FreeBSD se requiere de implementar y utilizar pfSense, y de hecho la mayoría de la base de usuarios nunca ha usado FreeBSD fuera de pfSense. Además de ser un sistema flexible de gran alcance, cortafuegos y plataforma de enrutamiento, que incluye una larga lista de características relacionadas y un sistema de paquetes que permite la capacidad de expansión más sin añadir hinchazón y las vulnerabilidades de seguridad potenciales para la distribución base. pfSense es un proyecto popular con más de 1 millón de descargas desde su creación, y probado en un sinnúmero de instalaciones que van desde pequeñas redes domésticas proteger un solo equipo a los grandes empresas, universidades y otras organizaciones de protección de miles de dispositivos de red.

1.1. Iniciación del Proyecto

Este proyecto fue fundado en 2004 por Chris Buechler y Ullrich Scott. Chris había sido contribuir a m0n0wall desde hace algún tiempo antes de eso, y encontró que es una gran solución. Sin embargo, al mismo tiempo emocionados con el proyecto, muchos usuarios anhelaba más capacidades que pueden tener cabida en un proyecto estrictamente enfocado hacia dispositivos integrados y su limitada los recursos de hardware. Introduzca pfSense. hardware moderno integrado también está bien apoyado y popular hoy pfSense. En 2004, hubo numerosas soluciones integradas con 64 MB RAM que no podía ponerse en práctica con la función deseada conjunto de pfSense.

1.2. ¿Qué significa para pfSense / media?

El proyecto duró un par de meses sin nombre. De hecho, la cárcel de FreeBSD que se ejecuta nuestro CVS servidor se sigue llamando `ProjectX`.

Scott y Chris eran los dos únicos miembros del proyecto en el tiempo, como sus fundadores. Corrimos a través de numerosas posibilidades, con la dificultad principal que encontrar algo con el dominio nombres disponibles. Scott llegó con pfSense, pf es el software de filtrado de paquetes utilizados, como en dar sentido a la PF. la respuesta de Chris fue menos que entusiasta. Pero después de un par de semanas con ninguna opción mejor, nos fuimos con él. Se llegó a decir: "Bueno, siempre podemos cambiarlo."

Desde entonces, un cambio de nombre fue considerado entre los desarrolladores, sin ganar ninguna de tracción como la mayoría de la gente era indiferente, y nadie sintió una necesidad imperiosa para el cambio. A mediados de 2007, un debate de nombres fue iniciado por una entrada de blog, y la abrumadora respuesta de la comunidad a través de comentarios e-mail y el blog fue "mantener el nombre!"

1.3. ¿Por qué FreeBSD?

Dado que muchos de los componentes principales en pfSense proceden de OpenBSD, usted puede preguntarse por qué eligió FreeBSD en lugar de OpenBSD. Hubo muchos factores en cuenta a la hora elegir un sistema operativo para este proyecto. Esta sección describe las principales razones para la elección de FreeBSD.

1.3.1. Soporte inalámbrico

Sabíamos soporte inalámbrico sería un elemento clave para muchos usuarios. En el momento este proyecto fue fundada en 2004, soporte inalámbrico de OpenBSD fue muy limitada. Su compatibilidad con el controlador era mucho más limitado que el de FreeBSD, y no tenía soporte para cosas importantes, tales como WPA (Wi-Fi Protected Access) y WPA2 con ningún plan de alguna aplicación de dicho apoyo en el momento. Algunos esto ha cambiado desde 2004, pero sigue adelante en FreeBSD capacidades inalámbricas.

1.3.2. Rendimiento de la red

el rendimiento de la red de FreeBSD es significativamente mejor que la de OpenBSD. Para pequeñas y medianas implementaciones de empresas, por regla general, no es de ninguna preocupación, como la escalabilidad superior es el principal problema en OpenBSD. Uno de los desarrolladores de pfSense gestiona varios cientos de servidores de seguridad de OpenBSD PF, y ha tenido que cambiar sus sistemas de alta carga más para los sistemas FreeBSD PF para manejar la alta paquetes por segundo necesarios en porciones de su red. Esto se ha convertido en un problema menor en OpenBSD desde 2004, pero sigue siendo válida.

1.3.3. La familiaridad y la facilidad de tenedor

Desde la base de código pfSense partió de m0n0wall, que se basa en FreeBSD, que era más fácil quedarse con FreeBSD. Cambiar el sistema operativo sería necesario modificar casi cada parte del sistema. Scott y Chris, los fundadores, también están más familiarizados con FreeBSD y había trabajado anteriormente juntos en un ahora-difunto solución comercial de firewall basado en FreeBSD. Esto en sí mismo no era una razón de peso, pero combinado con los últimos dos factores que era sólo otra cosa nos apuntan en esta dirección.

1.3.4. Alternativas de Apoyo al Sistema Operativo

En este momento, no hay planes para apoyar a cualquier otro sistema operativo, simplemente por razones de limitaciones de recursos. Sería un esfuerzo considerable al puerto a cualquiera de los otros BSD ya que se basan en algunas funciones que sólo están disponibles en FreeBSD, que tendría que ser completamente rediseñado.

1.4. Común de implementaciones

pfSense se utiliza en casi todos los tipos y tamaños de entorno de red imaginables, y es casi ciertamente adecuado para su red si contiene un ordenador, o miles. En esta sección se esbozarán las implementaciones más comunes.

1.4.1. Servidor de seguridad de perímetro

La implementación más común de pfSense es como un servidor de seguridad perimetral, con una conexión a Internet conectado a la WAN y la red interna de la LAN.

pfSense tiene capacidad para redes con necesidades más complejas, tales como Internet de múltiples conexiones múltiples redes LAN, DMZ múltiples redes, etc

Algunos usuarios también se suman BGP (Border Gateway Protocol) para proporcionar capacidades de conexión redundancia y balanceo de carga. Esto se describe más en Capítulo 8, Enrutamiento.

1.4.2. LAN o WAN del router

El segundo despliegue más común de pfSense es como una LAN o WAN del router. Se trata de un independiente papel del servidor de seguridad perimetral en las medianas a grandes redes, y se puede integrar en el perímetro de servidor de seguridad en entornos más pequeños.

1.4.2.1. LAN del router

En redes más grandes que utilizan varios segmentos de red interna, pfSense es una solución probada para conectar estos segmentos internos. Esto es más comúnmente implementados a través del uso de las VLAN 802.1Q con concentración de enlaces, que serán descritos en Capítulo 10, LAN virtuales (VLAN). Múltiples interfaces Ethernet se utiliza también en algunos entornos.

Nota

En entornos que requieren más de 3 Gbps de rendimiento sostenido, o más de 500.000 paquetes por segundo, sin router basado en hardware ofrece un rendimiento adecuado. Tales ambientes necesidad de desplegar conmutadores de nivel 3 (routing hecho en el hardware por el interruptor) o routers de gama alta basados en ASIC. Como los productos básicos aumentos en el rendimiento de hardware y sistemas operativos de propósito general como FreeBSD mejorar las capacidades de procesamiento de paquetes en línea con lo que el nuevo hardware capacidades pueden apoyar, escalabilidad seguirá mejorando con el tiempo.

1.4.2.2. WAN del router

Para la prestación de servicios WAN de un puerto Ethernet para el cliente, pfSense es una gran solución para privado routers WAN. Ofrece todas las funcionalidades mayoría de las redes requieren y en un mucho menor precio punto de que las ofertas de nombre comercial grande.

1.4.3. Punto de acceso inalámbrico

pfSense implementar Muchos estrictamente como un punto de acceso inalámbrico. capacidades inalámbricas también se pueden añadir a cualquiera de los otros tipos de despliegues.

1.4.4. Aparatos de uso especial

pfSense implementar muchos como un aparato de efectos especiales. Los siguientes son cuatro los escenarios que conocemos de, y no está seguro de que muchos casos similares que no son conscientes. La mayoría de cualquiera de las funciones de pfSense se puede utilizar en una implementación en dispositivos tipo. Usted puede encontrar algo único a el entorno donde este tipo de despliegue es un gran ajuste. Como el proyecto ha madurado, no Se ha prestado considerable atención en el uso como un marco de creación de equipo, especialmente en el La versión 2.0. Algunos aparatos especiales estarán disponibles en el futuro.

1.4.4.1. VPN

Algunos usuarios de la caída de pfSense como VPN detrás de un cortafuegos existente, para agregar VPN capacidades, sin crear ninguna interrupción en la infraestructura de servidor de seguridad existentes. La mayoría de pfSense implementaciones VPN también actuar como un servidor de seguridad perimetral, pero este es un mejor ajuste en algunas circunstancias.

1.4.4.2. DNS Server Appliance

pfSense ofrece un DNS (Domain Name System), paquete de servidor basado en tinydns, un pequeño, rápido, DNS servidor seguro. No está cargado de funciones, por lo que no es capaz de ser utilizado para ciertos fines, tales como Microsoft Active Directory, pero es un gran ajuste para alojamiento DNS públicos de Internet. Recuerde que la DNS charla vulnerabilidad en julio de 2008? Daniel J. Bernstein, autor de tinydns, se le atribuye con la idea original y la aplicación de los puertos de origen al azar en la resolución de DNS, el Resolución a que la vulnerabilidad. De hecho, tinydns fue el único servidor DNS principal que no necesitan ser parcheados en julio de 2008. Ha utilizado los puertos aleatorios de origen desde su creación. Varios Hace años, Bernstein incluso poner USD $ 1000 de su propio dinero en la línea para la primera persona para encontrar una escalada de privilegios agujero de seguridad. Que no ha sido reclamada. Si usted está recibiendo sólo pública DNS de Internet, tinydns debe considerarse seriamente. El paquete de pfSense también añade conmutación por error

capacidades.

1.4.4.3. Sniffer electrodomésticos

Un usuario estaba buscando un aparato rastreador de desplegar a un número de sucursales. aparatos comerciales sniffer están disponibles con numerosas campanas y silbidos, pero a un muy coste significativo, especialmente cuando se multiplica por un número de sucursales. pfSense ofrece una web interfaz para tcpdump que permite la descarga del archivo pcap que resulta cuando la captura ha terminado. Esto permite a esta empresa para capturar paquetes sobre una red de sucursales, descargue el resultante archivo de captura, y abrirlo en Wireshark [http://www.wireshark.org] Para el análisis.

pfSense no es tan elegante como aparatos rastreadores comercial, pero ofrece una funcionalidad adecuada para muchos fines, a un costo mucho más bajo.

Para obtener más información sobre cómo utilizar las características de la captura de paquetes de pfSense, consulte

Capítulo 25, Paquete Captura.

1.4.4.4. DHCP Server Appliance

Una despliega usuario instala pfSense estrictamente como DHCP (Dynamic Host Configuration Protocol) servidores para distribuir las direcciones IP para su red. En la mayoría de entornos de esto probablemente no tiene mucho sentido. Pero en este caso, el personal de los usuarios ya están familiarizados y cómodos con pfSense y este despliegue permitió seguir sin una formación adicional para los administradores, que fue una consideración importante en este despliegue.

1.5. Versiones

Esta sección describe los pfSense diferentes versiones disponibles actualmente y en el pasado.

1.5.1. 1.2.3 Publicación

Esta es la versión recomendada para todas las instalaciones en el momento de escribir este artículo. Es un hecho ampliamente probado y desplegado, y porque es la última versión 1.2.x es la única publicación que recibir comunicados de corrección de errores y cualquier versión de seguridad necesario fijar en 1.2.x en el futuro. El 1.2.3 liberación prevista una serie de correcciones de errores y mejoras de la 1.2.2, y actualizó la base de sistema operativo FreeBSD 7.2. Usted puede encontrar la versión actual recomendado por la navegación a www.pfsense.org/versiones [http://www.pfsense.org/versions]. Las referencias en este libro a 1.2 en su mayoría incluyen todos los versión 1.2.x, aunque algunas cosas que se mencionan en este libro sólo existen en 1.2.3 y versiones posteriores.

1.5.2. 1.2, 1.2.1, 1.2.2 Emisiones

1.2 fue la primera versión estable en la línea 1.2 de nuevos productos, y se puso a disposición de febrero 25, 2008. La actualización 1.2.1 proporciona una serie de correcciones de errores y algunos parches de seguridad de menor importancia, y
actualizó la base de sistema operativo FreeBSD 7.0. La versión 1.2.2 añade algunas correcciones de errores.

1.5.3. 1.0 Release

Esta fue la primera versión de pfSense clasificada como estable. Fue lanzado el 4 de octubre de 2006, con un seguimiento 1.0.1 versión de revisión de errores el 20 de octubre de 2006. Aunque sabemos aún de instalaciones la ejecución de algunas versiones alpha temprana y un sinnúmero de sitios aún en marcha 1.0, ya no se admite y recomendamos encarecidamente a todos los usuarios actualizar a 1.2.3. 1.0.1 contiene la seguridad de varios menores vulnerabilidades fijas, ya sea en 1.2 o 1.2.1.

1.5.4. Instantánea de prensa

El servidor de instantáneas pfSense construye una nueva imagen a partir del código actualmente en nuestro código fuente repositorio cada dos horas. Estos son principalmente para los desarrolladores y usuarios que prueben las correcciones de errores en
la solicitud de un desarrollador. Las instantáneas no siempre pueden estar disponibles, dependiendo del punto en el ciclo de liberación. Poco después de la versión 1.2, las instantáneas fueron tomadas en línea como la construcción de la infraestructura se ha actualizado para FreeBSD 7.0 y fue el 1.3 (en el momento, ahora 2.0) de liberación
preparado para los primeros lanzamientos a disposición del público. Situaciones similares pueden existir en el futuro. Usted puede ver lo que las instantáneas, en su caso, están disponibles visitando la instantánea del servidor [http://snapshots.pfsense.org].

1.5.5. 2.0 Publicación

La versión 2.0 de pfSense (antes conocido como 1.3) está disponible para las pruebas, y es el alfa calidad en el momento de escribir este artículo. Contiene numerosas mejoras significativas, muchas de las cuales todavía un trabajo en progreso. Una versión estable, o al menos la calidad de candidato de la versión de producción situación se espera a finales de 2009 o principios de 2010. Estará basado en FreeBSD 8.0, por lo que este programa depende un poco de calendario de lanzamiento de FreeBSD.

1.6. Plataformas

pfSense ofrece tres plataformas adecuadas para tres diferentes tipos de despliegues. En esta sección cubre cada uno, y los que debe elegir.

1.6.1. Live CD

La plataforma Live CD que permite ejecutar directamente desde el CD sin necesidad de instalar un disco duro o tarjeta Compact Flash. La configuración se puede guardar en un disquete o una unidad flash USB. La CD no es de acceso frecuente después del arranque ya que el sistema se ejecuta principalmente desde la RAM en ese momento, pero no debe ser eliminado de un sistema en funcionamiento. En la mayoría de los casos, esto sólo debería ser utiliza como una evaluación del software con el hardware en particular. Mucha gente lo utiliza mucho plazo, pero recomendamos el uso de instalaciones nuevas en su lugar. Los usuarios de Live CD no puede utilizar los paquetes, y la gráficos históricos de rendimiento se pierde al reiniciar.

1.6.2. Instalación completa

El CD en vivo incluye una opción de instalación para instalar pfSense en el disco duro en su sistema. Este es el método preferido de ejecución pfSense. Todo el disco duro debe ser sobreescrito; doble arrancando con otro sistema operativo no es compatible. instalaciones completas se recomienda para la mayoría de las implementaciones.
De las estadísticas de descarga que puede suponer al menos el 80% de todos los despliegues de pfSense se instala por completo.
La mayoría de los desarrolladores utilizan las instalaciones nuevas sobre todo si no del todo. Por lo tanto, es el más ampliamente probado mejor y con el apoyo de versión. No tiene por qué algunas de las limitaciones de las otras plataformas.

1.6.3. Embebido

La versión incorporada está diseñado específicamente para usarse con cualquier hardware usando Compact Flash (CF) en lugar de un disco duro. Las tarjetas CF pueden manejar solamente un número limitado de escrituras, por lo que el versión incorporada se ejecuta sólo lectura de CF, con lectura / escritura de sistemas de archivos como discos RAM. Incluso con esa limitación, son ampliamente compatibles con el hardware integrado y por medio de IDE a los convertidores-CF. Aunque las tarjetas CF son más pequeños que un conector de la unidad tradicional de disco duro ATA, el número de pines es los mismos y que sean compatibles. Esto hace que sea más fácil de implementar para los dispositivos que ya soporte IDE. CF siendo los medios de estado sólido, también no tienen la posible quiebra de un giro disco de qué preocuparse.
Los sistemas empotrados son muy populares por muchas razones, pero son los más convincentes que suelen tener pocas o ninguna las partes móviles, y consumen mucho menos energía y producen menos calor que los grandes sistemas al mismo tiempo un buen rendimiento suficiente para las necesidades de la mayoría de las redes. En este caso, menos partes móviles significa menos puntos de falla, menos calor, y se puede ejecutar en completo silencio.

Históricamente, se ha incorporado un ciudadano de segunda clase con pfSense, ya que las instalaciones nuevas se han el objetivo principal del proyecto. Esto ha cambiado con la nueva generación de integrados, basados en

en NanoBSD.

Una desventaja de los sistemas integrados es que algunos de los datos de gráficos históricos en RRDtool es perdido si el sistema no se cierra sin problemas. Por ejemplo, un corte de energía hará que algunos gráfico la pérdida de datos. Esto no afecta a la funcionalidad, sino que deja espacios en blanco en los gráficos históricos.

1.6.3.1. Antiguo incorporado (antes de la liberación 1.2.3)

Los paquetes no se admite en las versiones anteriores incrustado 1.2.2 y anteriores. Mayores incorporados actualizaciones también no siempre funcionan de forma fiable. El único 100% garantizado medio fiable de actualización se instala incorporado a la configuración de copia de seguridad, de re-flash de la FQ, y restaurar el de configuración. Estas limitaciones han sido eliminadas en la nueva configuración integrado.

1.6.3.2. NanoBSD incorporado

NanoBSD es una forma estándar de la construcción de FreeBSD en una manera amistosa incrustado. Es compatible con firmware dual, es fiable y ampliable. En el momento de escribir estas líneas, NanoBSD incrustado se completamente funcional y que se utilizan en la producción de algunos de nuestros desarrolladores. Habrá un 1.2.x liberación utilizando esta metodología integrado, momento en el que el antiguo incrustado será descontinuado. 2.0 sólo se utiliza la nueva metodología incrustado.

Además del apoyo de firmware múltiples que permite la conmutación entre dos instalaciones diferentes, esto aporta dos importantes beneficios adicionales. Los paquetes también contará con el apoyo, por las adecuadas para la un entorno integrado. También permite cruzar la creación de arquitecturas de hardware que no sea x 86, MIPS y con plataformas ARM potencialmente con el apoyo en el futuro.

1.7. Conceptos de Redes

Si bien esto no es un libro de introducción a la creación de redes, hay ciertos conceptos de red que son importantes para entender. Esta parte del libro no va a proporcionar una cobertura adecuada para los que carecen de conocimientos básicos de redes fundamentales. Si usted no posee este conocimiento, es probable que la necesidad de buscar material adicional de redes de introducción.

Los lectores con un conocimiento significativo de la propiedad intelectual público y privado que, subredes IP, CIDR notación CIDR y resumen puede saltar al siguiente capítulo.

1.7.1. Entender IP pública y privada Direcciones

Hay dos tipos de direcciones IP que se encuentran en la mayoría de redes - públicos y privados.

1.7.1.1. Direcciones IP privadas

Las direcciones IP privadas son las que dentro de una subred reservados, sólo para uso interno. La red estándar RFC 1918 [http://www.faqs.org/rfcs/rfc1918.html] Define subredes IP reservados para uso en redes privadas (Cuadro 1.1 ", RFC 1918 Espacio privado dirección IP"). En la mayoría de entornos, una subred IP privada de RFC 1918 es elegido y utilizado en todos los dispositivos de la red interna, que se conectan a Internet a través de un firewall o un router de aplicación de direcciones de red Traducción (NAT), como pfSense. NAT se explica más adelante en Capítulo 7, Red Traducción de direcciones.

CIDR Range	Intervalo de direcciones IP
10.0.0.0 / 8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

Tabla 1.1. RFC 1918 IP privada del espacio de direcciones

Hay otros rangos definidos como 1.0.0.0 / 8 y 2.0.0.0 / 8, pero éstos no están permanentemente reservados, como las direcciones RFC 1918. Aunque puede ser tentador utilizar estas, la probabilidad de que sean asignados a los aumentos reales, lugares enrutable como espacio IPv4 se hace más escasa. También debe evitar el uso de 169.254.0.0/16, que de acuerdo con RFC 3927 se reserva para "Link-Locales "configuración automática -, pero no debe ser asignada por DHCP o manualmente Hay más. de suficiente espacio de direcciones reservado por el RFC 1918, como se muestra en Tabla 1.1 ", RFC 1918 privadas Espacio de direcciones IP ", por lo que hay pocos incentivos para desviarse de esa lista. Nos hemos encontrado con redes con todo tipo de inadecuado direccionamiento, y conducirá a los problemas - no es un cuestión de "si", sino "cuando" los problemas se produzcan. Si usted se encuentra trabajando en una ya existente red mediante un espacio de dirección incorrecta, lo mejor es corregir el direccionamiento tan pronto como sea posible. Una lista completa de las redes IPv4 de uso especial se pueden encontrar en el RFC 3330.

1.7.1.2. Las direcciones IP públicas

Direcciones IP públicas son las asignadas por el ISP para todos, pero las redes más grandes. Redes que requieren cientos o miles de direcciones IP públicas suelen tener espacio de direcciones asignado directamente en el Registro Regional de Internet con su región del mundo. Regionales de Internet Los registros son las organizaciones que supervisan la asignación y registro de la dirección IP pública en su región designada por el mundo.

La mayoría de las conexiones a Internet residenciales cuentan con una única dirección IP pública, mientras que la mayoría de negocios conexiones de clase vienen con una opción de usar múltiples IPs públicas si es necesario. Un público único IP es adecuada en muchas circunstancias, y se puede utilizar en conjunto con NAT para conectar

cientos de direcciones privadas de sistemas a Internet. Contenido en este libro le ayudará a a determinar el número de IP pública de tu red requiere.

1.7.2. Subredes IP Conceptos

Al configurar el protocolo TCP / IP en un dispositivo, una máscara de subred debe ser especificado. Esta máscara permite al sistema determinar qué direcciones IP están en la red local, y que debe se llega por una pasarela en la tabla de enrutamiento del sistema. El valor por defecto de LAN IP 192.168.1.1 con una máscara de 255.255.255.0 o / 24 en notación CIDR, tiene una dirección de red 192.168.1.0/24. CIDR se explica en Sección 1.7.4, "Descripción de la notación CIDR Máscara de subred".

1.7.3. Dirección IP, subred y configuración de puerta de enlace

La configuración de TCP / IP de un host se compone de tres cosas principales - la dirección, máscara de subred y puerta de enlace. La dirección IP y la máscara de subred combinado es como el anfitrión sabe que las direcciones IP están en su red local. Para cualquier dirección fuera de la red local, el tráfico se envía (enviados) a la configurar puerta de enlace predeterminada que se debe saber cómo llegar al destino deseado. Una excepción a esta regla es una ruta estática, lo que indica a un router o del sistema en la forma de contacto específico no subredes locales accesibles a través de los routers conectados localmente. Esta lista de las pasarelas y rutas estáticas es mantiene en cada host en su tabla de enrutamiento. Para ver la tabla de enrutamiento utilizada por pfSense, consulte Sección 8.4.1, "Rutas de visión". Más información acerca del enrutamiento se pueden encontrar en Capítulo 8, Enrutamiento.
En una implementación típica de pfSense, los anfitriones se le asignará una dirección IP dentro del rango de la LAN pfSense, la misma máscara de subred que la interfaz LAN de pfSense y pfSense uso de IP de la LAN como su puerta de enlace predeterminada. Lo mismo se aplica a los hosts conectados a una interfaz que no sea inalámbrica, utilizando la configuración adecuada para la interfaz a la que el dispositivo está conectado.

Hosts dentro de una única red comunicarse directamente entre sí sin la participación de la puerta de enlace predeterminada. Esto significa que no hay cortafuegos, incluyendo pfSense, puede controlar un huésped a otro comunicación dentro de un segmento de red. Si esta función se requiere, los ejércitos o necesidad de ser segmentada a través de la utilización de múltiples switches o VLAN, o cambiar la funcionalidad equivalente, como PVLAN debe ser empleado. Las VLAN son cubiertos en Capítulo 10, LAN virtuales (VLAN).

1.7.4. Entender la notación de máscara de subred CIDR

pfSense utiliza un formato de máscara de subred es posible que no se conoce. En lugar de la común 255.xxx, usa CIDR (Classless InterDomain enrutamiento) notación.

Puede hacer referencia a Tabla 1.2, "Cuadro de subred CIDR" Para encontrar el equivalente de la subred CIDR máscara.

Máscara de subred	Total	Prefijo CIDR	IP Utilizables Direcciones	IP Número de / 24 redes
		Direcciones		
255.255.255.255	/ 32	1	1	1/256th
255.255.255.254 /	31	2	0	1/128th
255.255.255.252 /	30	4	2	1/64th
255.255.255.248 /	29	8	6	1/32nd
255.255.255.240 /	28	16	14	1/16o
255.255.255.224 /	27	32	30	1/8o
255.255.255.192 /	26	64	62	1/4o
255.255.255.128 /	25	128	126	Un medio
255.255.255.0	/ 24	256	254	1
255.255.254.0	/ 23	512	510	2
255.255.252.0	/ 22	1024	1022	4
255.255.248.0	/ 21	2048	2046	8
255.255.240.0	/ 20	4096	4094	16
255.255.224.0	/ 19	8192	8190	32
255.255.192.0	/ 18	16,384	16,382	64
255.255.128.0	/ 17	32,768	32,766	128
255.255.0.0	/ 16	65,536	65,534	256
255.254.0.0	/ 15	131,072	131,070	512
255.252.0.0	/ 14	262,144	262,142	1024
255.248.0.0	/ 13	524,288	524,286	2048
255.240.0.0	/ 12	1,048,576	1,048,574	4096
255.224.0.0	/ 11	2,097,152	2,097,150	8192
255.192.0.0	/ 10	4,194,304	4,194,302	16,384
255.128.0.0	/ 9	8,388,608	8,388,606	32,768
255.0.0.0	/ 8	16,777,216	16,777,214	65,536
254.0.0.0	/ 7	33,554,432	33,554,430	131,072
252.0.0.0	/ 6	67,108,864	67,108,862	262,144
248.0.0.0	/ 5	134,217,728	134,217,726	1,048,576

Máscara de subred	Total	Prefijo CIDR IP	Utilizables IP Direcciones	Número de / 24 redes
		Direcciones		
240.0.0.0	/ 4	268,435,456	268,435,454	2,097,152
224.0.0.0	/ 3	536,870,912	536,870,910	4,194,304
192.0.0.0	/ 2	1,073,741,824	1,073,741,822	8,388,608
128.0.0.0	/ 1	2,147,483,648	2,147,483,646	16,777,216
0.0.0.0	/ 0	4,294,967,296	4,294,967,294	33,554,432

Tabla 1.2. Tabla de subred CIDR

1.7.4.1. Entonces, ¿dónde estas cifras CIDR proceden de todos modos?

El número CIDR proviene del número de unos en la máscara de subred cuando se convierte a binario.

La máscara de subred 255.255.255.0 común es 11111111.11111111.11111111.00000000 en binario.
Esto se suma a los 24 o 24 horas (se pronuncia 'tala veinticuatro).

Una máscara de subred de 255.255.255.192 es 11111111.11111111.11111111.11000000 en binario, o 26
otros, por lo tanto un / 26.

1.7.5. CIDR de resumen

Además de especificar las máscaras de subred, CIDR también se puede emplear para la propiedad intelectual o de la red
efectos de compresión. El "total de direcciones IP" columna de la tabla de subred CIDR indica
¿Cuántas direcciones de una máscara CIDR dado a resumir. A los efectos de compresión de la red,
el "Número de redes / 24" de columna es útil. resumen CIDR se puede utilizar en varios
partes de la interfaz web de pfSense, incluyendo las reglas del cortafuegos, NAT, IPs virtuales, IPsec, rutas estáticas,
y mucho más.
Direcciones IP o redes que pueden estar contenidos dentro de una máscara CIDR único que se conoce como CIDR
resumibles.

Al diseñar una red a la que debe asegurar que todas las subredes IP privada en uso en un lugar determinado
CIDR son resumibles. Por ejemplo, si se necesitan tres / 24 subredes en un solo lugar, utilizar un 22 /
de la red en cuatro subredes / 24 redes. La siguiente tabla muestra los cuatro / 24 que subredes

puede utilizar con el 10.70.64.0/22 subred.
10.70.64.0/22 dividido en / 24 redes
10.70.64.0/24

10.70.64.0/22 dividido en / 24 redes
10.70.65.0/24
10.70.66.0/24
10.70.67.0/24

Tabla 1.3. CIDR de resumen de ruta

Esto ayuda a mantener más manejable de enrutamiento para redes multi-sitio (las vinculadas a otro ubicación física a través de la utilización de un circuito privado WAN o VPN). Con CIDR resumibles subredes, tiene un destino de la ruta que cubre todas las redes en cada lugar. Sin ella, tiene varias redes destino diferente por ubicación.

Ahora, si usted no es un gurú de subredes, te estás preguntando cómo diablos se me ocurrió la tabla anterior. Empiece por elegir un prefijo CIDR de la red, de acuerdo con el número de las redes que se requieren. A continuación, elija un / 24 de red que desea utilizar. Para ese ejemplo, yo eligió 10.70.64.0/24. Sé de memoria que xx64.0/24 será la primera / 24 de red en un 22 /, pero usted no tiene que escoger la primera red. Usted puede calcular esto utilizando las herramientas disponibles en el subnetmask.info [Http://www.subnetmask.info] página web.

Una de las herramientas se convierten en decimales con puntos de la máscara CIDR, y viceversa, esta función se muestra en la Figura 1.1, "convertidor de la máscara de subred". Si usted no tiene Tabla 1.2, "subred CIDR Tabla " desde principio de este capítulo en frente de usted, usted puede convertir su prefijo elegido CIDR a la notación decimal con puntos utilizando esta herramienta. Introducir un prefijo de CIDR y haga clic en el botón Calcular para su derecho, o entrar en una máscara decimal y haga clic en el botón Calcular a su derecha.

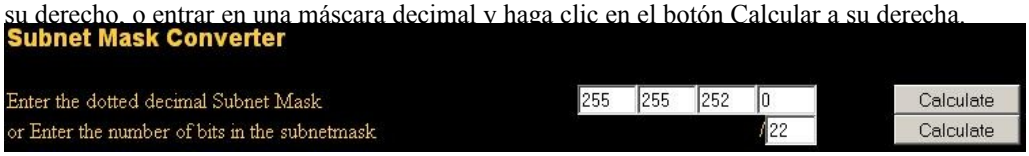


Figura 1.1. Máscara de subred convertidor

Armado con la máscara decimal con puntos, ahora ir a la sección de Red / Nodo Calculadora. Poner en la máscara de subred y una de las / 24 redes que desea utilizar. A continuación, haga clic en Calcular. La parte inferior cajas rellenar, y le mostrará la gama considerada en particular, que / 24, que se puede ver en Figura 1.2, "Red / Calculadora Nodo". En este caso, la dirección de red se 10.70.64.0/22, y se puede ver que el utilizables / 24 redes de 64 a 67. "Dirección de difusión" no es terminología pertinente cuando se utiliza esta herramienta para determinar un rango CIDR, que es simplemente la dirección más alta dentro de la gama.

Figura 1.2. Red / Calculadora Nodo

1.7.5.1. Encontrar un juego de red CIDR

Si usted tiene un rango de direcciones IP que desea resumir, el pfSense Electrodomésticos Herramientas [] Http://www.pfsense.org/toolsvm incluye cidr_range.pl, un script en Perl que calcula el CIDR redes necesarias para resumir una serie de direcciones IP. Si se ejecuta sin ningún argumento, podrás ver las instrucciones de uso.

#cidr_range.pl
```
Uso: cidr_range.pl <primer <IP <IP <Apellido>
```

Si desea resumir 192.168.1.13 192.168.1.20 a través, ejecute cidr_range.pl de la siguiente manera.

#cidr_range.pl 192.168.1.13 192.168.1.20
```
192.168.1.13/32
192.168.1.14/31
192.168.1.16/30
192.168.1.20/32
```

Esto demuestra que tomará cuatro rangos CIDR para incluir sólo a través de 192.168.1.13 192.168.1.20. Si uno mira hacia atrás en la mesa de CIDR, un / 29 máscara cubre 8 direcciones IP, y esto es de 8 direcciones IP, por lo que ¿por qué no un / 29 es suficiente? La respuesta es porque no se puede elegir una dirección arbitraria de partida para una amplia CIDR. Si usted va enchufe 192.168.1.13 255.255.255.248 y en la Red / Nodo Calculadora subnetmask.info [http://www.subnetmask.info/], Podrás ver las / 29 de red que contiene 192.168.1.13 es 192.168.1.8/29 con un rango de 0.8 a 0.15 (Figura 1.3, "Red / Nodo Ejemplo de la calculadora ").

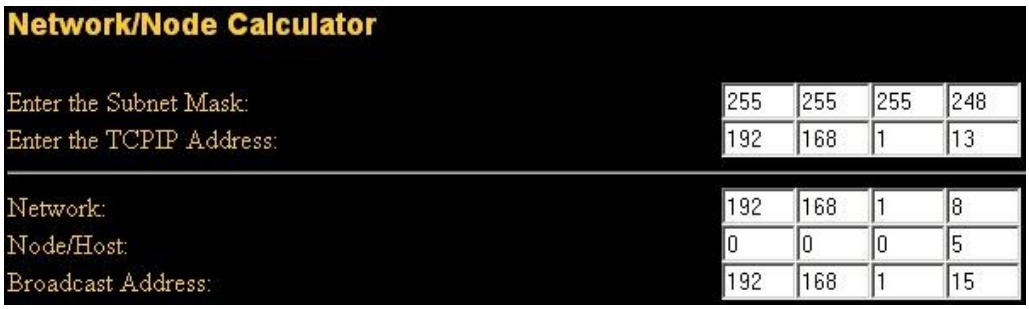


Figura 1.3. Red / Ejemplo calculadora Nodo

Si no necesariamente una coincidencia exacta, se puede conectar un número a la Red / Nodo Calculadora para acercarse a su resumen que desee.

1.7.6. Difusión de dominio

Un dominio de difusión es la parte de una red de intercambio de la misma capa dos segmento de red. En una red con un solo interruptor, el dominio de difusión es que el interruptor entero. En una red con múltiples switches interconectados sin el uso de VLANs, el dominio de broadcast incluye todos los de los interruptores.

Un dominio de difusión solo puede contener más de una subred IP, sin embargo, que es generalmente no se considera buen diseño de red. subredes IP deben ser segregados en emisión separada dominios a través de la utilización de interruptores separados, o VLANs.

dominios de difusión pueden ser combinados, cerrando dos interfaces de red juntos, pero debe cuidar deben adoptarse para evitar bucles de cambiar en este escenario. También hay algunos servidores proxy para protocolos determinados que no se combinan dominios de difusión, sino que el mismo efecto, como un relé DHCP que transmite las peticiones DHCP en el dominio de la difusión de otra interfaz. Más información sobre dominios de difusión y la forma de combinarlos se pueden encontrar en Capítulo 9, Puente.

1.8. Interfaz de nombres de Terminología

En esta sección se describe la interfaz de nombres terminología utilizada en pfSense y FreeBSD. La mayoría de la gente está familiarizada con las dos divisiones de la red básica: "WAN" y "Conexión", pero no se puede tantos segmentos como se puede imaginar. Usted está limitado únicamente por el número de interfaces (o VLAN) que tiene a su disposición.

Al examinar los nombres de interfaz, el tema de la segmentación de la red también viene a la mente. Es Es una buena práctica para mantener diferentes conjuntos de los sistemas alejados unos de otros. Por ejemplo, no

quieres que tu servidor web de acceso público, en la misma red que la LAN. Si el servidor se comprometido, el atacante podría fácilmente llegar a cualquier equipo de su LAN. Si han dedicado servidores de bases de datos, estos pueden ser aislados de todo lo demás y seguro de todo, menos los servidores que necesitan acceder a bases de datos. Al igual que con el ejemplo anterior, un comprometido web servidor no podría poner en peligro los servidores de bases de datos tanto como si estuvieran en la misma segmento sin un firewall en el medio.

1.8.1. LAN

La interfaz LAN es la primera interfaz interna del servidor de seguridad. Abreviatura de Red de área local, es más común el lado privado de un router que a menudo se utiliza un esquema de direcciones IP privadas. En implementaciones pequeñas, suele ser la única interfaz interna.

1.8.2. WAN

La interfaz WAN se utiliza para la conexión a Internet o conexión a Internet primaria en una despliegue multi-WAN. Abreviatura de red de área extensa, es la red social no son de confianza pública fuera de su router. Conexiones de Internet llegará a través de la interfaz WAN.

1.8.3. OPT

interfaces OPT u opcional se refieren a las interfaces conectadas a las redes locales que no sean LAN. interfaces OPT se utilizan comúnmente para los segmentos de LAN en segundo lugar, los segmentos DMZ, inalámbrica redes y mucho más.

1.8.4. OPT WAN

OPT WAN se refiere a las conexiones de Internet a través de una interfaz territorio palestino ocupado, ya sea los configurados para DHCP o especificando una dirección de puerta de enlace IP. Esto se discute en detalle en Capítulo 11, Múltiples Conexiones WAN.

1.8.5. DMZ

Corto para la zona desmilitarizada. El término fue tomado de su sentido militar, que se refiere a una especie de amortiguador entre un área protegida y una zona de guerra. En la creación de redes, es un área donde su servidores públicos que residen es accesible desde Internet a través de la WAN, pero también aislado de la LAN para que un compromiso en la zona de despeje no ponga en peligro los sistemas en otros segmentos. Algunas compañías de mal uso del término "zona de distensión" en sus productos de servidor de seguridad en referencia a 1:1 NAT en la IP WAN que expone una serie en la LAN. Hay más información sobre este tema en Sección 7.3.3, "1:1 NAT en la WAN IP, también conocido como" zona de distensión "en Linksys".

1.8.6. FreeBSD interfaz de nomenclatura

FreeBSD nombres de sus interfaces con el controlador de red utilizados, seguido de un número a partir de las 0 e incrementar en uno por cada interfaz adicional usando ese controlador. Por ejemplo, un común conductor `fxp`, Utilizado por las tarjetas de Intel Pro/100. La tarjeta Pro/100 por primera vez en un sistema se `fxp0`, el segundo es `fxp1`, Y así sucesivamente. Otras de las más comunes son `em` (Intel PRO/1000), `bge` (Varios Broadcom chipsets), `rl` (Realtek 8129/8139), entre muchos otros. Si su sistema de mezcla una tarjeta de Pro/100 y una Realtek 8139, las interfaces se `fxp0` y `rl0` , respectivamente. Interfaz asignaciones de nombres y están más cubiertos en Capítulo 3, Instalación y actualización.

1.9. Búsqueda de información y obtención de ayuda

En esta sección se ofrece orientación en la búsqueda de información en este libro, y en pfSense en general, así como el suministro de recursos sobre dónde obtener ayuda adicional si es necesario.

1.9.1. Búsqueda de información

La forma más sencilla de encontrar información sobre un tema específico en este libro es revisar el índice. Todos los características más comunes y las implementaciones de pfSense se tratan en este libro, y el índice de la voluntad ayudarle a encontrar la sección o secciones donde se cubre un tema específico.

Si usted no puede encontrar la información que busca en este libro, hay una gran cantidad de nuevos información y experiencias de usuario disponibles en los sitios pfsense.org diferentes. La mejor manera de Buscar en todos estos sitios es ir a Google, escriba en los términos que está buscando, y anexar **sitio: pfsense.org** a su consulta. Esto buscará en la página web, foros, wikis cvstrac, etc - Todas las fuentes oficiales de información. Hay una gran cantidad de información disponible en el foro, y esta es la mejor manera de buscar en ella. Esto también localizar información en la libre disposición partes de este libro.

1.9.2. Obtención de ayuda

El proyecto pfSense ofrece varias maneras de obtener ayuda, incluida una en el foro [http://forum.pfsense.org], wiki de documentación [Http://doc.pfsense.org], Listas de correo e IRC (Internet Relay Chat, # # PfSense en irc.freenode.net). Soporte comercial también está disponible a través de la suscripción de los fundadores del proyecto pfSense en el pfSense Portal [https: / / portal.pfsense.org]. Usted Puede encontrar más información sobre todas estas vías de apoyo en la La obtención de apoyo [http:// www.pfsense.org /] apoyo página en el sitio pfSense.

Capítulo 2. Hardware

pfSense es compatible con cualquier hardware que sea compatible con la versión de FreeBSD en uso, en i386 plataformas de hardware. Suplente arquitecturas de hardware, tales como PowerPC, MIPS, ARM, SPARC, etc no son compatibles en este momento. El nuevo incrustado puede traer MIPS y ARM apoyo en algún momento en 2009, aunque no está disponible en el momento de escribir este artículo. También hay aún no se haya comunicado de 64 bits, aunque la liberación de 32 bits funciona bien en el hardware de 64 bits. A de 64 bits entregar no entrará en el futuro para 2.0, y actualmente está en fase de pruebas por los desarrolladores. Para la fecha no ha sido una prioridad, porque el único beneficio que ofrece en relación con los cortafuegos es la capacidad para hacer frente a más memoria, e incluso la mayor pfSense instala la protección de miles de máquinas no utilizar 4 GB de RAM.

2.1. De compatibilidad de hardware

El mejor recurso para determinar la compatibilidad del hardware es la nota FreeBSD de hardware para el comunicado de la versión utilizada por la liberación pfSense va a instalar. pfSense 1.2.3 se basa en FreeBSD 7.2, por lo tanto una referencia definitiva sobre el hardware compatible se las notas de hardware en http://www.freebsd.org/releases/7.2R/hardware.html. La más general de hardware de FreeBSD Preguntas más frecuentes es otro buen recurso a utilizar para ayudar a la selección de hardware. Se puede encontrar en http://www.freebsd.org/doc/en_US.ISO8859-1/books/faq/hardware.html. En esta sección se ofrecen orientación sobre el mejor hardware soportado disponibles para fines de cortafuegos y enrutamiento. La consideración primordial y única recomendación fuera de las notas de hardware para la red adaptadores.

2.1.1. Adaptadores de red

Prácticamente todas las tarjetas de cable Ethernet (NIC) con el apoyo de pfSense. Sin embargo, no toda la red adaptadores son creados iguales. El hardware utilizado puede variar mucho en la calidad de un fabricante a otro, y en algunos casos, mientras que FreeBSD puede apoyar una determinada tarjeta de red, el soporte del controlador puede ser pobre con una implementación específica del chipset.

Tarjetas de red Intel Pro/100 y PRO/1000 son los más recomendables porque tienen sólidos ayuda al conductor en FreeBSD escrito por los empleados de Intel, y un buen desempeño. En el otro extremo del del espectro, Realtek 8139 `rl` tarjetas de hardware de calidad son muy comunes pero muy pobre. Un fragmento de un comentario en el código fuente para este controlador cuenta la historia - "El RealTek 8139 PCI NIC redefine el significado de 'gama baja'. Este es probablemente el peor controlador Ethernet PCI jamás se ha hecho, con la posible excepción del chip FIESTA realizado por SMC. "agrava la cuestión es el hecho de que numerosos fabricantes incorporar este chip en sus tarjetas de red, con una amplia diversos grados de calidad. Usted encontrará 8.139 tarjetas integrado en algunos de hardware integrado, y

los que en general son confiables y funcionan correctamente. De las diversas tarjetas PCI que existen algunos trabajos
bien, y algunos tienen varias cosas que se rompen. Las VLAN pueden no funcionar correctamente o en absoluto, y modo promiscuo necesarios para salvar no pueden trabajar, entre muchas otras posibilidades.

Si usted tiene tarjetas de red disponibles y están construyendo un sistema de piezas de repuesto, vale la pena intentar lo que tiene a mano. Muchas veces ellos no tendrán ningún problema. Si usted está buscando para comprar hardware para la implementación, van con las tarjetas de Intel. En las redes donde la fiabilidad y el rendimiento son de la mayor preocupación, no escatiman en gastos mediante el uso de cualquier NIC le sucede que tiene por ahí (A menos que estos resultan ser Intels).

Si utiliza VLAN, asegúrese de seleccionar los adaptadores que soporte VLAN de procesamiento en el hardware. Esto es discutido en Capítulo 10, LAN virtuales (VLAN).

2.1.1.1. USB Adaptadores de red

Muchos adaptadores de red USB son compatibles, pero en general no se recomienda. Realizan
mal, especialmente en sistemas que no son compatibles con USB 2.0, o con adaptadores que son estrictamente USB 1.1. NIC USB son ideales en caso de apuro, o cuando se añade la conectividad de red a una PC de escritorio, y están muy bien para algunas implementaciones casa cortafuegos, pero para un rendimiento fiable en el que los centros de datos
no debe ser considerada.

2.1.1.2. Adaptadores inalámbricos

Adaptadores inalámbricos compatibles con las recomendaciones y están cubiertos en Sección 18.1.2, "Wireless controladores incluidos en el apartado 1.2.3 ".

2.2. Requisitos mínimos de hardware

A continuación se describen los requisitos mínimos de hardware para pfSense 1.2.3. Tenga en cuenta la requisitos mínimos no son adecuados para todos los entornos, véase Sección 2.4, "Hardware tamaño Orientación " para el hardware de tamaño de orientación.

2.2.1. Base de Requisitos

Los siguientes requisitos son comunes a todas las plataformas de pfSense.

- CPU - 100 MHz o más rápido
- RAM - 128 MB o más

2.2.2. Requisitos Específicos de la Plataforma

Requisitos específicos para plataformas seguimiento individual.

2.2.2.1. Live CD

- Unidad de CD-ROM
- unidad flash USB o unidad de disco para almacenar archivos de configuración

2.2.2.2. Instalación completa

- CD-ROM para la instalación inicial
- 1 GB o disco duro más grande

2.2.2.3. NanoBSD incorporado

- 512 MB o más Tarjeta Compact Flash
- Puerto serie para la consola
- El cable de módem nulo para conectar con el puerto de consola

2.3. Selección de hardware

Abrir los sistemas operativos de fuente puede provocar muchos dolores de cabeza con la compatibilidad de hardware.

Mientras que una determinada pieza de hardware pueden ser compatibles, una implementación específica de la misma puede
no funciona correctamente, o ciertas combinaciones de hardware no pueden trabajar. Esto no se limita a FreeBSD (y por lo tanto pfSense) - distribuciones de Linux también sufren la misma suerte. En más de una década de experiencia en el uso BSD y varias distribuciones de Linux en una amplia variedad de hardware, Lo he visto infinidad de veces. Algunos sistemas que funcionan bien con Windows no funciona en absoluto con BSD o Linux, algunos funcionan bien con BSD, pero no Linux, algunos con Linux pero no BSD. Si le sucede a tener problemas relacionados con el hardware, Sección 3.5.4, "Solución de problemas de hardware" ofrece consejos que va a resolver estos problemas, en algunos casos.

2.3.1. La prevención de dolores de cabeza de hardware

Esta sección ofrece algunos consejos para evitar problemas de hardware.

2.3.1.1. Utilice el hardware de los desarrolladores el uso

Con los años, algunos fabricantes de hardware han donado equipo muy necesario para nuestra prueba los desarrolladores. Mediante el uso de equipos de estos vendedores, se asegura que el dispositivo que usted está comprando
está bien probado, y si FreeBSD regresiones que afectan al hardware de ocurrir en el futuro, serán fija antes de que siquiera sabía que existían. Animamos a nuestra base de usuarios para apoyar a las empresas que apoyan el proyecto. También estamos en la etapa de planificación de la oferta de venta directa por hardware,

ofreciendo plataformas de hardware en la pre-instalado que usamos, y sabemos que es roca sólida y plenamente compatibles.
Visita http://www.pfsense.org/vendors para la información más actualizada sobre recomienda proveedores de hardware.

2.3.1.2. Búsqueda de las experiencias de otros

Si está utilizando una pieza de hardware de un fabricante importante, si escribe su marca, modelo, y **sitio: pfsense.org** en Google, hay una alta probabilidad de que se encuentre a alguien que ha intentado o está utilizando el hardware. También puede intentar la búsqueda de la marca, modelo, y **pfSense** para encontrar experiencias personas han reportado en otros sitios web o los archivos de lista de correo. Informes de fracaso no necesariamente debe considerarse definitivo, ya que los problemas de un solo usuario en un sistema en particular puede ser el resultado de hardware defectuoso u otra anomalía en lugar de incompatibilidad. Repetir estas búsquedas con la misma **FreeBSD** en lugar de pfSense también puede resultar hasta experiencias de usuario útil.

2.4. Tamaño del hardware de Orientación

Al dimensionar el hardware para su uso con pfSense, dos factores principales que deben tenerse en cuenta: el rendimiento requerido y características que se utilizarán. En las secciones próximas cubrir estas consideraciones.

2.4.1. Consideraciones de rendimiento

Si necesita menos de 10 Mbps de rendimiento, puede llegar a funcionar con los requisitos mínimos.

Para los requisitos de rendimiento más alto se recomienda seguir estas directrices, basadas en nuestra ensayos y amplias experiencias de implementación. Estas directrices ofrecen un poco de espacio para respirar porque nunca se desea ejecutar el hardware para su plena capacidad durante períodos prolongados.

La elección de la tarjeta de red tiene un impacto significativo en el rendimiento máximo alcanzable, dependiendo de la velocidad de la CPU. Tabla 2.1, "el rendimiento máximo por CPU" muestra la rendimiento máximo alcanzable utilizando dos tarjetas de red Realtek 8139 en comparación con dos Intel PRO/1000 GT Desktop tarjetas de red para plataformas de hardware con las ranuras PCI.

CPU	A bordo de Max	Realtek Max	PRO/1000 Max
	Rendimiento (Mbps)	Rendimiento (Mbps)	Rendimiento (Mbps)
Pentium MMX	n / a	25 Mbps	40 Mbps
200 MHz WRAP - 266 MHz Geode	24 Mbps	n / a	n / a

CPU	A bordo de Max Rendimiento (Mbps)	Realtek Max Rendimiento (Mbps)	PRO/1000 Max Rendimiento (Mbps)
ALIX - 500 MHz Geode	85 Mbps	n / a	n / a
VIA de 1 GHz	93 Mbps (100 Mb velocidad de cable)	n / a	n / a
Netgate Hamakua (1 GHz Celeron)	250 Mbps	n / a	n / a
Pentium II a 350 MHz	n / a	51 Mbps	64 Mbps
Pentium III 700 MHz	n / a	84 Mbps	217 Mbps
Pentium 4 1.7 GHz	n / a	93 Mbps (100 Mb velocidad de cable)	365 Mbps

Tabla 2.1. Máximo rendimiento de la CPU

2.4.1.1. Diferencia de desempeño por tipo de adaptador de red

La elección de NIC tendrá un impacto significativo en el rendimiento. Baratos tarjetas de gama baja como Realteks se consumen CPU significativamente más que las tarjetas de buena calidad, tales como Intel. Su primera cuello de botella con un rendimiento de firewall será su CPU. Usted puede obtener el rendimiento significativamente más de una CPU dada usando una tarjeta de red de mejor calidad, como se muestra en Tabla 2.1, "Rendimiento Máximo por CPU " con la CPU más lenta. Si usted tiene una CPU capaz de rendimiento significativamente más de lo que requieren, la elección de las NIC tendrá poco o ningún impacto en el rendimiento, aunque menor NIC calidad pueden no ser fiables en algunas circunstancias.

2.4.1.2. De tamaño para el rendimiento gigabit

Cuando el tamaño de las implementaciones de Gigabit, primero tiene que determinar la cantidad que el rendimiento realmente necesita - 1 Gbps de velocidad de cable o simplemente Mbps a más de 100. En muchas redes no hay sistemas capaces de llenar de 1 Gbps con los datos del disco, como un disco de los sistemas de E / S es incapaz de tal ejercicio. Si lo que desea es ser capaz de golpear de 200 Mbps, un sistema de 1 GHz, con buena NIC calidad suficiente. Para un máximo de 400 a 500 Mb / s, un viejo servidor de 3.2 GHz es suficiente.

2.4.1.3. De tamaño de varios gigabits por segundo despliegues

Los números en Tabla 2.1, "el rendimiento máximo por CPU" parar en un nivel relativamente bajo debido a esa es la medida de lo que razonablemente puede probar en nuestro laboratorio. Pruebas múltiples servidores Gbps

requiere que los servidores y los sistemas de varias capaz de empujar una velocidad de cable Gbps. No tenemos
equipamiento adecuado para que la escala de las pruebas. Pero eso no quiere decir que pfSense no es adecuado en ese entorno, de hecho se utiliza en numerosos despliegues presionando en exceso de 1 Gbps.

Cuando el tamaño de los despliegues multi-Gbps, el factor principal es de paquetes por segundo, no Gbps. Usted llegará al límite de FreeBSD y hoy el más rápido de hardware de servidor de cuatro núcleos en torno a 500.000 paquetes por segundo (pps). ¿Cuánto rendimiento que esto equivale a depende de la red
medio ambiente, con algunas referencias proporcionadas en Tabla 2.2, "500.000 de pps en distintos tamaños de marco ".

Tamaño del marco	Rendimiento de procesamiento en 500Kpps
64 bytes	244 Mbps
500 bytes	1.87 Gbps
1000 bytes	3.73 Gbps
1500 bytes	5.59 Gbps

Tabla 2.2. 500.000 pps rendimiento de procesamiento en el marco de diversos tamaños

Para implementaciones que buscan lograr una velocidad de cable entre dos interfaces Gbps, un Pentium 4 3 GHz o más rápido con PCI-X o PCI NIC-e debe ser utilizado. PCI le permitirá alcanzar
varios cientos de Mbps, pero la velocidad del bus PCI limitaciones le impiden alcanzar la velocidad del cable rendimiento con dos tarjetas de red una Gbps.

Si usted es el hardware utilizado para algo capaz de un rendimiento Gigabit velocidad de cable en varios interfaces, consiga un nuevo servidor con un procesador de cuatro núcleos y tarjetas de red PCI-e y usted estará en buenas forma. Si usted necesita empujar más de 500.000 paquetes por segundo, que puede exceder la capacidad
de hardware de PC para impulsar paquetes. Consulte Sección 1.4.2.1, "Router LAN" para más de la información.

2.4.2. Característica Consideraciones

La mayoría de las características no tienen en cuenta en el hardware de tamaño, aunque algunos tienen un impacto significativo en la utilización de hardware.

2.4.2.1. Tablas Grandes Estado

La tabla de estado de servidor de seguridad es donde las conexiones activas de red a través del servidor de seguridad se realiza un seguimiento,
con cada conexión consume un estado. Estados están cubiertos en más Capítulo 6, Servidor de seguridad.
Entornos que requieren un gran número de conexiones simultáneas (y por lo tanto, estados)

requiere RAM adicional. Cada estado tiene aproximadamente 1 KB de memoria RAM. Tabla 2.3, "Estado Grande
Tabla de Consumo de RAM " proporciona una guía para la cantidad de memoria requerida para un gran número de estados. Tenga presente que esto es sólo la memoria utilizada para el seguimiento del estado y el otro componentes de pfSense se requieren por lo menos 32 a 48 MB de memoria RAM adicional en la parte superior de este y posiblemente
más, dependiendo de las características de uso.

Estados	RAM necesaria
100,000	~ 97 MB
500,000	~ 488 MB
1,000,000	~ 976 MB
3,000,000	~ 2900 MB

Tabla 2.3. Mesa grande del Estado de RAM Consumo

2.4.2.2. VPN (todo tipo)

La pregunta la gente suele preguntar acerca de VPN es "cuántas conexiones puede mi hardware manejar? "Ese es un factor secundario en la mayoría de las implementaciones, de menor consideración. El principal consideración en el hardware de tamaño de VPN es el rendimiento requerido.

El cifrado y descifrado de tráfico de red con todo tipo de VPN es muy intensivo de la CPU. pfSense ofrece seis opciones de cifrado para su uso con IPsec: DES, 3DES, Blowfish, Cast128, AES y AES 256. Los sistemas de cifrado diferentes actúan de forma diferente, y el máximo rendimiento de su servidor de seguridad
depende del sistema de cifrado utilizado. 3DES es ampliamente utilizado por su interoperabilidad con casi todos los dispositivos IPSec, sin embargo, es el más lento de todos los sistemas de cifrado con el apoyo de pfSense en ausencia de un acelerador de hardware criptográfico. Aceleradores criptográficos de hardware, tales como cartas de apoyo Hifn gran aumento máximo de la VPN, y eliminar en gran medida la diferencia de rendimiento
entre los sistemas de cifrado. Tabla 2.4, "Rendimiento de IPsec por Cipher - ALIX" muestra el máximo rendimiento al sistema de cifrado de hardware para PC Motores ALIX (Geode de 500 MHz) con y sin un Soekris vpn1411 acelerador criptográfico Hifn.

Protocolo de cifrado	Máximo rendimiento	Máximo rendimiento (con Hifn)
DES	13.7 Mbps	
3DES	8.4 Mbps	
Blowfish	16.5 Mbps	
CAST128	16.3 Mbps	

34.6 Mbps	no acelerada (sin cambios)	no acelerada (sin cambios)
34.3 Mbps		

Protocolo de cifrado	Máximo rendimiento	Máximo rendimiento (con Hifn)
AES	19.4 Mbps	34.2 Mbps
AES de 256	13.5 Mbps	34.2 Mbps

Tabla 2.4. IPSec por Cipher - ALIX

Tabla 2.5, "Rendimiento de IPsec por CPU" muestra el máximo rendimiento de IPsec por la CPU para la sistema de cifrado Blowfish, para ilustrar la capacidad de rendimiento máximo de CPU diferentes.

CPU	Rendimiento Blowfish (Mbps)
Pentium II a 350	12.4 Mbps
ALIX (500 MHz)	16.5 Mbps
Pentium III 700	32.9 Mbps
Pentium 4 1.7 GHz	53.9 Mbps

Tabla 2.5. IPSec por CPU

aceleradores de hardware criptográfico deben ser utilizados en gran ancho de banda a través de IPsec es

necesario,
excepto con CPUs dual o quad core, como las CPUs realizar cifrado más rápido que un acelerador
evitando la comunicación en el bus PCI.

2.4.2.3. Paquetes

Algunos paquetes tienen un impacto significativo en los requisitos de hardware en su entorno.

2.4.2.3.1. Bufido

Snort, el sistema de detección de intrusiones en la red disponibles en el sistema de paquetes pfSense, puede
requieren una cantidad significativa de memoria RAM, dependiendo de su configuración. 256 MB debería
considerarse como un mínimo, y algunas configuraciones pueden necesitar de 1 GB o más.

2.4.2.3.2. Calamar

Squid es un proxy-caché HTTP disponible como un paquete de pfSense servidor, y el disco E / S
es una consideración importante para los usuarios de Squid, ya que determina el rendimiento de la caché. Por el contrario,
para la mayoría de los usuarios de pfSense es en gran medida irrelevante, ya que el único impacto significativo que la
velocidad del disco
tiene en pfSense es el momento de arranque y el tiempo de actualización, no tiene importancia para el rendimiento de la red
u otros
funcionamiento normal.

En ambientes pequeños, incluso para Squid, cualquier unidad de disco duro es suficiente. Para implementaciones más de 200 usuarios
usando Squid, usted debe considerar 10K RPM SATA o discos SCSI. Utilice 15K RPM SCSI o SAS discos para un mejor rendimiento en entornos de gran tamaño.

pfSense soporta la mayoría de los controladores RAID de hardware que se encuentran en el hardware del servidor. El uso

de RAID
10 en sus arreglos RAID puede mejorar aún más el rendimiento del calamar, y se recomienda que para despliegues con miles de usuarios.

Capítulo 3. Instalación y actualización

El hardware ha sido elegido, junto con la versión de pfSense y la plataforma a utilizar. Ahora es el momento de descargar la versión apropiada pfSense e instalarlo en el dispositivo de destino. Después de descargar la versión correcta, continúe con la sección que describe la instalación de la plataforma que ha sido elegido: Instalación completa o Embedded. Si tiene algún problema durante el proceso, ver Sección 3.5, "Solución de problemas de instalación" adelante en este capítulo.

En este capítulo, también hablamos de métodos de instalación de recuperación y cómo actualizar pfSense. Recuperación de las instalaciones (Sección 3.6, "La recuperación de la instalación") Son formas de volver a instalar pfSense con una configuración existente, por lo general con mínimo tiempo de inactividad. Actualización de pfSense (Sección 3.7, "Actualización de una instalación existente") Mantendrá el sistema actual, añadir nuevas funciones, o fijar errores. La actualización es un proceso bastante indoloro que puede realizarse de varias maneras diferentes.

3.1. Descarga de pfSense

Examinar para www.pfsense.org [http://www.pfsense.org] Y haga clic en el **Descargas** enlace. En el página de descargas, haga clic en el enlace para las nuevas instalaciones. Esto llevará a la página de selección de espejo. Elija un espejo geográficamente cerca de su ubicación para un mejor rendimiento. Una vez que el espejo ha sido seleccionado, una lista de directorios aparecerá con los archivos de la versión actual pfSense para las nuevas instalaciones.

Por Live CD o instalaciones completas, descargue el `.iso` archivo. El nombre de la versión 1.2.3 del archivo es `pfSense-1.2.3-LiveCD-Installer.iso`. También hay un archivo MD5 a disposición por la mismo nombre, pero que terminan en `.md5`. Este archivo contiene un valor hash de la ISO, que puede ser utilizado para garantizar la descarga completa correctamente.

Para las instalaciones incrustadas, descargue el `.img.gz` archivo. El nombre de la versión 1.2.3 del archivo es `pfSense-1.2.3-nanobsd-`*tamaño*`.img.gz`, Donde *tamaño* es uno de los 512M, 1G, 2G, 4G o, para reflejar el tamaño de la tarjeta CF para el que se pretende que la imagen (los tamaños están en M de megabyte y G de gigabyte). Normalmente usted desea hacer coincidir el tamaño de la imagen al tamaño de su tarjeta CF, pero se puede utilizar una imagen de menor tamaño en una tarjeta CF más grande, como una imagen de 1G a 2G La tarjeta CF. Este archivo es una imagen comprimida con gzip. No es necesario extraer el archivo, ya que el proceso de instalación describen más adelante en este capítulo se encargará de eso.

Si en cualquier punto de la instalación de algo no va como se describe, visita Sección 3.5, "Solución de problemas de instalación".

3.1.1. Verificación de la integridad de la descarga

El archivo MD5 que acompañan pueden ser utilizados para verificar la descarga se completó correctamente, y que el lanzamiento oficial se está utilizando.

3.1.1.1. Verificación MD5 en Windows

Los usuarios de Windows pueden instalar HashTab [http://beeblebrox.org/hashtab/] o un programa similar al Hashes MD5 vista de cualquier archivo. Con HashTab instalados, haga clic derecho sobre el archivo descargado y habrá una pestaña File Hashes que contiene el hash MD5, entre otros. El MD5 generado hash se puede comparar con el contenido de la `. Md5` archivo descargado desde el sitio web de pfSense, que se puede ver en cualquier editor de texto sin formato como Bloc de notas.

3.1.1.2. MD5 de verificación en BSD y Linux

El comando md5 viene de serie en FreeBSD, y muchos otros UNIX y UNIX-como sistemas operativos. Un hash MD5 puede ser generada mediante la ejecución del siguiente comando de en el directorio que contiene el archivo descargado:

#md5 pfSense-1.2.3-LiveCD-Installer.iso

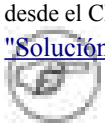
Comparar el hash resultante con el contenido de la `. Md5` archivo descargado desde el pfSense página web. (Sistemas GNU o Linux proporciona un comando md5sum que funciona de manera similar.)

3.1.1.3. MD5 de verificación en OS X

OS X también incluye el comando md5 como FreeBSD, pero también hay aplicaciones de interfaz gráfica de usuario disponibles, tales como MD5 de Tormentas Eterno [http://www.eternalstorms.at/md5/].

3.2. Instalación completa

En esta sección se describe el proceso de instalación de pfSense en un disco duro. En pocas palabras, se trata de el arranque desde el Live CD, realizar algunas configuraciones básicas, y luego invocar el instalador desde el CD. Si tiene problemas al tratar de arrancar o instalar desde el CD, consulte Sección 3.5, "Solución de problemas de instalación" adelante en este capítulo.



Nota

Si el hardware de destino no tiene una unidad de CD-ROM, un equipo diferente puede se utiliza para instalar en el disco duro de destino. Ver otras técnicas de instalación (Sección 3.4, "otras técnicas de la instalación") para más información.

3.2.1. Preparación de los CD

El CD tendrá que ser quemado de la imagen ISO descargada en la sección anterior. Desde el archivo descargado es una imagen de CD, tendrá que ser quemados apropiadamente para archivos de imagen - no como un CD de datos que contiene el archivo ISO solo. Procedimientos para hacerlo varía según la OS y software disponible.

3.2.1.1. Ardor en Windows

Prácticamente todos los principales quema de CD paquete de software para Windows incluye la posibilidad de grabar Imágenes ISO. Consulte la documentación del programa de grabación de CD que se utiliza. Una búsqueda en Google con el nombre del software de grabación y "**quemar iso**"Debería ayudar a localizar las instrucciones.

3.2.1.1.1. Grabación con Nero

Es fácil de grabar imágenes ISO con Nero. Comience haciendo clic derecho sobre el archivo ISO, a continuación, haga clic en Abrir

Con y seleccione Nero. La primera vez que se hace esto, puede que sea necesario para seleccionar Elija Predeterminado Programa de Nero y luego elegir de la lista. Este mismo proceso se debe trabajar con otros comerciales Software para quemar CD.

3.2.1.1.2. Grabación con el ISO Recorder

Si utiliza Windows XP, 2003 o Vista, la libre disposición ISO Recorder [http://] Isorecorder.alexfeinman.com herramienta puede ser utilizada. Descargar e instalar la versión adecuada de la norma ISO Recorder para el sistema operativo que se utilice, a continuación, busque la carpeta en la unidad que contiene la norma ISO pfSense, haga clic derecho sobre él y haga clic en la imagen Copiar a CD.

3.2.1.1.3. Otros software de grabación gratuito

Otras opciones gratuitas para los usuarios de Windows incluyen CDBurnerXP [http://www.cdburnerxp.se/], InfraRecorder [Http://infrarecorder.org/] Y burnatonce (BAO) [http://www.burnatonce.net/ descargas /], Entre otros. Antes de descargar e instalar cualquier programa, comprobar su función lista para asegurarse de que es capaz de grabar una imagen ISO.

3.2.1.2. Ardor en Linux

distribuciones de Linux como Ubuntu suelen incluir algún tipo de interfaz gráfica de usuario de aplicaciones de grabación de CD
que puede manejar imágenes ISO. Si uno se integra con el gestor de ventanas, haga clic derecho en la Archivo ISO y seleccione Grabar disco de. Otras opciones populares incluyen K3B y Brasero Disc Burner.

Si no hay una aplicación gráfica quema instalado, aún es posible grabar desde el
de línea de comandos. En primer lugar, determinar el dispositivo de grabación de SCSI ID / LUN (Logical Unit Number) con el siguiente comando:

#cdrecord - scanbus

```
Cdrecord-Clone 2.01 (i686-pc-linux-gnu) Copyright (C) 1995-2004 Jörg
Schilling
Linux versión del controlador sg: 3.1.25
Al usar la versión libscg 'Schily-0.8'.
scsibus0:
   0,0,0 100 'LITE-ON') 'COMBO LTC-48161H' KH0F 'extraíble de CD-ROM
```

Tenga en cuenta el SCSI ID / LUN *0,0,0*. Grabar la imagen como en el ejemplo siguiente, reemplazando ***<Max > Velocidad*** con la velocidad de la hornilla y *lun* con el ID SCSI / LUN del grabador:

**#cdrecord - dev =*lun* - Velocidad =*speed*> <*máximo* **
pfSense-1.2.3-LiveCD-Installer.iso

3.2.1.3. Ardor en FreeBSD

FreeBSD incluye el programa burncd en su sistema base que puede utilizarse para grabar imágenes ISO como tal.

#burncd-s e-max datos fijar pfSense-1.2.3-LiveCD-Installer.iso

Para obtener más información sobre la creación de CD en FreeBSD, por favor, consulte la entrada de grabación de CD en el
Manual de FreeBSD en http://www.freebsd.org/doc/en/books/handbook/creating-cds.html.

3.2.1.4. Verificación de la CD

Ahora que el CD está preparado, compruebe que se ha grabado correctamente consultando los archivos contenidos en
el CD. Más de 20 carpetas deben ser visibles, incluyendo depósito, de arranque, véase, conf, y mucho más. Si sólo
un archivo ISO grande que se ve, el CD no se ha grabado correctamente. Repita los pasos indicados anteriormente para
grabar un CD, y asegúrese de grabar el archivo ISO como una imagen de CD y no como un archivo de datos.

3.2.2. Arrancando desde el CD

Ahora el poder en el sistema de destino y colocar el CD en la unidad. pfSense debe empezar a arrancar, y mostrar el resultado de una asignación de interfaces del sistema que se trata en una sección siguiente.

3.2.2.1. Especificación de la Orden de arranque en la BIOS

Si el sistema de destino no arranque desde el CD, la razón más probable es que la unidad de CD-ROM no era lo suficientemente temprano en la lista de medios de arranque en la BIOS. Muchas placas base más nuevas también permiten
la educación de un menú de arranque una vez se pulsa una tecla durante el POST, comúnmente Esc o F12.

En su defecto, cambiar el orden de arranque en la BIOS. En primer lugar el poder, en el sistema y entrar en el BIOS de configuración. Es típicamente encontrado en una prioridad de arranque o la partida de inicio, pero podría estar en cualquier lugar. Si
arrancar desde el CD-ROM no está habilitado, o tiene una prioridad más baja que el arranque desde el disco duro y la unidad contiene otro sistema operativo, el sistema no arranque desde el CD de pfSense. Consulte el placa manual para obtener información más detallada en la modificación de la orden de inicio.

3.2.3. Asignación de interfaces

Después de que el Live CD pfSense ha completado el proceso de arranque, el sistema le pedirá para la interfaz asignación como en Figura 3.1 ", pantalla de asignación de interfaz". Aquí es donde las tarjetas de red instalado en el sistema reciben sus funciones como WAN, LAN, e interfaces opcionales (OPT1

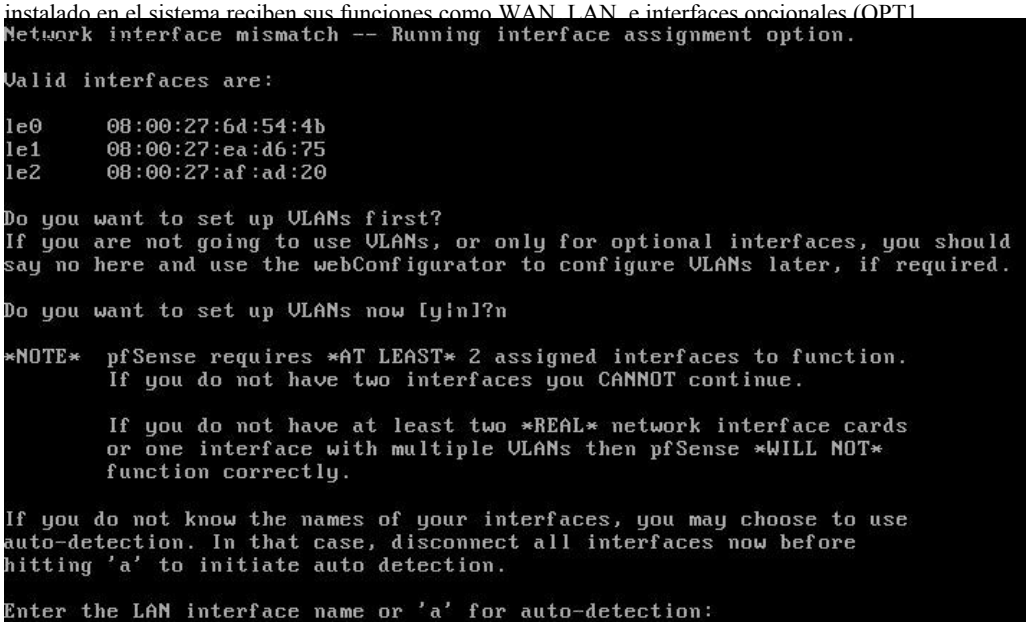


Figura 3.1. Interfaz de pantalla de asignación de

Una lista de las interfaces de red y sus direcciones MAC que se encuentra en el sistema aparecerá, junto con una indicación de su estado de vínculos si que es compatible con la tarjeta de red. El estado de los vínculos se denota por "(arriba)" que aparece después de la dirección MAC si un enlace se detecta en esa interfaz. La MAC (Media Access Control) de una tarjeta de red es un identificador único asignado a cada tarjeta, y no hay dos tarjetas de red deben tener la misma dirección MAC. (En la práctica, esto no es bastante duplicación cierto, la dirección MAC se produce con bastante frecuencia.) Después de eso, un mensaje aparecerá para La configuración de VLAN. Si se desean las VLAN, consulte Capítulo 10, LAN virtuales (VLAN) más adelante en el libro de los detalles de su configuración y uso. De lo contrario, escriba **n** y pulse Enter.

La interfaz LAN está configurada en primer lugar. Como pfSense 1.2.3 requiere al menos dos tarjetas de red, un dilema que se presente: ¿Cómo saber cuál es cuál? Si la identidad de cada tarjeta ya está conocida, simplemente escriba los nombres de los dispositivos adecuados para cada interfaz. Si la diferencia entre tarjetas de red es desconocida, la forma más sencilla de resolverlo sería utilizar la detección automática función.

Para la asignación automática de interfaz, en primer lugar desconecte todos los cables de la red del sistema, a continuación, escriba **una** y pulse Enter. Ahora conectar un cable de red en la interfaz que debe conectarse a la LAN, y pulse Enter. Si todo ha ido bien, pfSense debe saber ahora que la interfaz a utilizar para la LAN. El mismo proceso se puede repetir para la WAN y las interfaces opcionales que se le sea necesario. Si aparece un mensaje como No vinculación detecta, consulte la Sección 3.5, "Instalación Solución de problemas " Para obtener más información sobre la separación de las identidades de tarjeta de red.

Después de las interfaces se han configurado, aparecerá un mensaje pidiendo `¿Quieres continuar?`. Si la asignación de interfaz de red aparece tipo correcto, **y**, A continuación, presione ENTRAR. Si el cesión no es correcto, el tipo **n** y pulse Enter para repetir este proceso.

3.2.4. Instalación en el disco duro

Una vez que la asignación de interfaz es completa, aparecerá un menú con las tareas adicionales que puedan llevar a cabo. Para instalar pfSense en el disco duro del sistema, seleccione la opción **99** que poner en marcha el proceso de instalación.

La primera pantalla que aparece le pedirá que modifica configuración de la consola. A menos que un idioma alternativo teclado se está utilizando, elija aceptar esta configuración y pasar al siguiente paso.

A continuación, una lista de tareas se presentará. Si sólo hay un disco duro instalado en el sistema y no es necesario configurar las opciones de encargo, rápido / instalación sencilla se puede elegir. Esto la instalación en el primer disco duro se encuentra y acepta todas las opciones por defecto. Un diálogo de confirmación se mostrará. Pulse Aceptar para continuar o Cancelar para volver al menú anterior. La instalación continuará y que sólo deje para solicitar que el núcleo debe ser instalado.

Si decide utilizar el Quick / opción de instalación sencilla, vaya a Tabla 3.1, "Opciones del kernel" de opciones del kernel. De lo contrario, elige la primera opción: Instalar pfSense para realizar una instalación personalizada y continuar por el resto de esta sección.

Ahora escoja el disco duro para que pfSense se instalará. Cada unidad de disco duro conectado a la sistema debe ser mostrado, junto con los volúmenes RAID admitido o gmirror. Seleccione la unidad con las flechas arriba y abajo, a continuación, presione ENTRAR. Si no hay unidades se encuentran o son las unidades de disco incorrecta se muestra, es posible que la unidad deseada está conectado a un controlador compatible o un controlador establecido para un modo de no admitidos en el BIOS. Ver Sección 3.5, "Solución de problemas de instalación" de ayudar.

El siguiente paso es formatear la unidad que fue elegido justo. A menos que se sabe con certeza que el unidad contiene una partición de FreeBSD utilizable, seleccione Formato de este disco y pulse enter. De lo contrario, elegir Omitir este paso. Cuando se presentó la pantalla de la geometría del disco, es mejor elegir utilizar esta geometría. Es posible reemplazar este si hay más valores correctos son conocidos, pero en la mayoría de los casos los valores por defecto son correctos. Una pantalla de confirmación aparecerá, momento en el que la unidad de formato < opción name> debe ser elegido para continuar.

Nota

Este es un buen lugar para parar y asegurarse de que la unidad correcta ha sido seleccionada, como no hay vuelta atrás una vez que esta acción se ha realizado. Todo en el el disco se destruirán.

el arranque dual con otro sistema operativo es posible que los usuarios avanzados que saben configurar manualmente esas cosas, pero este tipo de configuraciones no se admiten oficialmente y se No se detallan aquí.

Particionado se indica, y simplemente debe aceptar los valores predeterminados eligiendo Aceptar y Crear, a continuación, elija Sí, la partición en la siguiente pantalla.

Un sistema se muestra a continuación para la instalación de bloques de arranque. Esto es lo que permitirá que el disco duro para arrancar.

Instalación de bloques de arranque ya estará seleccionada (aparece una X en la columna junto a la unidad que se configurado). Paquete modo puede o puede no ser necesario, dependiendo de la combinación de hardware en uso. Algunos de hardware más nuevo y más grande discos funcionarán mejor con el modo paquetes habilitado y hardware antiguo puede preferir el modo paquetes con discapacidad. Deja los valores por defecto seleccionado a menos que no trabajo en el sistema por alguna razón. A continuación, seleccione Aceptar y bloques de arranque de instalación y pulse Enter.

Un cuadro de confirmación aparecerá con el resultado de ese comando, y si se logró la prensa, introduzca una vez más para continuar.

Seleccione la partición en la que instalar pfSense en la siguiente pantalla que aparece. Si los valores por defecto se utilizaron como se sugiere, no es probable que sólo una opción. Si aparecen varias opciones, elija la

que se creó para pfSense. Otra ventana de confirmación de presentación de informes del éxito del proceso de formateo.

Subparticiones ahora se pueden crear, pero de nuevo los valores por defecto en esta pantalla será aceptable para casi todos los usos. Algunas personas prefieren tener subparticiones separado para `/ Var`,`/ Tmp`, Y así sucesivamente, pero
esto no es necesario, y no debe hacerlo a menos que tenga un conocimiento considerable de los requisitos de espacio específico para su instalación. Si va a realizar una instalación completa de flash los medios de comunicación como base una tarjeta CF o disco USB, asegúrese de retirar la `de intercambio` partición. Hacer
los cambios deseados, a continuación, seleccione Aceptar y Crear.

Ahora siéntese y espere, espere, y tienen unos pocos sorbos de café mientras que el proceso de instalación de copias pfSense
a la ubicación de destino. Después de que el proceso de instalación ha finalizado su trabajo, hay una indicación final para seleccionar el kernel para instalar en el sistema de destino. Hay cuatro opciones disponibles, cada uno con sus propios fines:

Kernel tipo	Objetivo / Descripción
Multiprocesamiento simétrico del núcleo	Se utiliza para los sistemas que tienen varios núcleos o procesadores.
Núcleo monoprocesador	Se utiliza para los sistemas que tienen un solo procesador
Embebido núcleo	Deshabilita VGA de la consola y el teclado, usa consola serie.
Los desarrolladores del kernel	Incluye opciones de depuración útil para los desarrolladores.

Tabla 3.1. Las opciones del kernel

En caso de duda, ya sea el núcleo monoprocesador (UP) o el núcleo de multiprocesamiento simétrico (SMP) debería funcionar, sin importar el número de procesadores disponibles. Hay temas poco frecuentes en cierto hardware, independientemente del número de procesadores, no funcionará de forma fiable, o en absoluto con el núcleo monoprocesador, pero funciona bien con el kernel SMP, así como viceversa. En caso de que problemas, intente cambiar su núcleo de leche desnatada en polvo a monoprocesador o viceversa.

Cuando la instalación haya finalizado, seleccione Reiniciar y, a continuación, una vez reiniciado el sistema, quite el CD antes de que el proceso de arranque comienza.

Felicidades, pfSense está totalmente instalado!

3.3. Embebido de instalación

La versión incorporada se lanza como una imagen de disco, que debe ser escrito a una Compact Flash tarjeta (CF) physdiskwrite utilizando o dd. Después de la imagen está escrito, que se coloca en la meta dispositivo y configurar.

Nota

Tenga mucho cuidado al hacer esto! Si se trata de ejecutar esto en una máquina que contiene

otros

unidades de disco duro es posible seleccionar la unidad equivocada y sobrescribir una parte de ese unidad con pfSense. Esto deja el disco completamente ilegible, salvo para ciertos programas de recuperación de disco, y que es golpeado y se pierda en el mejor. physdiskwrite para Windows contiene una revisión de seguridad que no permite sobrescribir una unidad más grande de 800 MB sin una opción específica en la línea de comandos. La manera más segura de instalar pfSense a un CF es a través de la redirección de USB con VMware, discutido más adelante en este capítulo en la instalación de técnicas alternativas para la sección (Sección 3.4, "Instalación Alternativa Técnicas ").

Una vez más, sea muy cuidadoso al hacer esto! Hago hincapié en esto porque sé de varios personas que han escrito mal un disco y sobrescribe el disco duro. Esto puede suceder a nadie, incluido el otro fundador de pfSense, que accidentalmente sobrescribió su 1 TB de datos de unidad en lugar de su CF con una imagen de pfSense.

3.3.1. Instalación incorporado en Windows

El programa physdiskwrite por Manuel Kasper, autor de m0n0wall, es el medio preferido de la escritura de la imagen pfSense a CF en Windows. Puede ser descargarse del sitio web m0n0wall [http://m0n0.ch/wall/physdiskwrite.php]. Guárdelo en algún lugar de la PC en uso, tales como `C: \ Herramientas` u otra ubicación conveniente. Si se elige otra ubicación, sustituya `C: \ herramientas` en el ejemplo con el directorio en el `physdiskwrite.exe` se ha colocado.

Nota

También hay disponible una interfaz gráfica de usuario para physdiskwrite llamado PhysGUI, pero sólo el versión disponible de este escrito fue en alemán. Dicho esto, la interfaz gráfica de usuario es simple suficiente para el uso que puede que no sea una barrera para muchas personas. De hecho, puede resultar más fácil de usar, incluso en un idioma extranjero, que la versión de línea de comandos se encuentra en Inglés. Por ejemplo, la identificación de los dispositivos adecuados es una tarea mucho más simple. Es También están disponibles en el sitio web de m0n0wall.

En Windows Vista o Windows 7, physdiskwrite debe ser lanzado desde un símbolo del sistema de ejecución como administrador. Simple hecho de tener derechos de administrador no es suficiente. La forma más sencilla de hacer esto
es hacer clic en el botón Inicio, a continuación, escriba **cmd** en el cuadro de búsqueda. Haga clic en `cmd.exe` cuando
aparece y seleccione Ejecutar como administrador. El programa physdiskwrite continuación, se puede ejecutar desde que el símbolo del sistema sin ningún problema. Ejecutarlo desde un símbolo del sistema que no ha
ejecutar como administrador se dará lugar a ningún disco que se encuentra.
Para utilizar physdiskwrite, en primer lugar iniciar un símbolo del sistema.

A continuación, cambie al directorio que contiene `physdiskwrite.exe` y ejecutarlo seguido por el ruta de acceso al `pfSense.img.gz` archivo descargado antes. Después de ejecutar el comando, un mensaje con una lista de unidades conectadas al sistema aparecerá. La manera más segura para garantizar la unidad correcta es elegido sería ejecutar physdiskwrite antes de insertar el registro CF, la salida, a continuación, pulse Ctrl + C para salir. Inserte la tarjeta CF y ejecutar physdiskwrite nuevo, comparar la salida a la anterior de ejecución. El disco se muestra ahora que no se había demostrado es la fibrosis quística. El número de cilindros ("Cilindros" de la producción physdiskwrite) también se puede utilizar para ayudar a indicar la unidad apropiada. Los 512 MB
CF utilizado en el ejemplo siguiente se cuenta con 63 cilindros, mientras que los discos duros tienen más de 30.000. Asimismo, recuerda que physdiskwrite tiene un mecanismo de seguridad que no se sobreponen a un disco más grande
de 2 GB, sin especificar `-U` después del comando physdiskwrite.
Tras seleccionar el disco a escribir, physdiskwrite a escribir la imagen. Esto tomará entre de dos a diez minutos en una máquina rápida con USB 2.0 y USB 2.0 escritor CF. Si el sistema o escritor de CF es sólo USB 1.1, esperamos que tome varias veces más largo debido a la velocidad muy baja de USB 1.1.
El siguiente es un ejemplo práctico del uso de physdiskwrite para escribir una imagen pfSense.

```
Microsoft Windows [Versión 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. Todos los derechos reservados.

C: \ Windows \ system32> cd \ tools

C: \ Herramientas> physdiskwrite.exe c: \ temp \ pfSense-1.2.3-nanobsd-512M.img.gz

physdiskwrite v0.5.1 por Manuel Kasper <mk@neon1.net>

La búsqueda de unidades físicas ...

Información para \ \ \ PhysicalDrive0.:
   Windows: cilindros: 36481
                    TPC: 255
                    SPT: 63
```

```
Información para \ \ \ PhysicalDrive1.:
   Windows: cilindros: 30401
                  TPC: 255
                  SPT: 63

Información para \ \ \ PhysicalDrive2.:
   Windows: cilindros: 63
                  TPC: 255
                  SPT: 63

Información para \ \ \ PhysicalDrive3.:
DeviceIoControl () falló en \ \. \ PhysicalDrive3.

Información para \ \ \ PhysicalDrive4.:
DeviceIoControl () falló en \ \. \ PhysicalDrive4.

Información para \ \ \ PhysicalDrive5.:
DeviceIoControl () falló en \ \. \ PhysicalDrive5.

Información para \ \ \ PhysicalDrive6.:
   Windows: cilindros: 30515
                  TPC: 255
                  SPT: 63

Información para \ \ \ PhysicalDrive7.:
   Windows: cilindros: 0
                  TPC: 0
                  spt: 0

Qué disco quieres escribir? (0 .. 7) 2
Acerca de sobreescribir el contenido del disco 2 con nuevos datos. ¿Desea
continuar? (Y / n) y
Que se encuentran comprimidos archivo de imagen
122441728 / 122441728 bytes escritos en total

C: \ Herramientas>
```

Después de physdiskwrite ha completado, el CF se puede quitar de la escritora y se coloca en el objetivo de hardware.

Nota

El escrito contiene CF BSD particiones formateadas sistema de archivos que no se pueden leer en Windows. Windows reclamará la unidad necesita ser formateado debe intentar para acceder a ella. No hacerlo, sólo tiene que mover el CF para el hardware de destino. No hay manera de ver el contenido del escrito CF en Windows.

3.3.2. Instalación incorporado en Linux

instalación incorporado en Linux se logra por medio de tuberías gunzip la salida de la imagen a dd.

#pfSense gunzip-c-1.2.3-nanobsd.img.gz | dd of = / dev / hd*X* bs = 16k

donde *X* especifica el nombre del dispositivo IDE de la tarjeta CF o disco IDE (consulte con **hdparm - i / dev / hd*X***) - Algunos adaptadores, en particular, USB, pueden aparecer bajo emulación SCSI como `/ dev / sd`*X*.

No haga caso de la advertencia sobre la final de basura - que es por la firma digital.

3.3.3. Instalación integrado en FreeBSD

gzip hilo a dd a escribir la imagen a CF en FreeBSD. Antes de empezar, tendrá que conocer el nombre del dispositivo que corresponde a la tarjeta CF en uso. Si CF un disco duro o-a-IDE adaptador se utiliza, puede ser un `anuncios` dispositivo, como `ad0`. Compruebe la salida de dmesg o `/ var / log / messages`. Si un lector USB CF se está utilizando, puede ser una `da` dispositivo, como `da0`,
de verificación `/ Var / log / messages` después de conectar el lector de tarjetas, se debe informar que el dispositivo
Se añadió.

Para la imagen de la tarjeta, usted debería ser capaz de descomprimir la imagen y copiarla a la tarjeta en un solo paso:

#pfSense gzip-dc-1.2.3-nanobsd.img.gz | dd of = / dev /*AdX* obs = 64k

No haga caso de la advertencia sobre la final de basura - que es por la firma digital.

Si la imagen se queda corta o errores después de sólo la transferencia de una pequeña cantidad de datos, es posible
necesidad de descomprimir la primera imagen:

#gunzip pfSense-1.2.3-nanobsd.img.gz
#dd if = pfSense-1.2.3-nanobsd.img of = / dev /*AdX* obs = 64k

3.3.4. Instalación incorporado en Mac OS X

Este proceso ha sido probado en Mac OS X 10.3.9 y versiones posteriores, hasta e incluyendo la nieve Leopard/10.6. Se recomienda que desconecte todos los discos, excepto para el disco de inicio antes de llevar a cabo este procedimiento, como un error en la especificación de la unidad que se escriben podrían ocasionar que los datos pérdida.

• Conecte su lector de CF con la tarjeta CF insertada.

• Si el Mac OS X aparece un mensaje diciendo que la tarjeta no se puede leer, haga clic en Ignorar.

• Abrir Utilidad de Discos.

• Seleccione las particiones de tu tarjeta CF que se montan, y haga clic en el botón de desmontar. La particiones debe aparecer ahora en gris.

• Seleccione el lector de tarjetas CF en la columna de la izquierda, y haga clic en el botón de información.

• Tenga en cuenta el "Identificador de disco: por ejemplo, 'Disk1.

• Abre Terminal.

• Vaya al directorio que contiene la imagen pfSense.

• Utilice este comando, en sustitución de *disco [n]* con el disco de identificador que se encuentran por encima de:

#gzcat pfSense-1.2.3-nanobsd.img.gz | dd of = / dev /*disco [n]* bs = 16k

También existe la siguiente alternativa para lograr esto por completo de la línea de comandos.

$lista diskutil

```
/ Dev/disk0
  #: TAMAÑO TIPO NOMBRE DE IDENTIFICACIÓN
  0: GUID_partition_scheme * 298.1 Gi disk0
  1: EFI 200.0 Mi disk0s1
  2: Apple_HFS Macintosh HD 297.8 Gi disk0s2
/ Dev/disk1
  #: TAMAÑO TIPO NOMBRE DE IDENTIFICACIÓN
  0: CD_partition_scheme 30 días a Gran Francés * 521.4 Mi disk1
  1: CD_DA 7.8 Mi disk1s1
  2: CD_DA 7.8 Mi disk1s2
  3: 18,2 CD_DA Mi disk1s3
  4: CD_DA 13.8 Mi disk1s4
  5: CD_DA 14.0 Mi disk1s5
```

```
  6: CD_DA 12.1 Mi disk1s6
  7: CD_DA 14.2 Mi disk1s7
  8: CD_DA 21.5 Mi disk1s8
  9: CD_DA 16.6 Mi disk1s9
 10: CD_DA 14.7 Mi disk1s10
 11: CD_DA 24.3 Mi disk1s11
 12: CD_DA 16.6 Mi disk1s12
 13: CD_DA 22.4 Mi disk1s13
 14: CD_DA 14.7 Mi disk1s14
 15: CD_DA 20.5 Mi disk1s15
 16: CD_DA 19.4 Mi disk1s16
 17: CD_DA 15.3 Mi disk1s17
 18: CD_DA 17.9 Mi disk1s18
 19: CD_DA 18.2 Mi disk1s19
 20: CD_DA 16.0 Mi disk1s20
 21: CD_DA 26.8 Mi disk1s21
 22: CD_DA 18.8 Mi disk1s22
 23: CD_DA 21.7 Mi disk1s23
 24: CD_DA 14.5 Mi disk1s24
 25: CD_DA 22.2 Mi disk1s25
 26: CD_DA 16.7 Mi disk1s26
 27: CD_DA 20.9 Mi disk1s27
 28: CD_DA 16.0 Mi disk1s28
 29: CD_DA 20.8 Mi disk1s29
 30: CD_DA 17.1 Mi disk1s30
/ Dev/disk2
  #: TAMAÑO TIPO NOMBRE DE IDENTIFICACIÓN
  0: GUID_partition_scheme * 90.0 Mi disk2
  1: Apple_HFS Procesamiento de 90.0 Mi disk2s1
/ Dev/disk3
  #: TAMAÑO TIPO NOMBRE DE IDENTIFICACIÓN
  0: FDisk_partition_scheme * 978.5 Mi disk3
  1: DOS_FAT_32 UNTITLED 978.4 Mi disk3s1
```

$diskutil umount disk3s1

$gzcat pfSense-embedded.img.gz | dd of = / dev/disk3s1 bs = 16k

```
7665 registros en un
7665 un registro de
125587456 bytes transferidos en 188.525272 secs (666157 bytes / seg)
```

3.3.5. Finalización de la instalación incorporado

Ahora que el CF contiene una imagen de pfSense, puede ser colocado en el dispositivo de destino, pero todavía puede
necesita alguna configuración. Los usuarios de Alix y Soekris 5501 hardware puede saltarse esta sección, como que utilizan vr (4) controladores en red, y supone la instalación por defecto implícitos que vr0 es LAN y WAN es VR1. Estos puertos deben estar etiquetados en el hardware. Si desea volver a asignar estas interfaces de la consola en lugar de la WebGUI, seguir adelante.

3.3.5.1. Conecte un cable serie

En primer lugar, una módem nulo [http://en.wikipedia.org/wiki/Null_modemcable serie] debe estar conectado entre el dispositivo y una PC. Dependiendo del puerto serie y cable que se utiliza, un cable serie cambiador de género [http://en.wikipedia.org/wiki/Gender_changer] También puede ser necesario para que coincida con los puertos disponibles. Si un cable de módem nulo de serie real no está disponible, también hay de módem nulo adaptadores que convierten un cable serie estándar en un cable de módem nulo.

3.3.5.2. Inicie un cliente de serie

En el PC se utiliza para configurar el dispositivo incorporado, un programa cliente de serie debe ser utilizado. Algunos clientes son populares para Windows Hyperterminal, que debería estar en casi cualquier XP instalación, y PuTTY [Http://www.chiark.greenend.org.uk/ ~ sgtatham / masilla /], Que es gratuito y mucho más fiable. En Linux, `minicom` deben estar presentes la mayoría en el paquete de distribución sistemas. En FreeBSD, utiliza el incorporado en el programa `punta`. Escribiendo **punta com1** se conectará para el primer puerto serie. Desconecte escribiendo "**~.**"Al principio de una línea.

Cualquiera que sea el cliente de serie, se procurará que se establece para la velocidad adecuada (9600), Bits de datos (8), Paridad (n), y los bits de parada (1). Normalmente, esto se escribe como 9600/8/N/1. Algunas unidades incrustado por defecto a una velocidad más rápida. PC Motores WRAP y por defecto ALIX a 38400/8/N/1 y Soekris por defecto de hardware para 19200/8/N/1. Muchos clientes por defecto de serie para 9600/8/N/1, por lo que la adaptación de éstas
configuración puede no ser necesario. Usted tendrá que utilizar 9600/8/N/1 con pfSense independientemente de la configuración de su hardware. Para el hardware con otras velocidades de 9600, es probable que desee cambia la velocidad de transmisión en 9600 en la configuración de la BIOS para que el BIOS y pfSense son accesibles con la misma configuración. Consulte el manual de su hardware para obtener información sobre la configuración de su velocidad de transmisión.

3.3.5.3. Asignar interfaces de red

Después de que el dispositivo está encendido y el proceso de arranque se ha iniciado, un mensaje aparecerá para VLAN y la asignación de interfaces de red. Este paso fue cubierto anteriormente bajo Sección 3.2.3, "Asignación de interfaces" para la detección automática, y más tarde en Sección 3.5.3.1, "Manualmente Asignación de interfaces " para la asignación manual de interfaces.

Una vez que las interfaces se les ha asignado, el sistema debe estar listo para configurar a través de la WebGUI.

3.4. Suplente técnicas de instalación

Esta sección describe algunos métodos alternativos de instalación que puede ser más fácil para algunos implementaciones.

3.4.1. Instalación con la unidad en un equipo diferente

Si es difícil o imposible para agregar una unidad de CD-ROM para el hardware de destino, otro sistema se puede utilizar para instalar pfSense en el disco duro de destino. El disco puede entonces ser trasladado a la máquina original.

Cuando se le solicite con `Asignar interfaces` durante el inicio del Live CD, seleccione **n** para VLANs y el tipo **salida** a asignar la interfaz LAN del sistema para pasar de asignación de interfaz. A continuación, proceder
a través de la instalación normalmente. Aparecerá un mensaje en el instalador para configurar la red configuración, y esto se puede omitir también. Después de la instalación, permiten que la máquina se reinicie y apagarlo, una vez que regresa a la pantalla del BIOS. Retire el disco duro de la instalación máquina y colocarla en el sistema de destino. Después del arranque, se le solicitará la asignación de interfaz y luego el resto de la configuración se puede realizar como de costumbre.

3.4.1.1. Error de inicio después de mudarse a la unidad de destino de la máquina

Si la máquina utilizada para realizar la instalación asignada la unidad con un nombre de dispositivo diferente el dispositivo de destino, el sistema se detiene el arranque en un `> Mountroot` del sistema. Esto puede suceder si la instalación se realizó con la unidad en el puerto IDE secundario y en el hardware de destino que reside en el puerto IDE primario. En el caso de VMware, el adaptador USB puede ser detectada como un dispositivo SCSI, mientras que el hardware de destino utiliza IDE.

Si este problema se encuentra, el sistema dejará de arrancar y se sientan en un `> Mountroot` del sistema, como en este ejemplo:

```
Timecounter "CET" frecuencia 431646144 Hz calidad 800
Timecounters marque todos los ms 10.000
Rápido IPsec: Procesamiento de iniciada la Asociación de Seguridad.
ad0: DN4OCA2A> <HMS360404D5CF00 3906MB en UDMA33 ata0-master
Tratando de montar la raíz de ufs: / dev /ad2s1a

Manual de sistema de archivos raíz de la especificación:
  <fstype>: <device> Monte <device> utilizando <fstype> sistema de
archivos
                        por ejemplo. ufs: da0s1a
```

```
  ? Lista válida dispositivos de disco de arranque
  <empty line> Cancelar entrada manual

> Mountroot UFS:ad0s1a
Tratando de montar la raíz de ufs: ad0s1a


    ___
 ___ / F \
/ P \ ___ / Sentido
\ ___ / \
    \ ___ /
```

El sistema está tratando de montar la unidad con el nombre de dispositivo incorrecto, como `ad2`. Una línea justo por encima de el `mountroot` sistema debe indicar la ubicación real de la unidad, tales como `ad0`. Para continuar con el proceso de arranque, escriba el nombre de dispositivo correcto. En este caso, **UFS:*ad0*s1a**. Basta con sustituir *ad0* en esa línea con el nombre del dispositivo de la unidad de disco duro, como se muestra por encima de este sistema. Tome nota de la nombre del dispositivo adecuado, ya que se necesitarán para el siguiente paso.

Ahora que el sistema ha arrancado, uno más el cambio es necesario. La tabla de sistema de archivos en `/ Etc / fstab` debe ser actualizada con el dispositivo apropiado. Para cambiar esto en el WebGUI, vaya a Diagnóstico → Editar el archivo y abra `/ Etc / fstab`. Reemplace cada instancia del nombre del dispositivo en ese archivo y guardar los cambios. Reiniciar el sistema para verificar el cambio.

Para quienes están familiarizados con las operaciones de línea de comandos, para cambiar esto en la línea de comandos elegir opción **8** una vez que la consola de cargas para entrar en el menú para iniciar una shell. En este ejemplo se utiliza el editor vi. Si vi no es una opción deseable, ee también está disponible y cuenta con ayuda en pantalla.

A continuación, introduzca el comando para editar el `fstab` archivo.

#vi / etc / fstab

El contenido del archivo aparecerá. Se verá algo como esto:

```
# Opciones de dispositivo Punto de montaje fstype dump pass #
/ Dev/ad2s1a / ufs rw 1 1
```

Haga los cambios necesarios. En este ejemplo, el dispositivo es incorrecta `ad2`, Esto debe ser cambiado a `ad0`:

```
# Opciones de dispositivo Punto de montaje fstype dump pass #
/ Dev/ad0s1a / ufs rw 1 1
```

Ahora guarda el archivo y salga del editor. (Esc, a continuación, **: Wq!** si vi fue utilizado.)

3.4.2. Instalación completa de VMware con USB redirección

Usted puede utilizar la redirección de USB en VMware Player y estaciones de trabajo para instalar un disco duro.

La mayoría de los adaptadores USB a IDE o SFF (Small Form Factor) IDE funciona para este propósito. La las instrucciones siguientes son específicas de VMware Workstation 6.0 y versiones anteriores.

- Crear un equipo virtual con redireccionamiento USB.
- Desconecte el escritor CF desde su PC.
- Conecte el CF / Microdrive CF en su escritor.
- Inicie la máquina virtual y haga clic en el interior de la máquina virtual para que tenga el foco.
- Conecte el escritor de CF en su PC. La máquina virtual se levante el dispositivo USB, y el pfSense CD de instalación reconocerá la tarjeta CF / Microdrive como un disco duro.
- Continúe con la instalación de la misma como una completa instalación normal.

En VMware Workstation 6.5, podrás ver un icono para cada dispositivo USB en la máquina a lo largo del parte inferior de la ventana de VMware. Haga clic en el dispositivo y haga clic en **Conecte (Desconecte de acogida)** para utilizarlo dentro de su máquina virtual. Consulte la documentación de VMware para más información en la redirección de USB.

3.4.3. Instalación incrustado en VMware con USB Redirección

La imagen incrustada puede escribirse también en VMware mediante su reorientación USB. Se trata de un seguro opción, ya que hace imposible para sobrescribir los discos en el host, lo que limita la posibilidad de daños lo que está en su máquina virtual. Para ello, basta con conectar el escritor de CF a la máquina virtual y realizar la instalación como lo haría en el mismo sistema operativo en una máquina física. Consulte el VMware documentación para obtener más información sobre la redirección de USB.

3.5. Solución de problemas de instalación

La gran mayoría de las veces, las instalaciones terminará sin problemas. Si los problemas surgen, la secciones siguientes se describen los problemas más comunes y las medidas adoptadas para resolverlos.

3.5.1. Arrancar desde el Live CD se produce un error

Debido a la amplia gama de combinaciones de hardware en uso, no es raro que un CD de arranque mal (o no). Los problemas más comunes y sus soluciones son:

Sucio CD-ROM	Limpie la unidad con un disco de limpieza o una lata de aire comprimido, o utilice otra unidad.
Media Bad CD-R	Grabar otro disco y / o grabar el disco a una velocidad inferior. Tal vez pruebe con otra marca de medios de comunicación.
Cuestiones del BIOS	Actualizar a la última BIOS y deshabilitar cualquier innecesarios periféricos tales como Firewire, unidades de disquete, y audio.
Cuestiones cable IDE	Pruebe con otro cable IDE entre la unidad de CD-ROM y el IDE Controlador o placa base
Problemas de arranque del cargador	Ha habido casos donde las versiones específicas de los CD de FreeBSD gestor de arranque no funciona en algunos sistemas. En este caso, consulte la sección anterior sobre cómo realizar la instalación en un disco duro PC por separado y luego pasar al sistema de destino.

Hay más técnicas de solución de problemas que aparecen en la documentación pfSense Wiki en Solución de problemas de arranque [Http://doc.pfsense.org/index.php/Boot_Troubleshooting].

3.5.2. Arrancar desde el disco duro después de la instalación de CD no

Después de que el CD de instalación completa y se reinicia el sistema, hay algunas condiciones que puede impedir que pfSense plenamente el arranque. Las razones más comunes suelen ser BIOS o duro variador de velocidad relacionados. Algunos de estos puede resolverse eligiendo diferentes opciones para el gestor de arranque durante el proceso de instalación, activar / desactivar el modo de paquetes, o mediante la instalación de

una tercera parte del gestor de arranque como GRUB[1]. Actualización de la BIOS a la última versión disponible También puede ayudar en este caso.

La alteración de las opciones de SATA en el BIOS ha mejorado el arranque en algunas situaciones también. Si un disco duro SATA se está utilizando, experimentar con cambiar las opciones de SATA en el BIOS para configuración, tales como AHCI, Legacy, o IDE.

1GRUB es un gestor de arranque con muchas características que soporta varios sistemas operativos, los medios de arranque, y sistemas de archivos. Su página web es http://www.gnu.org/software/grub/.

Al igual que en la sección anterior, hay más técnicas de solución de problemas enumerados en el la documentación en línea en Solución de problemas de arranque [Http://doc.pfsense.org/index.php/Boot_Troubleshooting].

3.5.3. Interfaz de enlace no se detectó hasta

Si el sistema se queja de que la interfaz de enlace hasta que no se detecta, en primer lugar asegurarse de que el cable esté desconectada y que la interfaz no tiene luz de enlace antes de la elección de la detección de vínculos opción. También es posible que desee probar o reemplazar el cable en cuestión. Después de seleccionar la opción, enchufe el cable de nuevo en la interfaz y asegúrese de que tiene una luz de enlace antes de pulsar Intro.

Si un cable de red está conectado directamente entre dos sistemas y no con un interruptor de garantizar, que un cable cruzado [] Http://en.wikipedia.org/wiki/Ethernet_crossover_cable se está utilizando. Algunos adaptadores nuevos pueden apoyar Auto-MDIX [http://en.wikipedia.org/wiki/Auto-MDIX] Y se encargará de esto internamente, pero muchos adaptadores más viejos no. Del mismo modo, si la conexión de un pfSense sistema a un switch que no soporta Auto-MDIX, utilice un cable de conexión directa parche.

Si la interfaz está conectado correctamente, pero pfSense aún no detecta el enlace hasta el interfaces de red se utiliza no detecta correctamente enlace por alguna razón. En este caso, asignar manualmente las interfaces es necesario.

3.5.3.1. La asignación manual de interfaces

Si la función de detección automática no funciona, todavía hay esperanza de decir la diferencia entre tarjetas de red antes de la instalación. Una forma es mediante la dirección MAC, que debe ser mostrado al lado a los nombres de interfaz en la pantalla de asignación:

```
le0 08:00:27:26: a4: 04
le1 08:00:27:32: CE: 2f
```

La dirección MAC es a veces impreso en una pegatina en algún lugar físicamente en la tarjeta de red. Las direcciones MAC también se asignan por el fabricante, y hay varias bases de datos en línea que le permitirá hacer una búsqueda inversa de una dirección MAC con el fin de encontrar la empresa que hizo la tarjeta.[2]

Las tarjetas de red de diferentes marcas, modelos o conjuntos de chips a veces se pueden detectar con diferentes conductores. Puede ser posible decir una tarjeta Intel utilizando el `fxp` además de un controlador Realtek tarjeta con la `rl` conductor mirando a las propias tarjetas y la comparación de las denominaciones en el circuito.

2http://www.8086.net/tools/mac/, http://www.coffer.com/mac_find/, Y http://aruljohn.com/mac.pl, entre muchos otros.

Una vez que se determina que la tarjeta de red se utilizará para una determinada función, escriba en la interfaz de
pantalla de asignación cuando se le solicite. En el ejemplo anterior, `le0` se WAN y `le1` será
LAN. Cuando se le pida primero para la dirección de LAN, se haría **le1** y pulse Enter. A continuación,
cuando se le pida la WAN, el tipo **le0**, Y pulse Enter. Dado que no existen interfaces opcionales, un
más prensa de entrar, a continuación, **y** completará la tarea. En casi todas las PC de torre, la más alta
ranura PCI será la primera tarjeta de red, ordenados secuencialmente en orden de arriba hacia abajo. Cuando tienes tres
Intel `fxp` tarjetas en un sistema, la tarjeta de red superior es normalmente `fxp0`, El uno por debajo de ese `fxp1`, Y el
más baja `fxp2`. Esto depende de la placa base, pero casi siempre es cierto. Si
tener una tarjeta de red a bordo que es la misma marca como un complemento de la NIC, tenga en cuenta que algunos sistemas se
lista de la tarjeta a bordo en primer lugar, y otros no.

3.5.4. Solución de problemas de hardware

Si tiene problemas con el hardware que está intentando utilizar, las siguientes sugerencias
ayudará a resolver en muchos casos.

3.5.4.1. Quitar hardware innecesario

Si el sistema contiene todo el hardware que no se utilizará, retírelo. Por ejemplo, si usted tiene
reasignan un escritorio antiguo con una tarjeta de sonido, retire la tarjeta de sonido. Esto normalmente no es un
problema, pero puede causar problemas y tiene el potencial de reducir el rendimiento. Si es desmontable y
no lo necesita, se lo quita.

3.5.4.2. Deshabilitar PNP OS en la BIOS

Esta es la solución más común para los problemas de hardware. Muchas pantallas de configuración del BIOS se
tienen una configuración de PNP OS o sistema operativo Plug and Play, que se debe establecer en **desactivar** o **No**. Algunos
tienen una configuración para el sistema operativo, que por lo general se debe establecer en **otros**.

3.5.4.3. Actualización de la BIOS

La corrección de segundo más común de problemas de hardware es actualizar la BIOS a la última
revisión. La gente parece tener dificultades para creer esto, pero confía en mí, sólo hazlo. BIOS
actualizaciones comúnmente corregir errores en el hardware. No es raro que se encontró con problemas inducidos por
errores de hardware en sistemas que tienen estable ejecutar Windows desde hace años. Supongo que cualquiera de las ventanas
no provoca el error, o tiene un trabajo en torno, como yo personalmente he visto esto en múltiples ocasiones.
Las cosas que la actualización del BIOS puede solucionar incluyen la falta de arranque, tiempo de mantenimiento de los problemas, y en general
la inestabilidad, entre otros.

3.5.4.4. Restablecer la configuración del BIOS a los valores de fábrica

Algunos sistemas de reciclado puede tener una atípica configuración del BIOS de su uso anterior. La mayoría de
contiene una opción que le permite restablecer todos los ajustes a los valores de fábrica. Trate de hacer esto. También de verificación Sección 3.5.4.2, "Deshabilitar PNP OS en la BIOS" de nuevo después de hacer esto.

3.5.4.5. Deshabilitar hardware no utilizado en la BIOS

Si la placa tiene integrado en los componentes que no se utilizará, trate de desactivar.
Los ejemplos más comunes incluyen el puerto paralelo, modems a bordo, los dispositivos de audio, Firewire, posiblemente USB y los puertos serie a menos que usted planea usar una consola serie.

3.5.4.6. Otras configuraciones de BIOS

Si su BIOS permite la configuración de administración de energía, trate de apagar o en. Puedes buscar cualquier cosa cosa que parece pertinente y tratar de cambiar algunas cosas. Si llegas a este punto, el hardware es probablemente una causa perdida y debe buscar alternativas de hardware. También puedes ver para ver si su BIOS tiene un registro de eventos que puede enumerar los errores de hardware, tales como fallas de prueba de memoria.

3.5.4.7. Otros problemas de hardware

También podría haber algún problema con el hardware de destino, que las pruebas de diagnóstico con software puede revelar. Debe probar el disco duro con software de diagnóstico del fabricante, y poner a prueba la memoria con un programa como el memtest86 +. Estas y más herramientas están disponibles en el "Ultimate Boot CD [http://www.ultimatebootcd.com/] ", Que se carga con muchas herramientas gratuitas de diagnóstico de hardware.
También asegúrese de que todos los fans están girando a gran velocidad, y que no son componentes de un sobrecalentamiento.
Si se trata de volver a utilizar hardware antiguo, algunos comprimidos / aire comprimido de limpieza de los ventiladores y disipadores de calor
puede hacer maravillas.

3.5.5. Problemas de arranque incrustado en el hardware ALIX

Si un sistema embebido no arranca correctamente, conecte un cable de serie para el dispositivo y el monitor el proceso de arranque en busca de pistas sobre cómo proceder. El problema más común serán los usuarios tanto de ALIX hardware. Si está utilizando una tarjeta ALIX, usted tendrá que asegurarse de que el BIOS más reciente disponible en el momento de escribir esto, 0.99h, se carga en el tablero con el fin de arrancar de forma adecuada NanoBSD imágenes de ambos sectores.
Un ALIX en la necesidad de una actualización del BIOS normalmente presentan los siguientes síntomas en el arranque:

```
PC Motores ALIX.2 v0.99
640 KB de memoria base
261.120 KB de memoria ampliada

01F0 Maestro 848A SanDisk SDCFH2-004G
Phys. C / H / S 7964/16/63 C Entrar / H / S 995/128/63

Un FreeBSD
2 FreeBSD

Arranque: 1 ############
```

El número de marcas de almohadilla (#) poco a poco crecerá con el tiempo como el arranque intenta continuar. Si este
comportamiento se ve, siga los procedimientos de actualización del BIOS de su proveedor de por lo menos la versión 0.99h

Además de necesitar la versión 0.99h BIOS, el BIOS también se debe establecer para el modo CHS (cilindro / Jefe / Sector modo para hacer frente a los datos en un disco), como en el ejemplo siguiente:

```
PC Motores ALIX.2 v0.99h
640 KB de memoria base
261.120 KB de memoria ampliada

01F0 Maestro 848A SanDisk SDCFH2-004G
Phys. C / H / S 7964/16/63 C Entrar / H / S 995/128/63

Configuración de la BIOS:

* 9 * 9600 (2) 19 200 baudios (3) 38 400 baudios (5) 57 600 baudios (1)
115.200 baudios
* C * CHS modo (L) el modo LBA (W) disco duro de espera (V) del disco duro
esclavo (U) UDMA permiten
(M) MFGPT solución
(P) a finales de inicio PCI
* R * de serie de la consola permiten
(E) de arranque PXE permiten
(X) Xmodem subir
(Q) Salir
```

Para llegar a esta pantalla, pulse **S** mientras que la prueba de memoria se muestra en la consola serie. A continuación,
prensa **C** para cambiar al modo CHS, a continuación, pulse **Q** dejar de fumar.

~~En este punto el ALIX debe arrancar de forma adecuada ya sea de corte de una imagen de Nano~~BSD.

3.6. Recuperación de instalación

Hay dos escenarios principales para la necesidad de reinstalar el sistema. En el primer caso, un disco duro o dispositivo de almacenamiento masivo puede haber fallado y un rápido instalar con una configuración de copia de seguridad es necesario.
En el segundo caso, la configuración sigue presente en el disco duro, pero algunos de los contenidos de el sistema de archivos puede estar dañado. pfSense ofrece un proceso fácil y relativamente sin dolor para recuperando rápidamente de este tipo de problemas, y si ninguno de estos escenarios se aplica entonces hay siempre el método tradicional de la restauración de una configuración desde dentro de la WebGUI.

3.6.1. Instalador de pre-vuelo Recuperación de la configuración

pfSense tiene, como parte de la rutina de instalación, un "pre-vuelo Instalar" o PFI. PFI se busca una configuración existente en una unidad USB y usarlo en lugar de pedir una nueva configuración.
Al instalar un disco duro, el programa de instalación copia esta configuración. Cuando el se complete el proceso, se reiniciará con el archivo de configuración restaurada.

En primer lugar, localizar una unidad USB que es el formato FAT. Si funciona en Windows, es probable que ya FAT formato.

Cree un directorio en la raíz de esta unidad USB llamada `conf`.

Coloque un archivo de configuración en esta carpeta. Si la copia de seguridad provenía de el pfSense WebGUI, lo más probable es nombrado como el siguiente: `config-routerhostname.example.com-20090520151000.xml`. Cambiar el nombre de este archivo para `config.xml`. Para obtener más información sobre cómo realizar copias de seguridad, consulte Capítulo 5, Backup y Recuperación.

La unidad ahora debe estar listo para su uso. Para corroborar que la configuración es en el lugar correcto, el archivo debe estar en *E*`: \ Conf \ config.xml` si la unidad USB *E:*. Sustituir el caso letra de unidad para el sistema que se utiliza.

Extraiga la unidad USB de la estación de trabajo, y luego enchúfelo en el sistema de pfSense se restaurado. Ponga el CD en vivo en su unidad de CD-ROM, y arrancar el sistema. Debe ser evidente que el sistema utilizado la configuración de la USB y no del sistema para configurar las interfaces.
Lo único que queda por hacer es seguir los pasos descritos en Sección 3.2.4, "Instalación del disco duro Drive " para realizar una instalación normal en un disco duro.

Cuando la instalación haya finalizado, apagar el sistema, desenchufe la unidad USB, y retire el CD de instalación. Encienda el sistema de nuevo, y debería arrancar con normalidad y estar en pleno funcionamiento. Si los paquetes estaban en uso, puede visitar los WebGUI y después de la entrada que se volverá a instalar automáticamente.

Nota

Tenga cuidado al quitar una unidad USB de un sistema de pfSense. Siempre es
más segura de hacerlo cuando el poder está apagado. Si la unidad USB se monta por una
que ejecutan el sistema pfSense y quitar sin desmontar, el sistema se bloqueará
y reiniciar el sistema con resultados posiblemente impredecibles. FreeBSD es incapaz de perder
Actualmente los sistemas de ficheros montados sin inducir el pánico. Esto ya no será un
tema en FreeBSD 8.0.

3.6.2. Recuperación de la configuración instalada

Si partes de la instalación en el disco duro no está trabajando (como resultado de un error de actualización o
otra causa), la configuración se puede conservar al mismo tiempo acabando con el resto de los archivos instalados.

Durante el proceso de instalación, antes de elegir pfSense instalación hay una opción del menú marcada Rescate
config.xml. Cuando se elige esta opción, la configuración se puede seleccionar desde cualquier almacenamiento masivo
los medios de comunicación relacionada con el sistema. El proceso de instalación se carga esta configuración, y una vez
la reinstalación completa, el sistema va a correr con la configuración de rescatados.

3.6.3. WebGUI recuperación

Si todo esto falla, procederá a efectuar una instalación normal, como se describe anteriormente en este capítulo a

continuación, restaurar
la configuración antigua visitando Diagnóstico → Copia de seguridad / restauración en la red una vez WebGUI
conectividad ha sido restaurada. En el área Restaurar configuración de la página, haga clic en Examinar,
encontrar el archivo de copia de seguridad de configuración. Una vez localizado, haga clic en Abrir y, finalmente, haga clic en Restaurar
De configuración. La configuración será restaurada y el sistema se reiniciará automáticamente. Después de
reiniciar el sistema, la configuración completa debe estar presente. Este proceso se describe con mayor detalle en
Sección 5.5, "La restauración de copias de seguridad".

3.7. Actualizar una instalación existente

Los medios de apoyo de la mejora de la liberación pfSense a otro dependerá de la plataforma
que se utiliza. En la mayoría de los casos, pfSense puede ser fiable actualizar a cualquier otra versión sin perder
la configuración existente.

Al mantener un sistema de pfSense actualizado con una versión actual apoyo, que nunca será obsoleto.
Las nuevas versiones se liberan periódicamente que contienen nuevas características, actualizaciones, corrección de errores, y varios
otros cambios. En la mayoría de los casos, la actualización de una instalación de pfSense es muy fácil. Si actualizas a una
nueva

liberación que es un sólo un punto de desenganche (por ejemplo, 1.2.2 a 1.2.3), la actualización debe ser mínimamente invasiva

y es improbable que cause problemas. El problema más común es la regresión específicos del hardware de una versión de FreeBSD a otro, aunque esto sea muy poco frecuente. Actualización versiones fijar más hardware que se rompen, pero regresiones son siempre posibles. Más grandes saltos, por ejemplo de 1.2.3 a 2.0 en el futuro debe ser manejado con cuidado, y lo ideal sería probado en hardware idéntico en una prueba el medio ambiente antes de su uso en la producción.

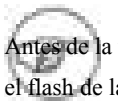
3.7.1. Hacer una copia de seguridad ... y un Plan de copia de seguridad

Lo primero es lo primero, antes de realizar cualquier modificación a un sistema de pfSense, es una buena idea hacer una copia de seguridad. En la WebGUI, visita de diagnóstico → Copia de seguridad / restauración. En la configuración de copia de seguridad sección de la página, asegúrese de que la zona de copia de seguridad se establece en **TODOS**, A continuación, haga clic en Descargar configuración.

Guardar este archivo en un lugar seguro, y no estaría de más hacer varias copias. Aquellos con un pfSense Portal [https: / / portal.pfsense.org /] suscripción debe considerar el uso de la configuración de copia de seguridad automática paquete, y hacer una copia de seguridad manual toma nota de la razón como antes de la actualización.

También puede ser una buena idea tener a mano para instalar los medios de comunicación la liberación actualmente en ejecución, en caso de que algo va mal y una reinstalación es necesario. Si eso ocurre, tiene el archivo de copia de seguridad en la mano y se refieren a la anterior Sección 3.6, "Instalación de Recuperación". También se refieren a Capítulo 5, Backup y Recuperación.

3.7.2. Actualización de una instalación incorporado



Antes de la versión 1.2.3, el único 100% garantizado manera confiable de actualización fue incorporado a la re-el flash de la FQ y restaurar una copia de seguridad de configuración anterior después. Este método todavía puede ser utilizado, pero, gracias a la nueva versión incrustada NanoBSD basado en el uso de la 1.2.3 hacia adelante actualizaciones fiables se puede realizar como una instalación completa. Continuará en la instalación completa instrucciones de actualización si ya está ejecutando la versión pfSense 1.2.3 o más reciente.

Nota

Si va a actualizar desde una versión anterior de pfSense hasta la versión 1.2.3, que se todavía tienen que reflash la tarjeta con una nueva imagen basada en NanoBSD. A partir de entonces se puede actualizar como de costumbre.

3.7.3. Actualización de una instalación completa

Hay varios métodos disponibles para la actualización de una instalación completa de pfSense. O bien el WebGUI o la consola se puede utilizar, y cualquiera de estos métodos tiene un medio de proporcionar una descarga archivo de actualización o tirar de una automáticamente desde Internet.

3.7.3.1. Actualización con la WebGUI

Hay dos opciones para actualizar utilizando la interfaz web, con el manual y automática actualización. En las secciones siguientes se describen estos métodos de actualización.

3.7.3.1.1. Manual de actualización de firmware

Con el fin de realizar una actualización manual del firmware, en primer lugar un archivo de actualización tendrá que ser descargado.

Examinar para http://www.pfsense.org y haga clic en el enlace de descarga. En la página de descargas, haga clic en el enlace de las actualizaciones. Esto llevará a la página de selección de espejo. Elija un espejo geográficamente cerca de su ubicación para un mejor rendimiento. Una vez que el espejo se ha seleccionado un directorio anuncio aparecerá con los archivos de actualización para la versión actual de pfSense. Descargue el `. Tgz` archivo, (Por ejemplo, `pfSense-Full-Update-1.2.3.tgz`) Y que acompaña a la `. Md5` archivo para verificar la descarga. Ver Sección 3.1.1, "Comprobar la integridad de la descarga" en MD5 para obtener detalles sobre cómo utilizar un `. Md5` archivo.

Para instalar el archivo de actualización, visite el pfSense WebGUI. Haga clic en Sistema → Firmware. Haga clic en Habilitar Cargar firmware. Haga clic en el botón Examinar situado junto al firmware de archivo de imagen. Busque la actualización archivo descargado en el paso anterior y haga clic en Abrir. Por último, haga clic en la actualización del Firmware botón. La actualización tendrá unos minutos para cargar y aplicar, en función de la velocidad de la conexión que se utiliza para la actualización y la velocidad del sistema de destino. El firewall se reiniciará automáticamente cuando haya terminado.

3.7.3.1.2. Actualización automática

Actualización automática es una característica nueva que pondrá en contacto con un servidor pfSense.com y determinar si hay es una versión más reciente en libertad que la que se ejecuta actualmente. Esta comprobación se realiza cuando se visite la página de actualizaciones automáticas que se encuentran bajo el Sistema → Firmware, haga clic en la actualización automática ficha en la WebGUI. Si hay una nueva actualización disponible, se mostrará. Haga clic en el botón para instalar el actualización. La actualización se tome unos minutos para descargar y aplicar, en función de la velocidad de la conexión a Internet utilizado y la velocidad del sistema de destino. El firewall se reiniciará automáticamente cuando haya terminado.

De forma predeterminada, la comprobación de actualización se refiere sólo a las versiones de pfSense lanzado oficialmente, pero es También es posible utilizar este método para realizar un seguimiento instantáneas también. La versión de actualización se puede cambiar visitando la ficha Configuración de actualización, que se encuentra inmediatamente a la derecha de la ficha de

actualización automática. Es
más seguro es utilizar las versiones oficiales, ya que ver la mayoría de las pruebas y debe ser razonablemente seguro y sin problemas. Sin embargo, como con cualquier actualización, primero debe visitar el sitio web de pfSense y lea las notas de actualización para esa versión.

3.7.3.2. Actualizar mediante la consola

Una actualización también puede ser ejecutado desde la consola. La opción de la consola está disponible en cualquier medio de acceso disponibles para la consola: Video / teclado, consola serie o SSH. Una vez conectado a la consola del sistema pfSense a ser rehabilitado, iniciar el proceso de actualización seleccionando la opción de menú **13**.

3.7.3.2.1. Actualizar desde una URL

Si la dirección URL completa a un archivo de actualización de pfSense se sabe, esta es una buena opción. Se evitará tener que primero descarga el archivo de actualización sólo para subirlo otra vez, ya diferencia de la característica Actualizaciones automáticas en la WebGUI también permite una ubicación de actualización del archivo de encargo para ser utilizado.

Desde el menú de la consola de actualización, seleccione la opción **1** para la actualización desde una dirección URL. Introduzca la dirección URL completa en el fichero de actualización, tales como:

```
http://files.pfsense.org/mirror/updates/pfSense-Full-
Update-1.2.3.tgz
```

Confirme que la actualización se debe aplicar, y entonces debería ser descargados y instalado. Una vez finalizada la instalación, el router se reiniciará automáticamente.

3.7.3.2.2. Actualización de un archivo local

Un archivo de actualización se puede descargar, como en el manual de actualización de firmware anterior, y luego se copia en el sistema de pfSense a través de scp o diagnósticos → Comando. Para instalar un archivo, desde la consola actualización del menú, seleccione la opción **2** para la actualización de un archivo local y, a continuación, escriba la ruta completa a la archivo que se ha subido, como `/ Tmp/pfSense-Full-Update-1.2.3.tgz`. Confirme que la actualización se debe aplicar, y entonces debe ser instalado de forma automática. Después de la instalación es completo, el router se reiniciará automáticamente.

3.7.4. La actualización de un Live CD de instalación

En un sistema por separado, descargar y quemar un CD que contiene la última versión. Asegúrese de que se han trasladado su configuración en un medio extraíble (USB o disquete) desde el menú de la consola (Véase el Sección 4.6.15, "Mover el archivo de configuración de dispositivo extraíble"). A continuación, reinicie el pfSense router y arrancar con el nuevo CD. Cuando las botas pfSense en el nuevo CD, el almacenamiento existentes

los medios de comunicación que contiene su configuración se encuentra y se utiliza.

Capítulo 4. Configuración

Después de la instalación, el router pfSense está listo para la configuración. La mayor parte de la configuración se realiza mediante el configurador de interfaz gráfica de usuario basada en web (webConfigurator), o WebGUI para abreviar. No
son algunas de las tareas que puede realizar fácilmente desde la consola, ya se trate de un monitor y teclado, más de un puerto serie, o a través de SSH. Algunos de ellos pueden ser necesarias antes de que usted pueda para acceder a la WebGUI, por ejemplo, si usted quiere traer a la LAN en una red LAN existente con una dirección IP diferente.

4.1. Conexión a la WebGUI

Con el fin de llegar a la WebGUI, debe conectarse desde otro PC. Este equipo podría estar directamente conectado con un cable cruzado, o conectados al mismo conmutador. De forma predeterminada, la IP LAN de un pfSense nuevo sistema es 192.168.1.1 con una máscara / 24 (255.255.255.0), y también hay un servidor DHCP servidor que ejecuta. Si el PC se utiliza para conectar se establece para obtener su dirección IP por DHCP, debe sólo una cuestión de apuntar su navegador web favorito para http://192.168.1.1.

Si necesita cambiar la dirección IP de la LAN o deshabilitar DHCP, esto se puede hacer desde la consola eligiendo la opción 2, a continuación, introduzca la nueva IP de LAN, máscara de subred, y especificar si desea o no activar DHCP. Si decide activar DHCP, también se le pedirá que introduzca el inicio y la
poner fin a la dirección del conjunto DHCP, lo que podría ser cualquier rango que, como en el interior de la subred determinada.

Cuando se deshabilita el servidor DHCP, debe asignar estáticamente una dirección IP en el pfSense subred de LAN del sistema en el PC se utiliza para la configuración, tales como *192.168.1.5*, Con una máscara de subred que coincide con la dada a pfSense, como 255.255.255.0.

Una vez que el PC está conectado a la misma LAN que el sistema de pfSense, vaya a la dirección IP de la LAN.

Nota

Tenga cuidado al asignar una nueva dirección IP LAN. Esta dirección IP no puede estar en el misma subred de la WAN o de cualquier otra interfaz activa.

4.2. Asistente para la instalación

Al navegar a la WebGUI, primero será recibido por un inicio de sesión del sistema. Por el nombre de usuario entrar **admin** y la contraseña, introduzca **pfSense**.

Dado que esta es la primera vez que visita la WebGUI, el asistente de configuración se iniciará automáticamente, y
se verá como Figura 4.1, "Asistente de configuración de inicio de la pantalla". Haga clic en Siguiente para iniciar la configuración
proceso.

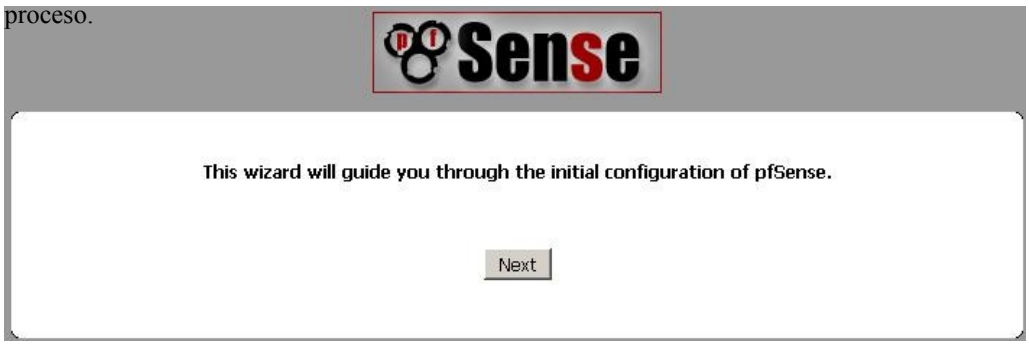


Figura 4.1. Asistente para la instalación de la pantalla Inicio

4.2.1. Pantalla de información general

La siguiente pantalla (Figura 4.2, "Pantalla de Información General") Le pedirá el nombre de este pfSense router, y el dominio en el que reside. El nombre de host puede ser cualquier cosa que te gusta, sino que debe comenzar con una letra, y luego puede contener letras, números, o un guión. Después de el nombre de host, escriba un dominio, por ejemplo, **example.com**. Si no tienes un dominio, puede utilizar ***<algo>*. Locales**, Donde <*algo*> es todo lo que quieras: un nombre de empresa, su apellido, apodo, y así sucesivamente. El nombre de host y el nombre de dominio se combinan para formar el nombre de dominio completo de su router.

El servidor DNS primario y el servidor DNS secundario puede ser llenado, si se conoce. Si usted está utilizando un tipo dinámico WAN como DHCP, PPTP o PPPoE, estos por lo general se asignado automáticamente por el ISP y puede dejarse en blanco. Estos tipos de WAN se explican en más detalle más adelante en el asistente de configuración. Haga clic en Siguiente cuando haya terminado.

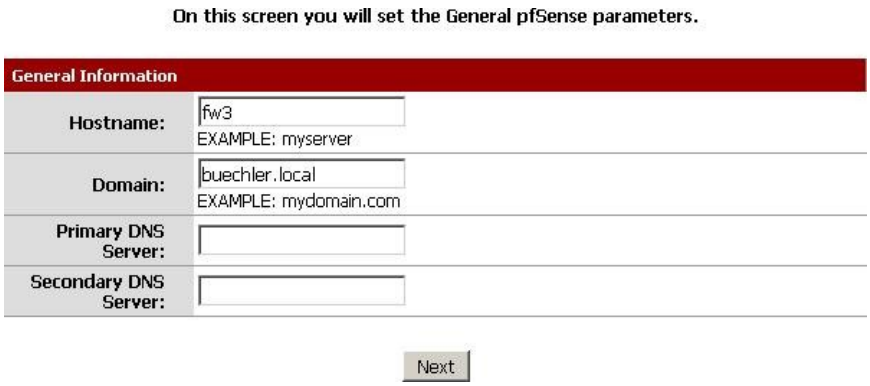


Figura 4.2. Pantalla de información general

4.2.2. NTP y Configuración del huso horario

La siguiente pantalla (Figura 4.3, "Zona de NTP y el tiempo de la pantalla de configuración") Tiene un lugar para una red
Time Protocol (NTP), y la zona horaria en la que este servidor reside. A menos que tenga una
preferencia específica por un servidor NTP como uno dentro de su LAN, lo mejor es dejar el Tiempo
servidor de nombre de host en el valor predeterminado **0.pfsense.pool.ntp.org**, Que recogerá los servidores al azar
de un grupo de hosts NTP en buen estado.

Para la selección de zona horaria, seleccione una zona geográficamente nombre que mejor coincide con el pfSense sistema de localización. No utilice el GMT (Greenwich Mean Time) compensar las zonas de estilo. Para obtener más información, consulte Sección 4.7.1, "Zonas de Tiempo" más adelante en este capítulo. Cuando termine, haga clic en Siguiente para continuar.

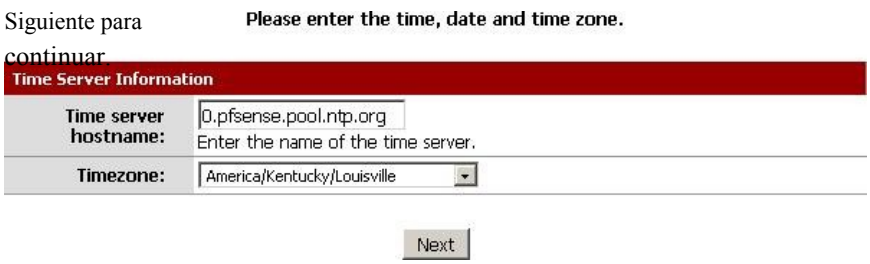


Figura 4.3. NTP y la pantalla de configuración de zona horaria

4.2.3. Configuración de WAN

Estos párrafos próximos y sus imágenes asociadas ayudará a guiar a través de la creación de la interfaz WAN en el sistema de pfSense. Dado que este es el lado que da a su ISP o aguas arriba router, hay opciones de configuración para el apoyo de varios tipos comunes de conexión ISP. La primera elección es para el tipo de WAN (Figura 4.4, "Configuración de la WAN"). Este debe coincidir con lo su ISP soporta, o lo que sea el router anterior se ha configurado para su uso. Entre las posibles opciones son Estática, DHCP, PPPoE y PTP. La opción por defecto es DHCP ya que es muy común y, en mayoría de los casos permiten que un router "sólo trabajo" sin ninguna configuración adicional. Si no está seguro que la WAN tipo de uso o de los campos para configurar, tendrá que obtener esta información de su ISP.

Nota

Si usted tiene una interfaz inalámbrica para la interfaz WAN, algunas opciones adicionales puede parecer que no están cubiertas en este tutorial de la instalación estándar Asistente. Usted puede referirse a Capítulo 18, Wi-fi, Que tiene una sección sobre Wireless WAN para obtener información adicional. Es posible que deba omitir la configuración de la WAN por ahora, a continuación, realizar la configuración inalámbrica después.

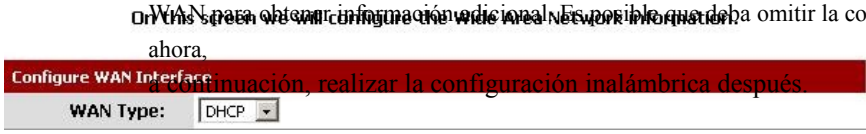


Figura 4.4. Configuración de WAN

La dirección MAC de campo en la siguiente sección (Figura 4.5, "Configuración de la WAN en General") Es útil para la sustitución de un router existente con mínimas complicaciones. Algunos proveedores de Internet, sobre todo las dirigidas por proveedores de cable, no funcionará correctamente si una nueva dirección MAC se encuentra. Algunos requieren apagar y encender el módem, otros requieren el registro de la nueva dirección con ellos por teléfono. Si esta conexión WAN está en un segmento de red con otros sistemas que se busque a través de ARP, cambiar la MAC para que coincida o más piezas de equipo también puede ayudar a facilitar la transición, en lugar de tener que borrar cachés ARP o actualizar las entradas ARP estáticas.

La unidad de transmisión máxima (MTU), el tamaño del campo se ve en Figura 4.5, "WAN General Configuración " Normalmente se puede dejar en blanco, pero se puede cambiar si lo desea. Algunas situaciones pueden convocatoria de una MTU inferior para asegurar los paquetes son de tamaño apropiado para su conexión a Internet. En mayoría de los casos, el valor por defecto asume valores para el tipo de conexión WAN funciona correctamente.

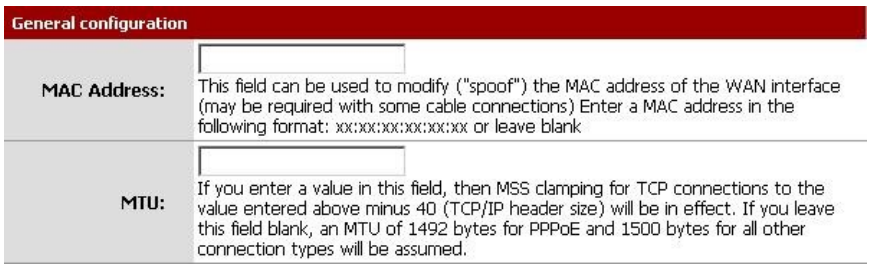


Figura 4.5. Configuración General WAN

Si la "estática" opción para el tipo de WAN es elegido, la dirección IP, máscara de subred CIDR, y Puerta de enlace debe ser completado (Figura 4.6, "Configuración de IP estática"). Esta información debe ser obtenidos a partir de su ISP o quien controla la red de la WAN de su pfSense router. La dirección IP y puerta de enlace de ambos deben residir en la misma subred.

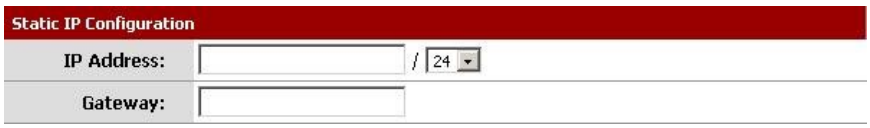


Figura 4.6. Configuración de IP estática

Algunos ISP requieren un cierto nombre de host DHCP (Figura 4.7, "nombre de servidor Marco") para ser enviados junto con la solicitud de DHCP para obtener una dirección IP WAN. Si no está seguro de qué poner en este campo, tratar de dejar en blanco a menos que indique lo contrario por su ISP.

Figura 4.7. DHCP Hostname Marco

Cuando se utiliza la conexión PPPoE (Point-a-Punto sobre Ethernet) tipo de WAN (Figura 4.8, "PPPoE Configuración "), debe al menos rellenar los campos para PPPoE nombre de usuario y contraseña PPPoE. Estos serán proporcionados por su ISP, y suelen ser en forma de una dirección de correo electrónico, tales como **mycompany@ispexample.com**. El nombre del servicio PPPoE puede ser requerida por algunos proveedores de Internet, pero a menudo se deja en blanco. Si tiene alguna duda, dejarlo en blanco o en contacto con su ISP y pregunte si es es necesario.

Acceso telefónico PPPoE de la demanda hará que pfSense para dejar la conexión abajo / en línea hasta que los datos se
solicitó que se necesita la conexión a Internet. conexiones PPPoE suceder muy rápido, por lo que en
mayoría de los casos el retraso, mientras que la conexión se configura sería insignificante. Si planea ejecutar
los servicios detrás de la caja pfSense, no comprobarlo, ya que se quiere mantener una línea
con la medida de lo posible en ese caso. También tenga en cuenta que esta opción no va a caer una ya existente
conexión.

El tiempo de espera inactivo PPPoE especifica cómo pfSense tiempo que le permitirá la conexión PPPoE ir
sin transmisión de datos antes de desconectar. Esto es realmente sólo es útil cuando se combina con
Marcar en la demanda, y por lo general se deja en blanco (discapacitados).

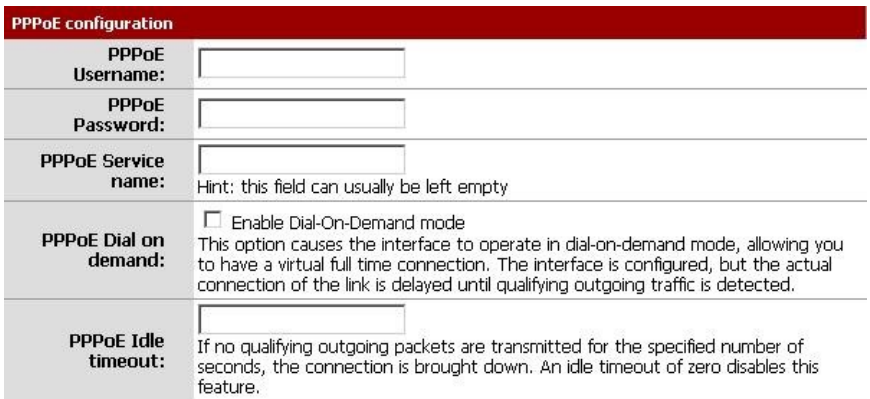


Figura 4.8. Configuración de PPPoE

El PPTP (Point-to-Point Tunneling Protocol) WAN tipo (Figura 4.9, "PPTP WAN
Configuración ") es la fuente de una cierta confusión. Esta opción es para los proveedores de Internet que requieren un
PPTP
entrada, y no para la conexión a un remoto VPN PPTP. Estos ajustes, al igual que el PPPoE
configuración, será proporcionado por su ISP. A diferencia de PPPoE, sin embargo, con una WAN PPTP debe
También se especifica una dirección IP local, la máscara de subred CIDR, y establecer la dirección IP remota a la
conexión.

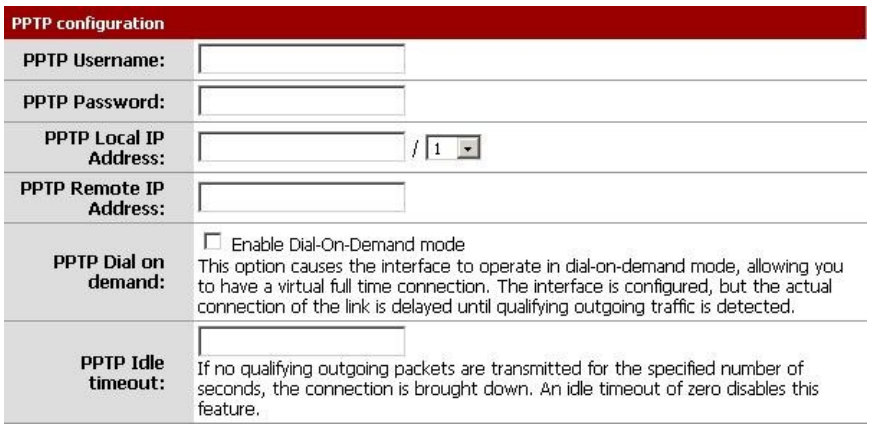


Figura 4.9. PPTP Configuración WAN

Estas dos últimas opciones, se ve en Figura 4.10, "Piedra-en el filtrado de entrada Opciones", son útiles para prevenir el tráfico válido entren en su red, también conocido como "El filtrado de entrada". Habilitación Bloque RFC 1918 Redes Privadas bloqueará registrados redes privadas, tales como 192.168.xx 10.xxx y de realizar las conexiones a la dirección de la WAN. Una lista completa de estos redes se encuentra en Sección 1.7.1.1, "Direcciones IP privada". El Bloque Bogon redes opción detener el tráfico de venir en que se obtiene de reservada o no asignado el espacio IP que no debe estar en uso. La lista de redes Bogon se actualiza periódicamente en el fondo, y no requiere manual de mantenimiento. redes Bogon se explican en Sección 6.5.1.4, "Bogon Bloque Redes ". Haga clic en Siguiente para continuar cuando haya terminado.

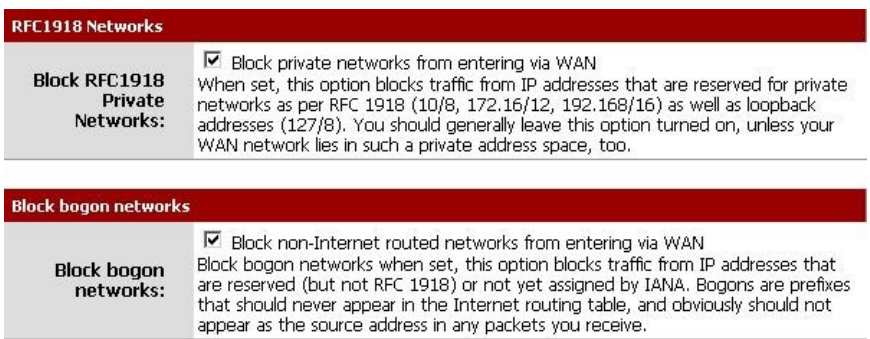


Figura 4.10. Construido en el filtrado de entrada Opciones

4.2.4. Configuración de la interfaz LAN

Aquí se le da la oportunidad de cambiar la dirección IP de la LAN y la máscara de subred (Figura 4.11, "Configuración de LAN"). Si no planea siempre sobre la conexión de la red para cualquier otra red a través de VPN, el defecto está muy bien. Si usted quiere ser capaz de conectarse a la red mediante VPN desde ubicaciones remotas, usted debe elegir un intervalo de direcciones IP privadas mucho más oscuro que el mismo 192.168.1.0/24 común. Espacio en el RFC 1918 172.16.0.0/12 bloque de direcciones privado parece ser el menos frecuente, así que escoja algo entre 172.16.xx y 172.31.xx menos para probabilidad de tener dificultades de conectividad VPN. Si la LAN es 192.168.1.x, y usted está en un punto de acceso inalámbrico utilizando 192.168.1.x (muy común), no podrá comunicarse a través de la VPN - 192.168.1.x es la red local, no a su red a través de VPN.
Si la IP de la LAN tiene que ser cambiado, introduzca aquí junto con una nueva máscara de subred. Tenga en cuenta que si cambia esta configuración, también tendrá que ajustar la dirección IP de su PC, libere o renueve su concesión DHCP, o realizar una "reparación" o "Diagnóstico" en la interfaz de red cuando haya terminado con el asistente de configuración.

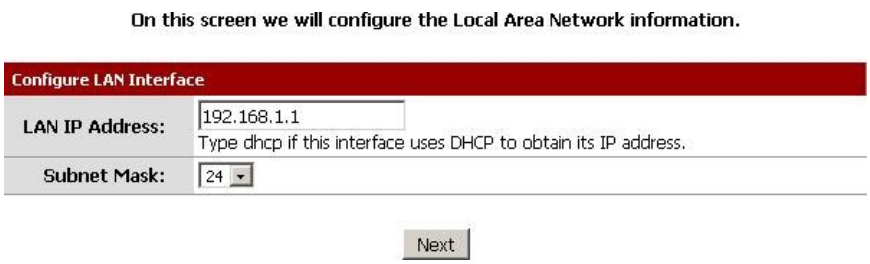


Figura 4.11. Configuración de LAN

4.2.5. Establezca la contraseña de administrador

A continuación, debe cambiar la contraseña de administración para la WebGUI como se muestra en Figura 4.12, "Cambiar la contraseña administrativa". Esta contraseña debe ser algo fuerte y segura, pero no hay restricciones aplicadas de forma automática. Introduzca la contraseña dos veces para estar seguro de que ha sido introducido correctamente, a continuación, haga clic en Siguiente.

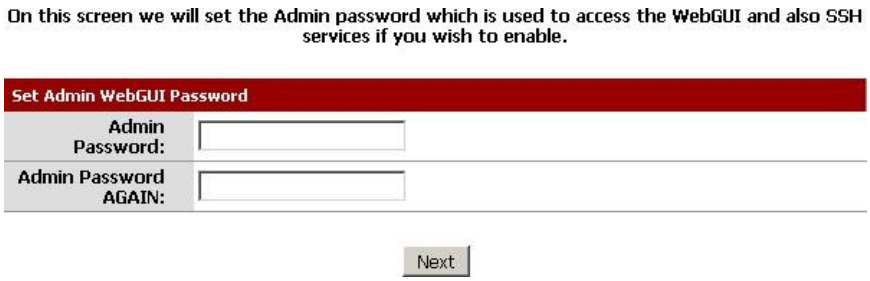


Figura 4.12. Cambiar Contraseña Administrativa

4.2.6. Finalización del Asistente para la instalación

Ese es el final del asistente de configuración, haga clic en Actualizar (Figura 4.13, "pfSense Actualizar WebGUI") y
WebGUI volverá a cargar. Si ha cambiado la IP de la LAN, modifica la dirección IP de su PC en consecuencia.
También se le pedirá la contraseña de nuevo. El nombre de usuario sigue siendo **admin**.

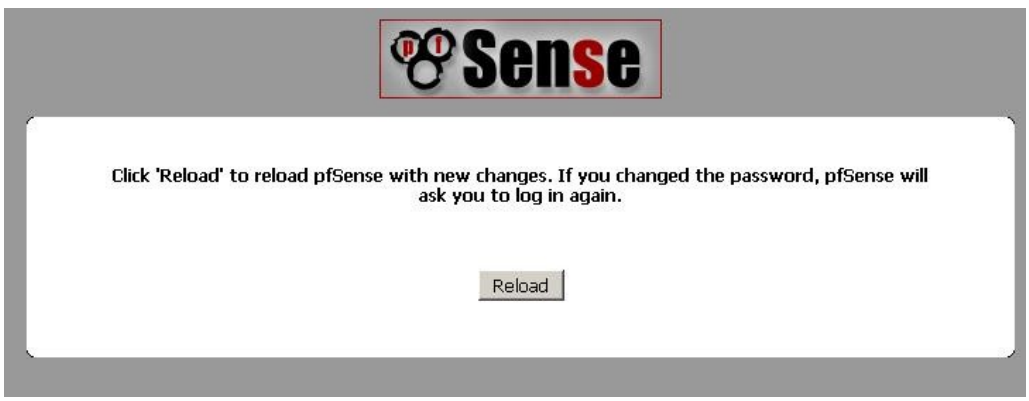


Figura 4.13. Actualizar pfSense WebGUI

En este punto usted debe tener conectividad básica a Internet, o la red de la WAN

secundarios. Los clientes de la LAN debe ser capaz de llegar a los sitios a través del router pfSense. Si en cualquier vez que se tenga que repetir esta configuración inicial, puede hacerlo en Sistema → El programa de instalación
El asistente desde la WebGUI.

4.3. Interfaz de configuración

Como se ha visto, algunos de configuración de interfaz se puede realizar en la consola y en la configuración asistente para iniciar las cosas, pero los cambios también se pueden hacer después de la configuración inicial al visitar el lugares apropiados en el menú de interfaces.

4.3.1. Asignar interfaces

Si interfaces adicionales se añaden después de la instalación, entonces se le puede asignar funciones al visitar Interfaces → (Asignar). Hay dos pestañas aquí, las asignaciones de la interfaz y las VLAN. (VLAN configuración se expone más adelante en Capítulo 10, LAN virtuales (VLAN).) Las asignaciones de la interfaz pestaña muestra una lista de todas las interfaces actualmente asignado: WAN, LAN, y cualquier OPTX que configurado. Al lado de cada interfaz es una lista desplegable de todas las interfaces de red o puertos que se encuentran en el sistema, incluyendo interfaces de hardware real, así como interfaces VLAN. La dirección MAC o VLAN etiquetas se mostrarán junto a los nombre de la interfaz para facilitar la identificación.

Usted puede cambiar las interfaces actualmente asignado al decantarse por un puerto de red nuevos, o añadir un interfaz adicional OPTX haciendo clic. Esto añadirá otra línea, con una interfaz nueva OPT, número más alto que cualquier interfaz de OPT existentes, o si no los hay, OPT1. De forma predeterminada, se seleccione automáticamente la interfaz disponible siguiente que no esté asignado. Por ejemplo, si el objetivo sistema ha `fxp0`,`fxp1`, Y `fxp2`, Y ha establecido WAN `fxp0`, Y LAN fijado para `fxp1`, elegir para agregar otra interfaz asumirá automáticamente OPT1 se `fxp2`. Si usted tiene interfaces adicionales y esto no es el lugar previsto, y puede ser modificado. Si los cambios son hecho, asegúrate de hacer clic en Guardar.

4.3.2. De interfaz WAN

Casi todas las opciones que se encuentran en las interfaces → WAN son idénticos a los especificados en el la parte WAN del Asistente para la instalación. El tipo de WAN se puede cambiar, así como la asignación de un dirección IP estática, máscara de subred, puerta de entrada, la configuración de DHCP, PPPoE y PPTP. También puede activar o desactivar el bloqueo de redes privadas y redes Bogon. Una notable excepción a esta es la tecnología inalámbrica WAN, que mostrará las opciones de configuración inalámbrica al lado de la típica WAN opciones.

Una de las opciones disponibles aquí que no se muestra en el asistente de configuración es la capacidad de deshabilitar la espacio de usuario de aplicación FTP-Proxy, también conocido como el ayudante de FTP. Si está ejecutando un FTP público (File Transfer Protocol) detrás de pfSense, es posible que desee para que el ayudante de FTP para que conexiones FTP funcione correctamente. Tenga en cuenta que al hacer esto todas las conexiones FTP se parecen

vienen desde el router pfSense ya estará actuando como un proxy. Ver Sección 7.8.1, "FTP" de más información en profundidad sobre el proxy FTP y temas relacionados con el FTP.

4.3.3. Interfaz LAN

Algunas opciones adicionales para el lado de la LAN están disponibles en las interfaces → LAN además de establecer
la dirección IP, que fue cubierto en el Asistente para la instalación.

El puente con opción puente de la interfaz LAN a otra interfaz en el sistema. Consulte
a Capítulo 9, Puente Para obtener más información sobre el puente.

Al igual que con la configuración de la interfaz WAN, también hay una opción para deshabilitar el espacio de usuario de

FTP

aplicación Proxy. Usted debe casi siempre dejar este habilitado. Cuando está activo en la LAN
lado, esto proxy conexiones FTP y hacerlo de modo que los clientes de la LAN pueden utilizar la
protocolo FTP normalmente en modo activo, y el proxy se abrirá y redireccionar los puertos adecuados
dinámicamente durante una sesión FTP.

4.3.4. Interfaces opcionales

Cualquier adicional opcional (OPTX) interfaces también se mostrarán en este menú, bajo OPT1, OPT2 ...
OPTX, o nombres de encargo dado a la interfaz. Estas interfaces tienen unas cuantas opciones más de
la interfaz LAN, pero menos de la WAN.

Para habilitar una interfaz territorio palestino ocupado, primero debe comprobar la Habilitar opcional *x*

Interfaz de casilla,

donde *x* es el número actual de la interfaz del territorio palestino ocupado que está configurando. Por ejemplo, en OPT1, diría Habilitar una interfaz opcional. También puede cambiar el nombre de esta interfaz mediante la introducción de una Breve descripción. Esta descripción (DMZ, servidores de la Oficina, Ingeniería, etc) aparecerá en su lugar de "OPT1" en los menús y de configuración. Esto hace que sea mucho más fácil de recordar no sólo lo que es una interfaz para el, sino también para identificar a un interfaz para añadir reglas de firewall o elegir otras funciones de cada interfaz.

interfaces de OPT se puede fijar para DHCP o IP estático, y como con la red WAN que puede alterar el MAC
dirección y MTU. Al igual que el interfaz LAN, es posible que también puente de una interfaz a otra OPT
interfaz, uniéndose a ellos en el mismo dominio de broadcast. Usted puede usar esto para añadir otro puerto
a la LAN, o crear un puente DMZ.

Si va a ser una interfaz WAN OPT-tipo, para una configuración multi-WAN, debe entrar en
una dirección de puerta de enlace IP, así a menos que esté utilizando DHCP. En 1.2.x pfSense sólo se puede usar un servidor DHCP o estático conexión IP por un período adicional de interfaz WAN, no un tipo PPPoE o PPTP conexión. Esta cuestión será debatida en pfSense 2.0. Para obtener más detalles sobre la configuración de múltiples conexiones WAN, consulte Capítulo 11, Múltiples conexiones WAN.

La opción de ayuda de FTP también está disponible. Consulte Sección 7.8.1, "FTP" para más información.

4.4. Opciones generales de configuración

Algunas opciones de sistema general se encuentran en Sistema → Configuración general, la mayoría de ellos se verá
familiares del asistente de configuración.

El nombre de host y de dominio, servidores DNS, los órganos de administración de usuario y contraseña, y el Zona horaria y el servidor NTP de tiempo se puede cambiar si se desea, como se explica en el asistente de configuración.

Junto con la capacidad de cambiar los servidores DNS, no hay otra opción: la lista de admitidos del servidor DNS que sea reemplazada por DHCP / PPP en WAN. Este es en esencia lo que dice, si está marcada, pfSense utilizará los servidores DNS que se asignan de forma dinámica por DHCP o PPP. Que se utilizará por el propio sistema y como aguas arriba servidores DNS para el promotor de DNS. Estos servidores se no se transmite a los clientes DHCP detrás del sistema de pfSense, sin embargo.

El puerto y el Protocolo WebGUI WebGUI se puede establecer. HTTP y HTTPS están disponibles. La las mejores prácticas sería el uso de HTTPS para que el tráfico WebGUI se cifra, sobre todo si la servidor de seguridad se gestiona de forma remota. Traslado de la WebGUI a un puerto alternativo es también una buena táctica
para mayor seguridad, y se va a liberar los puertos de Internet estándar para su uso con el puerto o hacia delante otros servicios, como un proxy squid. Por defecto, el WebGUI utiliza HTTP en el puerto 80 para el mejor compatibilidad y facilidad de configuración inicial.

Por último, un tema también se puede elegir. Varios están incluidos en el sistema base, y sólo hacer cosméticos - cambios en la apariencia de la WebGUI - no funciona.

4.5. Opciones avanzadas de configuración

En virtud del sistema → Avanzada se encuentra una gran cantidad de opciones que son de carácter más avanzado.

Ninguna de estas opciones debería ser necesario el ajuste de una base de enrutamiento y configuración de NAT, pero es posible
que algunos de los cambios rigen por estas opciones le ayudará en la personalización de la configuración de su de manera beneficiosa.

Algunas de estas opciones pueden ser cubiertos en más detalle en otras secciones del libro en su discusión sería más actual o relevante, pero todos ellos son mencionados aquí con una breve descripción.

4.5.1. Consola serie

Si este sistema pfSense va a correr "sin cabeza" (sin teclado, vídeo, ratón adjunto) que puede ser deseable para habilitar esta opción, que se redirigir la consola de entrada / salida a la serie

puerto. Esto desactivará el teclado a bordo, vídeo y ratón, pero le permitirá conectar un cable de módem nulo al puerto serie y que gestiona directamente desde otro PC o dispositivo de serie. Después de de hacer cualquier cambio, asegúrese de hacer clic en Guardar cuando haya terminado.

Para obtener más información sobre la conexión a una consola serie, consulte Sección 3.3.5.1, "Conectar una serie Cable " y Sección 3.3.5.2, "Empezar un cliente de serie".

4.5.2. Secure Shell (SSH)

El Secure Shell (SSH) servidor puede ser activado a distancia que permitirá a la consola y el archivo de gestión. Usted puede conectar con cualquier cliente estándar de SSH, como el comando de OpenSSH línea de cliente ssh, PuTTY, SecureCRT o iTerm. O bien la WebGUI nombre de usuario (como administrador) o la cuenta de root puede ser utilizado, y ambos aceptan la contraseña WebGUI de entrada.

Las transferencias de archivos desde y hacia el sistema de pfSense también son posibles mediante el uso de una copia segura (SCP) cliente, como scp de OpenSSH de línea de comandos, FileZilla, WinSCP o Fugu. Para usar SCP, debe conectarse como usuario root no admin.

Para habilitar el SSH, active la casilla junto a Activar Secure Shell. También es más seguro para mover el Servidor SSH a un puerto alternativo. Al igual que con mover el WebGUI a un puerto alternativo, que proporciona una pequeña mejora de la seguridad, y libera el puerto si desea que lo remita a un sistema interno. Para cambiar el puerto, escriba el nuevo puerto en el cuadro del puerto SSH.

También puede configurar SSH para permitir que sólo los inicios de sesión basada en clave y no una contraseña. Para ello, visita Deshabilitar la contraseña de inicio de sesión de Secure Shell (CLAVE solamente) y pegar las teclas permite pública en el Autorizado Claves campo de texto. Cambiar a la entrada única clave basada en una práctica mucho más segura, aunque hace falta ser un poco más de preparación para configurar.

Si usted se encuentra en una situación que exige que se deje libre el acceso SSH por el firewall normas, que puede ser peligroso, es muy recomendable que en esta situación que ambos se mueven el servicio SSH en un puerto aleatorio suplentes, y cambiar a la autenticación basado en claves. El logro de un puerto alternativo evitará que el ruido de registro de los intentos de fuerza bruta de inicio de sesión SSH y exploraciones ocasionales. Todavía se puede encontrar con un escaneo de puertos, por lo que cambiar a la autenticación basada en claves siempre deben debe hacerse en cada servidor SSH de acceso público para eliminar la posibilidad de éxito bruta ataques de fuerza.

4.5.3. Física compartida de red

Si tiene dos o más interfaces que comparten la misma red física, como en un escenario en múltiples interfaces están conectados a la misma transmisión de dominio, la opción única en este sección, se oculta la espuria mensajes ARP que de otro modo, la sobrecarga de los registros con inútiles las entradas.

4.5.4. IPv6

En la actualidad, pfSense no es compatible con IPv6 de filtrado, aunque las reglas muy permisiva podría permitir
el tráfico IPv6 que la mayoría de los usuarios no esperan que el tráfico IPv6 a abandonar su red, ya que no se utiliza. Como tal, el tráfico IPv6 se bloquea de forma predeterminada. Si usted requiere IPv6 para pasar el firewall, consulte la caja para permitir el tráfico IPv6. También puede activar NAT encapsulado de paquetes IPv6 (el protocolo IP 41/RFC 2893) comprobando que la caja y entrar en una dirección IPv4 a que los paquetes deben se transmitirá.

4.5.5. Filtrado de Puente

Antes de la versión 1.2.1 de pfSense, no fue una elección de si o no para filtrar el tráfico en el puente interfaces, retenido desde el método más antiguo de tender un puente utilizado en m0n0wall. Más reciente de FreeBSD comunicados de utilizar una metodología distinta puente que hizo la primera opción obsoleta. Sin embargo una descripción se conserva aquí para evitar confusiones, ya que muchos usuarios están acostumbrados a utilizarla, y es mencionado en numerosos lugares.

4.5.6. WebGUI certificado SSL / clave

Al utilizar el modo HTTPS para la WebGUI para cifrar el acceso a la interfaz web, por defecto el sistema utilizará un certificado con firma personal. Eso no es una situación ideal, pero es mejor que nada cifrado en absoluto. Esta opción le permite utilizar un certificado existente para mejorar aún más la seguridad y proteger contra los ataques "man-in-the-middle.

Si usted tiene un certificado SSL existentes y la clave, usted puede pegar aquí. También hay un enlace denominado "Creación de certificados de forma automática", lo que disparará una función interna de pfSense a generar un nuevo certificado con firma personal en su lugar.

La desventaja principal de usar un certificado personalizado de auto-generada es la falta de fiabilidad de la la identidad del huésped, ya que el certificado no está firmado por una autoridad de certificación de confianza por su navegador. Además, dado que la mayor parte de los usuarios de Internet, un certificado no válido debería ser considera un riesgo, los navegadores modernos han estado combatiendo en la forma en que se manejan. Firefox, por ejemplo, ofrece una pantalla de advertencia y obliga al usuario a importar el certificado y permiten excepción permanente. Internet Explorer mostrará una pantalla de advertencia con un enlace para continuar. Opera mostrará un diálogo de advertencia que también permite una derivación permanente.

4.5.7. Equilibrio de carga

El texto de la WebGUI explica mejor opción Adherido Conexiones en esta sección: Sucesivos conexiones serán redirigidos a los servidores de una forma de round-robin con conexiones desde el

misma fuente que se envía al mismo servidor web. Esta "conexión pegajosa" existirá siempre y cuando hay estados que hacen referencia a esta conexión. Una vez que los estados expirará, por lo que será la conexión pegajosa. Otras conexiones de host que será remitido a un servidor web, el próximo en el round robin.

"Sticky" conexiones son deseables para algunas aplicaciones que dependen de las IPs mismo ser mantenido a lo largo de un determinado período de sesiones. Esto se utiliza en combinación con la carga del servidor equilibrio de la funcionalidad, describe con detalle en Capítulo 17, Servidor de equilibrio de carga.

4.5.8. Varios

A pocas opciones que no encajan en ninguna otra categoría se puede encontrar aquí.

4.5.8.1. Dispositivo de votación

dispositivo de votación es una técnica que permite que el sistema periódicamente dispositivos sondeo de la red para los nuevos datos
en lugar de depender de las interrupciones. Esto evita que su WebGUI, SSH, etc de ser inaccesibles debido a la interrupción de las inundaciones cuando bajo carga extrema, a costa de latencia ligeramente superior (hasta 1 ms). Este suele ser innecesaria, a menos que su hardware es insuficiente.

Sondeo también requiere soporte de hardware en las tarjetas de red de su sistema. De acuerdo con la de votación (4) La página man para FreeBSD 7.2 (sobre el cual se basa pfSense 1.2.3), la `bge (4)`,`CC (4)`, `em (4)`,`EFT (4)`,`fwip (4)`,`fxp (4)`,`ixgb (4)`,`educación no formal (4)`,`ESN (4)`,`Re (4)`,`rl (4)`, `sf (4)`,`sis (4)`,`ste (4)`,`stge (4)`,`GVE (4)`,`vr (4)`, Y `xl (4)` dispositivos son compatibles, con el apoyo de otras pendientes en futuras versiones de FreeBSD.

4.5.8.2. Menú de la consola

Normalmente, el menú de la consola siempre se muestre en la consola del sistema, y estará disponible como siempre y cuando tenga acceso físico a la serie o el vídeo de la consola. En algunas situaciones esto no es deseable, por lo que esta opción permitirá a la consola para ser protegido por contraseña. Usted puede ingresar con el mismo nombre de usuario y contraseña que se utiliza para la WebGUI. Después de configurar esta opción, debe reiniciar el sistema
el sistema de pfSense antes de que surtan efecto.

Nota

Si bien esto deja de pulsaciones de teclas accidentales, y mantener a los usuarios ocasionales, esto no es en mediante un método de seguridad perfecto. Una persona con conocimientos de acceso físico podría restablecer las contraseñas (véase Sección 4.10.2, "He olvidado la contraseña con un Cerrado consola "). Debe tener en cuenta otros métodos de seguridad física si es que un requisito de su instalación.

4.5.8.3. WebGUI anti-bloqueo

De forma predeterminada, el acceso a la WebGUI en la interfaz LAN se dará siempre, independientemente de la
las reglas de filtrado definidas por el usuario. Al habilitar esta característica permite un control más preciso sobre el cual LAN direcciones IP pueden acceder a la WebGUI, pero asegúrese de tener una regla de filtrado en su lugar para permitir que
acceso antes de habilitar esta opción!

Nota

Restablecimiento de la IP LAN de la consola del sistema también se restablecerá esta opción. Si encuentra bloqueado después de habilitar esto, elegir la opción de menú de la consola para configurar la IP de la LAN, y entrar en la dirección exactamente la misma IP y la información adjunta.

4.5.8.4. Ruta estática de filtrado

Las reglas de firewall bypass para el tráfico en la opción misma interfaz sólo se aplica si se han definido una o más rutas estáticas. Si está habilitada, el tráfico que entra y sale por la misma interfaz no se comprobará por el firewall. Esto puede ser deseable en algunas situaciones en las múltiples subredes están conectadas a la misma interfaz.

4.5.8.5. IPsec Preferral SA

De forma predeterminada, el caso de varias asociaciones de seguridad IPSec (SA) partido, el más nuevo es preferible si se trata de
por lo menos 30 segundos de edad. Seleccione esta opción para preferir siempre SA de edad en los nuevos. Esto rara vez es deseable. Para más información sobre asociaciones de seguridad, consulte Sección 13.1.1, "Asociación de Seguridad"

4.5.9. Traffic Shaper y Firewall avanzado

Estas opciones se rigen algunas de las funcionalidades más avanzadas y el comportamiento de bajo nivel filtrado de paquetes realizado por pf.

4.5.9.1. FTP RFC 959 datos solución puerto de violación

Solución para los sitios que violan RFC 959, que especifica que la conexión de datos se obtienen de menos un puerto que el puerto de comandos (normalmente el puerto 20). Esta solución no expone a un riesgo mucho más como el servidor de seguridad sigue siendo sólo permite conexiones a un puerto en el que el proxy FTP está escuchando.

4.5.9.2. Borrar DF bits en lugar de dejar caer

Esta es una solución para los sistemas operativos que generan paquetes fragmentados con el no fragmento (DF) bit. Linux NFS (Network File System) es conocido por hacer esto. Esto hará que el filtro de no dejar caer los paquetes tales, sino que borrar el bit no fragmentar. El filtro también aleatorizar el campo de identificación IP de los paquetes de salida con esta opción, para compensar sistemas operativos que establezca el bit DF, pero establece un cero de identificación IP campo de cabecera.

4.5.9.3. Servidor de seguridad de Opciones de optimización

Hay aquí algunas opciones que controlan cómo el servidor de seguridad caduca establece lo siguiente:

Normal	El algoritmo de optimización estándar.
Alta latencia	Utilizadas para las conexiones de alta latencia, como los enlaces por satélite. Expira conexiones inactivas a más tardar el defecto.
Agresivos	Expira inactivo conexiones más rápidas. Un uso más eficiente de la CPU y la memoria pero puede caer conexiones legítimas antes de lo esperado.
Conservador	Trata de evitar que se caigan las conexiones legítimas a expensas de mayor uso de memoria y utilización de la CPU.

4.5.9.4. Deshabilitar el firewall

Si opta por desactivar todos los filtros de paquetes, que a su vez, el sistema pfSense en una ruta de sólo plataforma. Como consecuencia, NAT también se desactivará.

4.5.9.5. Desactivar Firewall de fregado

Desactiva la opción de lavado de fondos de pensiones, que a veces pueden interferir con NFS y el tráfico PPTP. De forma predeterminada, pfSense utiliza la opción de fregar al azar-id que aleatoriza la identificación IP campo de un paquete para mayor seguridad, y fragmentos de la opción de volver a montar la que se vuelva a montar paquetes fragmentados antes de enviarlos a. Más información sobre la función Scrub se pueden encontrar en el OpenBSD PF Scrub Documentación [http://www.openbsd.org/faq/pf/scrub.html].

4.5.9.6. Servidor de seguridad de Estados máximo

Establece el número máximo de conexiones de celebrar en la tabla de estado de servidor de seguridad. El valor por defecto es de 10,000 y debe ser suficiente para la mayoría de las instalaciones, pero se puede ajustar mayores o menores dependiendo de la carga y la memoria disponible. Cada estado consume alrededor de 1 KB de memoria RAM, o aproximadamente 1 MB de RAM por cada 1 000 estados, así que asegúrese de tener suficiente memoria RAM antes de aumentar este. Servidor de seguridad de los estados se tratan más en Sección 6.1.2, "filtrado con estado".

4.5.9.7. Desactivar Auto-agregó reglas VPN

Esto desactiva automáticamente añadido normas para IPSec, PPTP, y OpenVPN. Normalmente, cuando se habilitar una de estas redes privadas virtuales, las reglas se agregan automáticamente a la interfaz adecuada que permitir el tráfico a los puertos. Al desactivar estas reglas automático, usted puede tener un mayor control sobre las que las direcciones pueden conectarse a la VPN.

4.5.10. Network Address Translation

El Deshabilitar NAT Reflexión opción, cuando está activada, desactive la creación automática de NAT redirigir las normas para acceder a sus direcciones IP públicas dentro de sus redes internas. Este opción está activada de forma predeterminada, las reglas de reflexión para NAT no se crean a menos que cambie este ajuste. NAT reflexión sólo funciona en el puerto elementos tipo de desvío y no funciona para los grandes rangos de más de 500 puertos. Consulte Sección 7.5, "Reflexión NAT" para una discusión sobre la fondo de Reflexión NAT en comparación con otras técnicas como Split DNS.

4.5.11. Opciones de hardware

Hay algunas opciones específicas del hardware que se pueden establecer. Estas opciones generalmente se debe dejar solo, a menos que uno de los casos mencionados se aplica a su hardware.

4.5.11.1. Descarga de suma de comprobación de hardware

Al seleccionar esta opción, se deshabilita la descarga de suma de comprobación de hardware. descarga de suma de comprobación se rompe en algunos de hardware, en particular algunas tarjetas Realtek. En raras ocasiones, los conductores pueden tener problemas con de control de descarga y algunas tarjetas de red específica. Los síntomas típicos de la suma de comprobación roto descarga incluyen los paquetes dañados y un rendimiento pobre.

4.5.11.2. Deshabilitar la carga glxsb

El procesador AMD Geode LX de Seguridad del bloque (`glxsb`) Controlador se utiliza principalmente en Alix y Soekris sistemas embebidos. Es un acelerador criptográfico que puede mejorar el rendimiento de ciertos sistemas de cifrado, como AES-128. Esto puede mejorar el rendimiento de VPN y otros subsistemas que pueden AES uso-128, tales como SSH. Este controlador puede entrar en conflicto con otras tarjetas aceleradoras de criptografía, tales como los de Hifn, y tienen prioridad sobre ellos, cuando ambos se encuentran. Si usted tiene un Hifn tarjeta, debe configurar esta opción para que el `glxsb` dispositivo no está cargado. Si el controlador ya está en uso, debe reiniciar el sistema después de establecer esta opción para que pueda ser descargada.

4.6. Conceptos básicos del menú de la consola

Algunas tareas de configuración y mantenimiento también se puede realizar desde la consola del sistema. La la consola puede ser alcanzado mediante el teclado y el ratón, la consola de serie si está activado o el uso de incorporado, o usando SSH. A continuación se muestra un ejemplo de lo que el menú de la consola será similar, pero puede variar ligeramente dependiendo de la versión y plataforma.

```
*** Bienvenidos a pfSense-1.2.3 de pfSense pfSense ***

LAN -> fxp1 -> 192.168.1.1
WAN -> fxp0 -> 1.2.3.4

pfSense configuración de la consola
***********************
 0) Cerrar sesión SSH (solamente)
 1) Asignar interfaces
 2) Establecer la dirección IP LAN
 3) Reiniciar contraseña webConfigurator
 4) Restablecer los valores predeterminados de fábrica
 5) Reiniciar el sistema
 6) Sistema de Parada
 7) Ping acogida
 8) Shell
 9) PFtop
10) Filtro de Registros
11) Reiniciar webConfigurator
12) pfSense desarrolladores Shell
13) Actualización de la consola
14) Desactivar Secure Shell (sshd)
98) Mover el archivo de configuración de dispositivo extraíble

Ingrese una opción:
```

Lo que sigue es una descripción general de lo que es posible mediante el uso de la mayoría de estas opciones. Al igual que con
otras opciones avanzadas, algunos de ellos pueden ser cubiertos con más detalle en otras secciones de la libro en el que la discusión sería más actual o relevante.

4.6.1. Asignar interfaces

Esto reiniciará la tarea de asignación de interfaz, que fue cubierto en detalle en Sección 3.2.3, "Asignación de interfaces" y Sección 3.5.3.1, "manual de Asignación de interfaces". Usted puede crear interfaces VLAN, reasignar las interfaces existentes, o asignar nuevos.

4.6.2. Establecer la dirección IP de la LAN

Esta opción se puede utilizar de la manera obvia, para establecer la dirección IP de la LAN, pero también hay algunas otras tareas útiles que suceden al restablecer la IP de la LAN. Para empezar, cuando esta se establece, también tienes la opción de convertir DHCP encendido o apagado, y establecer el rango DHCP IP.

Si ha deshabilitado la regla WebGUI anti-bloqueo, se le pedirá que vuelva a habilitarlo. Será
Además del sistema para volver a HTTP en el puerto por defecto si se utiliza un puerto no estándar. Esto se hace para ayudar a los que pueden encontrarse bloqueado el uso de la WebGUI recuperar el acceso.

4.6.3. Perdí mi contraseña webConfigurator

Esta opción se restablecerá el nombre de usuario y contraseña WebGUI de nuevo a **admin** y **pfSense**, , respectivamente.

4.6.4. Restablecer los valores predeterminados de fábrica

Esto restaurará la configuración del sistema a los valores predeterminados de fábrica. Tenga en cuenta que esto no será, Sin embargo, realizar ningún cambio en el sistema de archivos o los paquetes instalados en el sistema operativo. Si usted sospecha
que los archivos del sistema se han dañado o alterado de alguna manera no deseada, lo mejor es
hacer una copia de seguridad, y volver a instalar desde el CD u otros medios de instalación. (También posible en el WebGUI
Diagnóstico en → valores predeterminados de fábrica)

4.6.5. Reinicio del sistema

Esto limpia el apagado del sistema de pfSense y reiniciar el sistema operativo (Diagnóstico → Reiniciar en WebGUI).

4.6.6. Detener el sistema

Esto limpia apagar el sistema y, o bien fuera de detener o de energía, dependiendo en el hardware
apoyo. No se recomienda para sacar siempre el enchufe de un sistema en funcionamiento, incluso incrustados sistemas. Detener antes de quitar el poder es siempre la opción más segura si alguna vez necesita dar vuelta

apagar el sistema. En sistemas embebidos, tirando del enchufe, es menos peligroso, pero si el tiempo es malo también podría ser perjudicial (Diagnóstico → Detener sistema en el WebGUI).

4.6.7. Ping de acogida

Solicita una dirección IP, que se envió a tres peticiones de eco ICMP. La producción de la ping se muestra, incluyendo el número de paquetes recibidos, los números de secuencia, los tiempos de respuesta, y el porcentaje de pérdida de paquetes.

4.6.8. Shell

Inicia un shell de línea de comandos. Muy útil, y muy potente, pero también tiene el potencial de ser muy peligroso. Algunas tareas de configuración compleja puede requerir que trabajan en la cáscara, y algunas tareas de reparación son más fáciles de lograr de aquí, pero siempre hay una oportunidad de causar daños irreparables en el sistema si no se maneja con cuidado. La mayoría de los usuarios pfSense nunca tocar la concha, e incluso saben que existe.

Veterano de usuarios de FreeBSD puede sentir un poco como en casa, pero hay muchos comandos que no están presentes en un sistema de pfSense, ya que las partes innecesarias del sistema operativo se retiran por razones de restricciones de seguridad y tamaño.

La concha comenzó de esta manera se tcsh, y la cáscara sólo están disponibles en otros es mierda. A pesar de que puede ser posible instalar otros shells (véase Sección 24.4, "Utilización de Software de los puertos de FreeBSD Sistema (paquetes) ") Para la comodidad de aquellos que están muy familiarizados con el sistema operativo, esto no es recomienda ni se admite.

4.6.9. PFtop

PFtop le da una visión en tiempo real de los estados de firewall, y la cantidad de datos que han enviado y recibidos. Puede ayudar a identificar las direcciones IP y las sesiones de momento está usando el ancho de banda, y también puede ayudar a diagnosticar otros problemas de conexión de red. Ver Sección 22.6.2, "Cómo ver con pftop " para más detalles.

4.6.10. Filtrar registros

Utilizando la opción de filtro Registros, podrás ver ninguna de las entradas de registro de filtro aparece en tiempo real, en su forma cruda. Hay bastante más información que se muestra por la línea de lo que normalmente se ven en la vista del registro de firewall en el WebGUI (Estado → Registros del sistema, pestaña Firewall), pero no todos los de este la información es fácil de leer.

4.6.11. Reinicie webConfigurator

Reiniciar el webConfigurator se reiniciará el proceso del sistema que ejecuta el WebGUI. En raras ocasiones puede haber un cambio que puede ser que necesite esto antes de que entrará en vigor, o en muy algunos casos el proceso puede haberse detenido por alguna razón, y reiniciar será restaurar el acceso.

4.6.12. pfSense desarrolladores Shell (antes de shell PHP)

La cáscara de desarrolladores, que solía ser conocido como el pfSense shell PHP, es una herramienta muy poderosa que le permite ejecutar código PHP en el contexto del sistema en ejecución. Al igual que con la consola normal, también puede ser muy peligroso utilizar, y fácil para que las cosas van mal. Este es utilizado principalmente por los desarrolladores y los usuarios experimentados que están íntimamente familiarizado con PHP y pfSense la código base.

4.6.13. Actualización de la consola

Con esta opción, se puede actualizar mediante la introducción de una dirección URL completa a una imagen del firmware pfSense,
o una ruta de acceso completa locales de una imagen cargada de alguna otra manera. Este método de actualización es cubiertos en más detalle en Sección 3.7.3.2, "Aumentar el uso de la consola".

4.6.14. Activar / Desactivar Secure Shell (sshd)

Esta opción le permitirá cambiar el estado del demonio de Secure Shell, sshd. Funciona
de manera similar a la misma opción en el WebGUI cubiertos anteriormente en este capítulo, pero es accesible desde la consola.

4.6.15. Mueva el archivo de configuración de dispositivo extraíble

Si desea mantener la configuración del sistema de almacenamiento extraíble, como una memoria USB
unidad, esta opción se puede utilizar para trasladar el archivo de configuración. Una vez usado, asegúrese de asegurarse de que
los medios de comunicación es accesible en tiempo de arranque para que pueda volver a cargar. Esto no es un método normal de
copias de seguridad de la configuración. Para información sobre cómo hacer copias de seguridad, consulte Capítulo 5, Copia de seguridad y Recuperación.

4.7. Sincronización de la hora

El tiempo y los problemas del reloj no son tan poco frecuentes en la configuración de cualquier sistema, pero se puede importante hacerlo bien en los routers, sobre todo si está realizando cualquier tipo de tareas que implican validación de certificados como parte de una infraestructura de PKI. Obtención de sincronización de tiempo para trabajar adecuadamente es también una necesidad absoluta en sistemas embebidos, algunos de los cuales no tienen una batería

a bordo para preservar su fecha y la hora cuando se desconecta la alimentación. No puede haber algunas peculiaridades de obtener no sólo una fecha adecuada y el tiempo en el sistema, y mantener de esa manera, pero también en asegurarse de que la zona horaria está bien reflejada.

No sólo va a conseguir esta ayuda en línea en todas las tareas críticas del sistema, pero asegura también que su los archivos de registro están debidamente fechados, que puede ser de gran ayuda en la solución de problemas, el mantenimiento de registros,
y la gestión general del sistema.

4.7.1. Zonas de tiempo

Usted verá un comportamiento inesperado si se selecciona una de las compensaciones de tiempo con GMT zones.The son lo contrario de lo que esperas de ellos se basará en sus nombres. Por ejemplo, la
GMT-5 zona es realmente GMT más horas 5. Esto viene de la base de datos TZ que FreeBSD y
muchos otros sistemas operativos Unix y Unix-como el uso.

Garrett Wollman describe la razón de esto en un FreeBSD PR entrada de la base de datos [http://www.freebsd.org/cgi/query-pr.cgi?pr=24385]:

> Estas zonas se incluyen la compatibilidad con los antiguos sistemas UNIX. Usted tienen más probabilidades de convencer a los desarrolladores de bases de datos TZ a caer por completo
> de lo que van a conseguir que cambien las definiciones. En cualquier caso, FreeBSD seguir la práctica de la base de datos TZ.

Actualmente contamos con un billete abierto para examinar este asunto confuso para pfSense 2.0. Podemos quitar todas estas zonas con GMT desde la interfaz web por completo. En este momento, se recomienda utilizar
sólo el nombre husos horarios y no las zonas con GMT.

4.7.2. Tiempo de Mantenimiento de Problemas

Puede ejecutar en el hardware que tiene problemas importantes de mantenimiento de tiempo. Todos los relojes de la PC a

la deriva

hasta cierto punto, pero usted puede encontrar un poco de hardware que se deriva tanto como un minuto por cada par de minutos que pasan y recibe completamente fuera de sincronización con rapidez. NTP está diseñado de forma periódica
actualizar la hora del sistema para dar cuenta de la deriva normal, razonablemente, no puede corregir los relojes que la deriva
de manera significativa. Esto es muy raro, pero si lo encuentro, el siguiente esquema se
las cosas que suelen solucionar este problema.

Hay cuatro cosas para comprobar si se encuentra con el hardware con el tiempo de mantenimiento de importantes problemas.

4.7.2.1. Protocolo de red Tiempo

De forma predeterminada, pfSense está configurado para sincronizar su hora con el ntp.org de tiempo de red Protocol (NTP) grupo de servidores. Esto asegura una fecha exacta y la hora en su sistema, y

cabida a la deriva reloj normal. Si la fecha de su sistema y el tiempo son correctos, asegúrese de NTP sincronización funciona. El problema más común es la prevención de la sincronización la falta de configuración de DNS correcta en el firewall. Si el servidor de seguridad no puede resolver nombres de host, el sincronización NTP fallará. Los resultados de la sincronización se muestran en el arranque de la registro del sistema.

4.7.2.2. Actualizaciones de BIOS

He visto a hardware antiguo que corrió bien durante años en el encuentro de Windows hora normal de las principales problemas después de su repliegue en FreeBSD (y en consecuencia pfSense,). Los sistemas se ejecutando una versión de varias revisiones del BIOS de la fecha. Una de las revisiones dirigió una cronometraje cuestión que al parecer nunca afectadas de Windows por alguna razón. La aplicación de la BIOS actualización solucionado el problema. Lo primero que debe comprobar es asegurarse de que tiene la última BIOS de su sistema.

4.7.2.3. PNP configuración de sistema operativo en la BIOS

Me he encontrado con otro hardware que tuvo tiempo de mantenimiento de las dificultades en FreeBSD y pfSense a menos PNP OS en el BIOS se pone en "No". Si su BIOS no tiene una configuración de PNP OS opción, buscar un "sistema operativo" ajuste y en "Otros".

4.7.2.4. Deshabilitar ACPI

Algunos proveedores de BIOS han producido ACPI (Advanced Configuration and Power Interface) implementaciones que están en el mejor de los buggy y peligrosos en el peor. En más de una ocasión han encontrado que los sistemas de arranque o no funcione correctamente si se ha desactivado la compatibilidad con ACPI en el BIOS y / o en el sistema operativo.

La mejor manera de desactivar ACPI en el BIOS. Si no hay opción de BIOS para desactivar ACPI, a continuación, puede intentar correr sin ella de dos maneras diferentes. El primer método, temporal es deshabilitar ACPI en el arranque. Temprano en el proceso de arranque, aparece un menú con varias opciones, una de los cuales es de arranque pfSense con discapacidad ACPI. Al elegir este, ACPI se desactivará para este de inicio único. Si el comportamiento mejora, entonces debería deshabilitar ACPI de forma permanente.

Para desactivar permanentemente ACPI, debe agregar un valor a la `/ Boot / device.hints` archivo. Usted Para ello, la navegación de los Diagnósticos → Editar archivo, introduzca `/ Boot / device.hints` y luego haga clic en Cargar. Añadir una nueva línea al final y luego escriba:

```
hint.acpi.0.disabled = "1"
```

A continuación, haga clic en Guardar.

Para una forma alternativa de hacer esto, a partir de diagnósticos → De comandos o desde una shell tipo, lo siguiente:

#echo "hint.acpi.0.disabled = 1">> / boot / device.hints

Nota

La `/ Boot / device.hints` archivo se sobrescribirán durante la actualización. Se consciente de que tendrá que repetir este cambio después de realizar una actualización de firmware.

4.7.2.5. Ajuste Timecounter Marco de hardware

En muy pocos sistemas, el valor sysctl kern.timecounter.hardware posible que tenga que ser cambiado a corregir un reloj inexacta. Para probar esto, vaya a Diagnósticos → Comando y ejecutar la siguientes:

#kern.timecounter.hardware sysctl-w = i8254

Esto hará que el sistema de utilizar el chip timecounter i8254, que normalmente mantiene la hora buena, pero puede no ser tan rápido como otros métodos. Las opciones timecounter otros se explicará más adelante.

Si el sistema mantiene la hora correctamente después de realizar este cambio, usted necesita para hacer este cambio permanente. El cambio anteriores no sobrevivirá a un reinicio. Examinar para diagnóstico → Edición de archivos, la carga `/ Etc / sysctl.conf`, Y añadir esto al final:

```
kern.timecounter.hardware = i8254
```

Haga clic en Guardar y, a continuación, que el establecimiento debe ser leído de nuevo en el siguiente inicio.

Alternativamente, usted podría agregue la línea utilizando un método similar al deshabilitar ACPI arriba:

#echo "kern.timecounter.hardware i8254 ="">> / etc / sysctl.conf

Nota

La `/ Etc / sysctl.conf` archivo se sobrescribirán durante la actualización. Tenga en cuenta que tendrá que repetir este cambio después de realizar una actualización de firmware.

Dependiendo de la plataforma y el hardware, también puede haber otros timecounters a intentarlo. Para una lista de timecounters disponibles se encuentran en su sistema, ejecute el siguiente comando:

#kern.timecounter.choice sysctl

A continuación, debería ver una lista de timecounters disponibles y su "calidad" según lo informado por FreeBSD:

```
kern.timecounter.choice: TSC (-100) ACPI de seguridad (850) i8254 (0)
ficticia (-1.000.000)
```

A continuación, podría tratar de probar cualquiera de los cuatro valores para el kern.timecounter.hardware sysctl ajuste. En términos de "calidad" en este listado, cuanto mayor sea el número, mejor, pero real de la facilidad de uso varía de sistema a sistema. El TSC es un contador de la CPU, sino que está vinculada a la velocidad de reloj y no es legible por otras CPUs. Esto hace que su uso en sistemas SMP imposible, y en aquellos con procesadores de velocidad variable. El i8254 es un chip de reloj que se encuentran en la mayoría del hardware, que tiende a ser seguro, pero puede tener algunos problemas de rendimiento. El contador de ACPI de seguridad, si el apoyo adecuado en el hardware disponible, es una buena opción, ya que no sufren de la limitaciones de rendimiento de i8254, pero en la práctica su precisión y la velocidad varían ampliamente dependiendo sobre la aplicación. Esto y más información sobre Timecounters FreeBSD se puede encontrar en el de papel Timecounters: Eficiente y cronometraje preciso en núcleos SMP [http://phk.freebsd.dk/pubs /] timecounter.pdf por Poul-Henning Kamp del Proyecto FreeBSD.

4.7.2.6. Ajuste la frecuencia del temporizador del kernel

En algunos casos también puede ser necesario ajustar la frecuencia del temporizador del kernel, o núcleo kern.hz armonioso. Esto es especialmente cierto en entornos virtualizados. El valor por defecto es 1000, pero en algunos casos de 100, 50 o incluso 10 será un mejor valor en función del sistema. Cuando se pfSense instalado en VMware, que detecta y configura automáticamente el 100, que debería funcionar bien en casi todos los casos con los productos de VMware. Al igual que con el timecounter ajuste anterior, para ajustar este ajuste que añadir una línea a `/ Boot / loader.conf` con el nuevo valor:

```
kern.hz = 100
```

4.8. Solución de problemas

El Asistente para la instalación y las tareas relacionados con la configuración funcionará para la mayoría, pero puede haber algunos cuestiones conseguir paquetes a fluir con normalidad en sus direcciones previsto. Algunas de estas cuestiones puede ser único para su configuración particular, pero se puede trabajar a través con algunos problemas básicos.

4.8.1. No se puede acceder desde la LAN WebGUI

Lo primero que debe verificar si usted no puede acceder a la WebGUI de la LAN es el cableado. Si están directamente la conexión de un PC cliente a un interfaz de red en un sistema de pfSense, usted puede necesitar una cable de conexión a menos que uno o dos tarjetas de red de apoyo de Auto-MDIX.

Una vez que esté seguro de que hay una luz de enlace en ambos tarjeta de red del cliente y la red LAN pfSense la interfaz, el siguiente paso es comprobar la configuración TCP / IP en el PC desde el que se tratando de conectar. Si el servidor DHCP está habilitado en el sistema de pfSense, ya que será por defecto, asegurar que el cliente también se establece para DHCP. Si el DHCP está desactivado en el sistema de pfSense, que

tendrá que codificar una dirección IP en el cliente que residen en la misma subred que el pfSense sistema de dirección IP LAN, con la misma máscara de subred, y utilizar la dirección IP LAN pfSense como su puerta de enlace y servidor DNS.

Si la configuración de cableado y la red es correcta, usted debe poder hacer ping a la IP LAN del sistema de pfSense desde el PC cliente. Si puede hacer ping, pero sigue sin poder acceder a la WebGUI, todavía hay algunas cosas más para intentarlo. En primer lugar, si el error que recibe en la PC cliente es un restablecimiento de la conexión o el fracaso, a continuación, o el demonio del servidor que ejecuta el WebGUI no se está ejecutando, o si está intentando acceder a él desde un puerto equivocado. Si el error que recibe es en cambio una conexión tiempo de espera, que apunta más hacia una regla de firewall.

Si recibe un restablecimiento de la conexión, puede que intenta reiniciar el proceso del servidor de la WebGUI consola del sistema, por lo general la opción 11. En caso de que no ayuda, iniciar un shell de la consola (opción 8), y escriba:

#sockstat | grep lighttpd

Esto debería devolver una lista de todos los procesos que se ejecutan lighttpd, y el puerto en los que se Música, así:

```
raíz lighttpd 437 9 TCP4 *: 80 *: *
```

En esa salida, muestra que el proceso está escuchando en el puerto 80 de cada interfaz, pero que puede variar según la configuración. Pruebe a conectar a la pfSense IP LAN utilizando ese puerto directamente, y con http y https. Por ejemplo, si tu IP LAN fue 192.168.1.1, y se escucha en el puerto 82, intenta **http://192.168.1.1:82** y **https: / / 192.168.1.1:82**.

Si recibe un tiempo de espera de conexión, consulte Sección 4.10, "Qué hacer si se bloquea de WebGUI ". Con una conexión de red ha configurado correctamente, esto no debería ocurrir, y que sección ofrece vías de solución de problemas regla de firewall.

También es una buena idea para corroborar que la WAN y LAN no están en la misma subred. Si WAN se establece para DHCP y está conectado detrás de otro router NAT, también pueden estar usando 192.168.1.1. Si la misma subred que está presente en WAN y LAN, resultados imprevisibles que puede suceder, incluyendo no ser capaz de enrutar el tráfico o acceder a la WebGUI. En caso de duda, desconecte el cable de WAN, reinicie el router pfSense, y vuelve a intentarlo.

4.8.2. No Internet desde la LAN

Si usted es capaz de llegar a la WebGUI, pero no en Internet, hay varias cosas a considerar.

La interfaz WAN no esté correctamente configurado, la resolución DNS puede no estar funcionando, no podría ser un problema con las reglas del firewall, las reglas NAT, o incluso algo tan simple como un local puerta de entrada cuestión.

4.8.2.1. Temas de interfaz

WAN

En primer lugar, comprobar la interfaz WAN para asegurarse de que pfSense ve como operacionales. Vaya a Estado → Interfaces, y ver el estado de la interfaz WAN allí. El estado debe mostrar como "arriba". Si muestra abajo, vuelva a revisar el cableado y la configuración de la WAN en interfaces → WAN. Si son a través de PPPoE o PPTP para el tipo de WAN, hay una línea de situación que indica si el conexión PPP está activa. Si no funciona, intente presionar el botón Conectar. Si eso no funciona, Compruebe todos los ajustes en interfaces → WAN, cheque o reiniciar el equipo ISP (Módem de cable o DSL, etc), y tal vez consultar con su ISP para obtener ayuda con respecto a la configuración que se debe utilizar.

4.8.2.2. Problemas DNS Resolución

Dentro de la WebGUI, vaya a Diagnósticos → Ping, e introduzca su dirección de puerta de enlace del ISP si saberlo. Se cotiza en estado → Interfaces para la interfaz WAN. Si usted no sabe la puerta de entrada, puede intentar alguna otra dirección conocida válida como **4.2.2.2**. Si usted es capaz de ping a esa dirección, a continuación, repetir que la prueba de ping mismo desde su PC cliente. Abra un símbolo del sistema o ventana de terminal, y ping esa misma dirección IP. Si puede hacer ping a la dirección IP, a continuación, intente ping a un sitio por su nombre como **www.google.com**. Inténtelo de la pfSense WebGUI y de la PC cliente. Si la prueba de ping IP funciona, pero no puede hacer ping por nombre, entonces hay un problema con la resolución de DNS. (Véase Figura 6.20, "la resolución Pruebas nombre para actualizaciones Bogon" para un ejemplo.) Si la resolución de DNS no funciona en el sistema de pfSense, compruebe la configuración del servidor DNS en Sistema de → Configuración general, y en Estado → Interfaces. Consulte con ping para asegurarse de que están alcanzable. Si se puede llegar a la puerta de acceso a su ISP, pero no a sus servidores DNS, puede ser aconsejable contactar con su ISP y comprueba los valores. Si los servidores DNS son obtenidos a través de DHCP o PPPoE y no se puede contactar con ellos, también puede ponerse en contacto con su proveedor de Internet sobre esa cuestión. Si todo esto falla, usted puede desear considerar el uso de OpenDNS [http://www.opendns.com/] (Véase el Sección 24.2, "filtrado de contenidos con OpenDNS") servidores de nombres en el router pfSense en lugar de los proporcionados por su ISP.

Si el DNS funciona desde el router pfSense, pero no desde un PC cliente, podría ser el reenviador DNS configuración en el sistema de pfSense, la configuración del cliente, o las reglas del cortafuegos. Fuera de la caja, pfSense tiene un promotor de DNS que se encargará de las consultas DNS para los clientes detrás del router. Si PC de los clientes están configurados con DHCP, que va a obtener la dirección IP del pfSense interfaz del router al que están conectados como un servidor DNS, a menos que especifique un reemplazo. Por ejemplo, si un ordenador está en el lado de la LAN, y el sistema de LAN de pfSense dirección IP es 192.168.1.1, a continuación, el servidor DNS del cliente también debe ser 192.168.1.1. Si ha deshabilitado el reenviador DNS, también puede ser necesario ajustar los servidores DNS que se asignan a los clientes DHCP en Servicios

→ Servidor DHCP. Normalmente, cuando el reenviador DNS está deshabilitado, el sistema de servidores de DNS son
asignados directamente a los clientes, pero si eso no es el caso en la práctica para su configuración, defina los aquí. Si el equipo cliente no está configurado para DHCP, asegúrese de que tiene la adecuada servidores DNS conjunto: o la dirección IP LAN del sistema de pfSense o servidores DNS lo interno o externo
que le gustaría para que utilice.

Otra posibilidad para DNS de trabajo de pfSense en sí, pero no un cliente local es demasiado estricta
reglas del firewall. Comprobar estado → Registros del sistema, en la pestaña Firewall. Si usted ve bloqueado las conexiones
de su cliente local tratando de llegar a un servidor DNS, entonces usted debe agregar una regla de firewall en el parte superior del conjunto de reglas para que la interfaz que permite conexiones a los servidores DNS en TCP y el puerto UDP 53.

4.8.2.3. Cliente Número de puerta de enlace

Para que el sistema de pfSense adecuadamente el tráfico de Internet de las rutas de PC de su cliente, debe
ser su puerta de enlace. Si el PC del cliente se configuran usando el servidor DHCP de pfSense, esto será ajusta automáticamente. Sin embargo, si los clientes reciben información de DHCP de un suplente DHCP servidor, o de sus direcciones IP han sido introducidos de forma manual, verifique que su puerta de enlace se establece para la dirección IP de la interfaz a la que se conectan en el sistema de pfSense. Por ejemplo, si los clientes están en el lado LAN pfSense, y es la dirección IP para la interfaz LAN de pfSense 192.168.1.1, entonces la dirección de un cliente de puerta de enlace se debe establecer en 192.168.1.1.

4.8.2.4. Firewall de Asuntos artículo

Si el defecto "Conexión a cualquier" norma se ha modificado o eliminado desde la interfaz LAN, el tráfico
intentar acceder a Internet desde los equipos cliente a través del router pfSense pueden ser bloqueados. Este debe ser fácilmente confirmado por la navegación a Estado → Registros del sistema, y busca en el servidor de seguridad ficha. Si no hay entradas que muestran bloqueado las conexiones de PC LAN tratando de llegar a
servidores de Internet, revisar su conjunto de reglas en el Firewall de Conexión → Reglas, a continuación, la ficha Conexión y hacer
los ajustes necesarios para permitir que el tráfico. Consultar Capítulo 6, Servidor de seguridad para más detalle información sobre la edición o la creación de normas adicionales.

Si funciona desde el lado de la LAN, pero no desde una interfaz territorio palestino ocupado, asegúrese de tener las normas en vigor para
permitir que el tráfico de salida. No hay ninguna regla se crea de forma predeterminada en las interfaces de territorio palestino ocupado.

4.8.2.5. NAT Cuestiones artículo

Si las reglas NAT de salida han sido cambiados de sus valores por defecto, también puede ser posible que
el tráfico de intentar llegar a la Internet no tiene NAT se aplica correctamente. Vaya a Servidor de seguridad

→ NAT, y vaya a la ficha de salida. A menos que esté seguro que usted necesita es establecer el manual, el cambio
el ajuste a la salida de generación de reglas NAT (pasarela IPsec) y luego tratar de llegar a
a Internet desde un PC cliente nuevo. Si eso no ayudó a un PC en la LAN para salir, entonces el
cuestión es probable que en otros lugares.

Si usted tiene este conjunto en Manual de generación de reglas de salida NAT (NAT avanzada de salida
(AON)), y funciona desde la LAN, pero no desde una interfaz territorio palestino ocupado, tendrá que configurar manualmente
una regla que coincide con el tráfico que viene de allí. Mira a la norma existente para LAN y ajustarlo
en consecuencia, o consulte el capítulo NAT para más información sobre cómo crear reglas de NAT de salida.
Lo mismo se aplica para el tráfico procedente de usuarios de VPN: PPTP, OpenVPN, IPsec, etc Si estos usuarios
necesidad de llegar a Internet a través de este router pfSense, se necesitan reglas NAT de salida para su
subredes. Ver Sección 7.6, "NAT Saliente" para más información.

4.9. pfSense XML del archivo de configuración

tiendas pfSense todas sus configuraciones en un archivo de configuración de formato XML. Todos los ajustes del sistema - escenarios, incluyendo los paquetes - se llevan a cabo en este archivo un. Todos los otros archivos de configuración para el sistema
los servicios y el comportamiento se generan dinámicamente en tiempo de ejecución basado en la configuración de celebrarse dentro de
el archivo de configuración XML.

Algunas personas que están familiarizados con FreeBSD y sistemas relacionados con la operación han encontrado esto de la manera difícil, cuando sus cambios en algunos archivos de configuración del sistema se sobrescribe varias veces por el sistema antes de llegar a entender que pfSense se encarga de todo automáticamente.

La mayoría de la gente nunca se necesita saber dónde reside el archivo de configuración, pero para la referencia es en `/ Cf / conf / config.xml`. Por lo general, `/ Conf /` es un enlace simbólico a `/ Cf / conf`, Por lo que también puede
ser accesible directamente desde `/ Conf / config.xml`, Pero esto varía según la plataforma y sistema de archivos
diseño.

4.9.1. Editar manualmente la configuración de su

Algunas opciones de configuración están disponibles únicamente editando manualmente el archivo de configuración, aunque esto no es necesario en la gran mayoría de los despliegues. Algunas de estas opciones están cubiertos
en otras partes de este libro.

El método más seguro y más fácil de editar el fichero de configuración es hacer una copia de seguridad
Diagnóstico → Copia de seguridad / restauración, guarde el archivo en su PC, edite el archivo y realizar los necesarios
cambios, a continuación, restaurar el archivo de configuración modificado para el sistema.

4.10. ¿Qué hacer si usted consigue acceder a la WebGUI

Bajo ciertas circunstancias usted puede encontrarse excluido de la WebGUI, sobre todo debido a la piloto de error. No tengas miedo, si esto le sucede, hay varias maneras de volver pulg Algunos métodos son un poco difícil, pero siempre debería ser posible recuperar el acceso. Lo peor de los casos escenarios requieren acceso físico. Como usted recordará a principios de este capítulo se menciona que cualquier persona con acceso físico puede pasar por alto las medidas de seguridad y ahora usted ve cómo fácil que es.

4.10.1. ¿Olvidó su contraseña

Si ha olvidado la contraseña para el sistema que se puede restablecer con facilidad con acceso a la consola. Llegar a la opción de física de la consola (teclado / monitor, o de serie) y el uso **3** para restablecer la contraseña WebGUI.

4.10.2. He olvidado la contraseña con una consola Cerrado

Si la consola está protegido por contraseña y no tengo la contraseña, no todo está perdido. Será tomar un par de reinicios para llevar a cabo, pero puede ser fija con acceso físico a la consola:

- Reiniciar el cuadro de pfSense
- Seleccione la opción 4 (modo de usuario único) desde el menú del gestor (el uno con el pfSense ASCII logo)
- Pulse Intro cuando se le pida para iniciar / bin / sh
- Volver a montar todas las particiones como regrabables:

  #/ Sbin / ufs mount-t-

- Ejecute el comando integrado de restablecimiento de contraseña:

  #/ Etc / rc.initial.password

- Siga las instrucciones para restablecer la contraseña
- Reiniciar

Ahora debería ser capaz de acceder al sistema con el nombre de usuario y contraseña por defecto de **admin** y **pfSense**, Respectivamente.

4.10.3. vs HTTP HTTPS confusión

Asegúrese de que está conectando con el protocolo adecuado, HTTP o HTTPS. Si uno no trabaja, tratar a los demás. Usted puede encontrar que hay que probar el protocolo de lo contrario en el puerto de los demás, así:

- **http://pfsensebox:443**
- **https: / / pfsensebox: 80**

Si necesita restablecer este de la consola, vuelva a la IP LAN, escriba la misma IP, y pronto se para restablecer la WebGUI volver a HTTP.

4.10.4. Acceso bloqueados con reglas de firewall

Si se bloquea de la WebGUI de forma remota con una regla de firewall, todavía puede haber esperanza. Esto no puede suceder de la LAN a menos que se desactive la norma anti-bloqueo que mantiene el acceso a la WebGUI de esa interfaz.

Tener que caminar a alguien en el lugar a través de fijación de la norma es mejor que perderlo todo!

4.10.5. Servidor de seguridad de forma remota evadir bloqueo con las reglas

Usted puede (muy temporalmente) deshabilita las reglas de firewall utilizando la consola. Puede utilizar la física consola, o si todavía son capaces de obtener a través de SSH, que también va a funcionar. Desde la consola, utilice opción 8 para iniciar un shell, a continuación, escriba:

#pfctl-d

Que desactivar el firewall. A continuación, debería ser capaz de entrar en la WebGUI desde cualquier lugar, al menos por unos minutos o hasta que se guarda algo en la WebGUI que hace que el conjunto de reglas para se vuelve a cargar (que es casi en cada página). Una vez que haya ajustado a las normas y recuperó el el acceso es necesario, activar el firewall de nuevo, escribiendo:

#pfctl-e

Alternativamente, el conjunto de reglas de carga se mantiene en `/ Tmp / rules.debug`. Si está familiarizado con la PF conjunto de reglas de sintaxis, puede editar que para arreglar el problema de conectividad y volver a cargar las reglas de este modo:

#pfctl-f / tmp / rules.debug

Después de volver a meterse en la WebGUI con ese arreglo temporal, hacer lo que el trabajo que tiene que hacer en WebGUI para hacer la revisión permanente. Al guardar las reglas de la WebGUI, que temporal conjunto de reglas se sobrescribirá.

4.10.6. Servidor de seguridad de forma remota evadir bloqueo con SSH
Túnel

Si bloqueado el acceso a la WebGUI de forma remota, pero todavía tiene acceso con SSH, entonces no es una forma relativamente fácil de conseguir en: túnel SSH.

Si la WebGUI está en el puerto 80, configurar el cliente para reenviar el puerto local 80 (o 8080, o lo que sea) al puerto remoto "localhost: 80", a continuación, dirija su navegador a **http://localhost:80** o lo de puerto local que ha elegido. Si su WebGUI está en otro puerto, utilice en su lugar. Si usted está a través de HTTPS que todavía tendrá que usar HTTPS para acceder a la WebGUI esta manera.

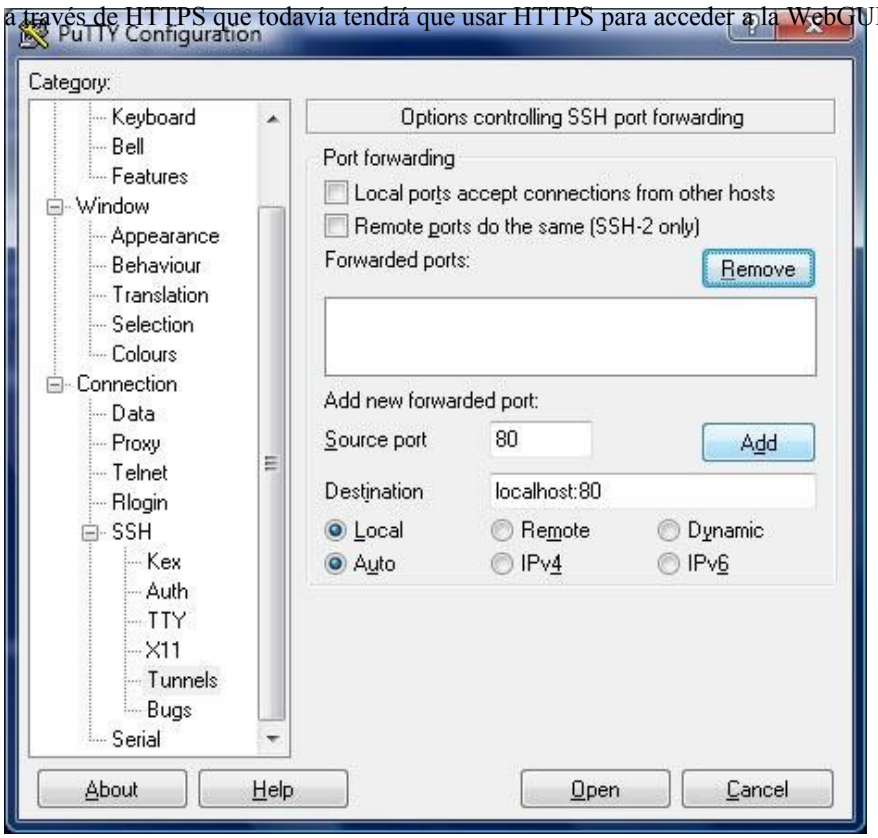


Figura 4.14. Configuración de un túnel SSH puerto 80 en PuTTY

Llene las opciones como se muestra en Figura 4.14, "Configuración de un túnel SSH puerto 80 en PuTTY", a continuación,
haga clic en Agregar. Una vez que se conecte y escriba su nombre de usuario / contraseña, puede acceder a la WebGUI utilizando el puerto redirigido locales.

4.10.7. Bloqueada debido a un error de configuración de Squid

Si accidentalmente configurar Squid para utilizar el mismo puerto que la WebGUI, y luego no pueden obtener de nuevo a arreglar la configuración, puede que tenga que arreglarlo mediante el siguiente procedimiento.

• Conecte el sistema de pfSense consola con SSH o el acceso físico

• Iniciar una concha, opción 8 de la consola.

• Terminar el proceso de calamar de este modo:

#/ Usr / local / etc / rc.d / parada squid.sh

Si eso no funciona, trate de esta manera:

#killall -9 calamar

o

#squid-k cierre

Una vez que el proceso de calamar está totalmente terminado, usted debería ser capaz de recuperar el acceso a la WebGUI. Tenga en cuenta que puede que tenga que trabajar con rapidez, o repetir el comando shutdown, como el calamar puede se reiniciará automáticamente.

4.11. Pensamientos finales de configuración

Hay millones de formas de configurar un sistema de pfSense, por lo que es imposible cubrir todos los aspectos de cada configuración y solución de problemas en este libro. En este capítulo se proporciona una visión general de algunas de las opciones de configuración general. Los próximos capítulos entrar en detalles sobre las capacidades individuales del software. Como hemos mencionado al final del capítulo introductorio, hay varias otras vías para obtener ayuda. Si ha intentado todas las sugerencias aquí y que todavía no son capaces de hacer pfSense realizar como se esperaba, hay foros, IRC, listas de correo, Búsquedas de Google, y soporte comercial. Usted es libre de adoptar el enfoque de bricolaje, o si quisiera profesionales para cuidar de la configuración para usted, el equipo de Soporte Comercial es más que capaz. Para los enlaces a los medios de soporte en línea, consulte Sección 1.9.2, "Cómo Ayuda ".

Capítulo 5. Backup y Recuperación

Gracias al archivo de configuración basado en XML utilizado por pfSense, copias de seguridad son una brisa. Todos los
configuración del sistema se llevan a cabo en un solo archivo (véase Sección 4.9, "pfSense XML de configuración Archivo "). En la gran mayoría de los casos, este archivo se puede utilizar para restaurar un sistema a pleno funcionamiento
estado idéntico a lo que se estaba ejecutando anteriormente. No hay necesidad de hacer una copia de seguridad de todo el sistema,
como los archivos de sistema de base no se modifican por una normal, correr, sistema. La única excepción es la caso de algunos paquetes, como FreeSwitch, que dispongan de datos fuera del archivo de configuración.

5.1. Estrategias de copia de seguridad

La mejor práctica es hacer una copia de seguridad después de cada cambio de menor importancia, y tanto antes como después de cada
grandes cambios (o una serie de cambios). Por lo general, una copia de seguridad inicial se toma sólo en caso de que el cambio
están haciendo tiene efectos indeseables. Una copia de seguridad después de los hechos-se toma después de evaluar el cambio
y asegurarse de que tuvo el resultado previsto. copias de seguridad periódicas son también ser de ayuda, independientemente de
cambios, especialmente en los casos en que puede ser una copia de seguridad manual se perdió por una razón u otra.

pfSense hace una copia de seguridad interna en cada cambio, y es una buena idea para descargar un manual
uno también. Las copias de seguridad automáticas realizados en cada cambio es bueno para volver a antes de
configuraciones después de los cambios han demostrado ser perjudiciales, pero no son buenos para la recuperación de desastres
están en el propio sistema y no se mantienen al exterior. Como es un proceso bastante sencillo y sin dolor,
debe ser fácil hacer un hábito de descargar una copia de seguridad de vez en cuando, y mantenerlo en un
lugar seguro. Si usted tiene una suscripción de portal.pfsense.org [https: / / portal.pfsense.org], Copias de seguridad se pueden manejar con facilidad y de forma automática para usted.

Si realiza cambios en los archivos del sistema, tales como parches personalizados o modificación de los códigos, que
Hay que recordar hacer una copia de estos cambios con la mano o con el paquete de copia de seguridad descritos en Sección 5.6, "Archivos de copia de seguridad y directorios con el paquete de copia de seguridad", ya que no será respaldada
de seguridad o restauración de la incorporada en el sistema de copia de seguridad. Esto incluye modificaciones en los archivos del sistema mencionado
en el resto del libro, como `/ Boot / device.hints`,`/ Boot / loader.conf`,`/ Etc / sysctl.conf`, Y otros.

Además de hacer copias de seguridad, también debe probarlos. Antes de introducir un sistema en
producción, es posible que desee hacer copia de seguridad de la configuración, y luego limpie la unidad de disco duro, y

luego intentar
algunas de las diferentes técnicas de restauración en este capítulo. Una vez que esté familiarizado con la forma de copia de seguridad y restaurar una configuración, es posible que desee poner a prueba periódicamente copias de seguridad en un
no-producción de la máquina o la máquina virtual. La única cosa peor que una copia de seguridad que falta es una copia de seguridad inservible!

En 1.2.x pfSense, los datos del gráfico de RRD, que se encuentra en `/ Var / db / RRD`, No está respaldada por ninguna de las
copia de seguridad de los procesos de acción. Este problema se solucionará en la próxima versión, donde los datos RRD puede ser considerado
en la copia de seguridad de archivos XML de configuración, pero esto puede no ser conveniente para algunas personas debido a la
el aumento de tamaño de este trae. Hay otras maneras de asegurarse de estos datos es una copia de seguridad, sin embargo. Ver
Sección 5.6, "Archivos de copia de seguridad y directorios con el paquete de copia de seguridad" más adelante en este capítulo.

5.2. Hacer copias de seguridad en la WebGUI

Hacer una copia de seguridad en la WebGUI es bastante simple. Diagnóstico Sólo tienes que visitar → Copia de seguridad / restauración. En
la sección de configuración de copia de seguridad de la página, asegúrese de que la zona de copia de seguridad se establece en **TODOS**, (El valor predeterminado
elección) a continuación, haga clic en Descargar configuración (Figura 5.1, "Copia de seguridad WebGUI").

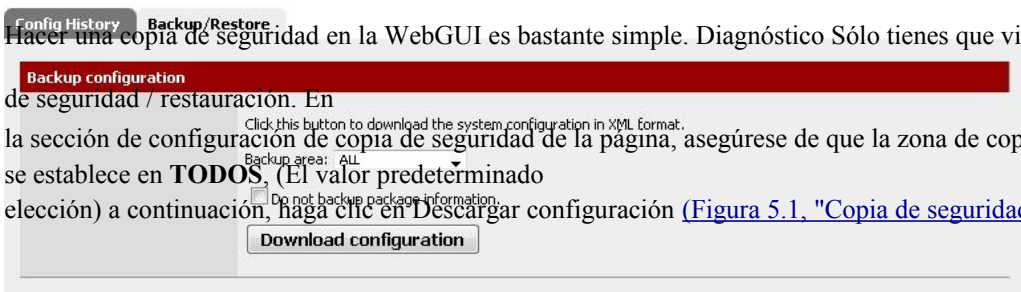


Figura 5.1. WebGUI de copia de seguridad

Tu navegador web a continuación, le pedirá que guarde el archivo en algún lugar de la PC se utiliza para ver la WebGUI. Será nombrado `config-`<*hostname*>`-`<*timestamp*>`. Xml`, Pero que puede ser cambiado antes de guardar el archivo.

5.3. Uso del Paquete AutoConfigBackup

Suscriptores de portal.pfsense.org [https: / / portal.pfsense.org] Tienen acceso a nuestro automático Configuración de copia de seguridad de servicio, AutoConfigBackup. La información más actualizada sobre AutoConfigBackup se puede encontrar en el sitio de documentación de pfSense. [http://doc.pfsense.org/index.php / AutoConfigBackup]

5.3.1. Funcionalidad y Beneficios

Cuando usted hace un cambio en su configuración, es automáticamente encriptado con la clave

entró en su configuración, a través de HTTPS y subido a nuestro servidor. Sólo cifrado

configuraciones se conservan en nuestro servidor. Esto le proporciona copia de seguridad instantánea, segura fuera del sitio de su
servidor de seguridad sin intervención del usuario.

5.3.2. pfSense Compatibilidad de versiones

El paquete AutoConfigBackup trabajará con pfSense 1.2-RELEASE y posteriores a todos
versiones incluyendo 2.0.

Nota

Hay una advertencia a la utilización de este paquete en pfSense 1.2 - la única forma de poder
empate la copia de seguridad automática en versión 1.2 es para activar a todos los filtros de recarga.
La mayoría guarda la página se activará un filtro a cargar, pero no todos.

5.3.3. Instalación y configuración

Para instalar el paquete, visite System → Paquetes y haga clic en el lado de la AutoConfigBackup
paquete. Se descargará e instalará el paquete. A continuación, haga clic en el logotipo de pfSense en la parte superior de la página, que le devolverá a la primera página, y volver a cargar sus menús. A continuación, encontrará
AutoConfigBackup en el menú de diagnóstico.

5.3.3.1. Configuración del nombre de host

Asegúrese de que tiene un nombre de dominio único y conjunto en el Sistema → Configuración General
página. Las configuraciones se almacenan por FQDN (Fully Qualified Domain Name, es decir, el nombre de host + dominio), por lo que debe asegurarse de que cada servidor de seguridad que son una copia de seguridad tiene un único nombre de dominio completo, de lo contrario
el sistema no puede diferenciar entre varias instalaciones.

5.3.3.2. Configuración AutoConfigBackup

El servicio se configura en virtud de Diagnóstico → AutoConfigBackup. En la ficha Configuración, rellene portal.pfsense.org su nombre de usuario y contraseña, e introduzca una contraseña de cifrado. Usted debe usar una contraseña larga y compleja para asegurar que su configuración es segura. Para su seguridad, conservamos sólo las configuraciones de cifrado que no sirven de nada sin la contraseña de cifrado.

Nota

Es muy importante guardar esta clave de cifrado en algún lugar fuera de su firewall
- Si lo pierde, será imposible restaurar la configuración si se pierde la
disco duro en el servidor de seguridad.

5.3.3.3. Prueba de la funcionalidad de copia de seguridad

Realice un cambio en vigor una copia de seguridad de configuración, tales como la edición y el ahorro de un cortafuegos o NAT
regla, haga clic en Aplicar cambios. Visita de los diagnósticos → AutoConfigBackup pantalla, y usted se mostrará la pestaña Restaurar, que mostrará una lista de las copias de seguridad disponibles, junto con la página que hizo el cambio (si está disponible).

5.3.3.4. Realizar copias de seguridad de forma manual

A veces, puede obligar a una copia de seguridad de su configuración. Usted puede hacer esto en la restauración ficha de la página AutoConfigBackup haciendo clic en el botón de copia de seguridad ahora en la parte inferior. Esto aparecerá un cuadro donde se puede introducir manualmente una descripción de la copia de seguridad. Es posible que desee hacer
esto antes de hacer una serie de cambios significativos, ya que te dejará con una copia de seguridad específicamente que muestra la razón de la copia de seguridad, que a su vez hace que sea fácil volver a la configuración previa de iniciar los cambios. Debido a que cada cambio en la configuración activa una copia de seguridad, al realizar una serie de cambios puede ser difícil saber por dónde empezar, si usted necesita para volver. O
puede que desee manualmente copia de seguridad antes de actualizar a una versión nueva pfSense, y el nombre copia de seguridad por lo que es claro que es la razón por la que hizo la copia de seguridad.

5.3.3.5. La restauración de la configuración

Para restaurar una configuración, haga clic en el botón a la derecha de la configuración como se muestra en el diagnóstico → AutoConfigBackup pantalla en la ficha Restaurar. Se descargará el configuración especificada de nuestro servidor, descifrarlo con su clave de cifrado, y restaurar
que. De forma predeterminada, no se reiniciará. Dependiendo de los elementos de configuración restaurada, un reinicio puede
no ser necesario. Por ejemplo, las reglas de cortafuegos y NAT se vuelve a cargar automáticamente después de la restauración de una configuración. Después de la restauración, se le pregunta si desea reiniciar el sistema. Si su restauración
configuración de nada los cambios que no sean las reglas de NAT y firewall, debe elegir Sí.

5.3.4. Restauración de metal desnudo

Si usted pierde su disco duro, a partir de ahora debe hacer lo siguiente para recuperarse en una instalación nueva.

1. Instale pfSense en el disco duro nuevo.
2. Abrir LAN y WAN, y asignar el nombre de host y de dominio exactamente la misma que fue previamente configurado.
3. Instale el paquete AutoConfigBackup.

4. Configurar el paquete AutoConfigBackup como se describió anteriormente, utilizando su cuenta de portal y la contraseña de cifrado que utilizaba anteriormente.
5. Visita la ficha Restaurar y elegir la configuración que desea restaurar.
6. Cuando se le pida que reinicie después de la restauración, que lo hagan.

Ahora estará de regreso al estado de su servidor de seguridad de el cambio de configuración anterior.

5.3.5. Comprobación del estado AutoConfigBackup

Puede comprobar el éxito de una carrera AutoConfigBackup mediante la revisión de la lista de copias de seguridad se muestra
en la ficha Restaurar. Esta lista se extrae de nuestros servidores - si la copia de seguridad está en la lista, se creado con éxito.

Si una copia de seguridad falla, una alerta se registra, y usted lo verá de desplazamiento en la parte superior de la interfaz web.

5.4. Suplente técnicas de copia de seguridad remota

Las siguientes técnicas pueden también utilizarse para realizar copias de seguridad remota, pero cada método sus propios problemas de seguridad que puede descartar su uso en muchos lugares. Para empezar, estas técnicas no cifrar la configuración, que puede contener información confidencial. Esto puede resultar en
la configuración de su transmisión a través de un enlace no es de confianza en el claro. Si tiene que usar uno de estas técnicas, lo mejor es hacerlo desde un enlace no WAN (LAN, DMZ, etc) oa través de una VPN.
El acceso a los medios de almacenamiento celebración de la copia de seguridad también deben ser controlados, si no cifrado.
El paquete AutoConfigBackup es un medio mucho más fácil y más segura de la automatización a distancia copias de seguridad.

5.4.1. Tire con wget

La configuración se puede recuperar desde un sistema remoto utilizando wget, y podría ser un guión con cron o por cualquier otro medio. Incluso cuando se utiliza HTTPS, esto no es un transporte realmente seguro desde el modo de comprobación del certificado está desactivado para dar cabida a los certificados con firma personal, lo que permite
el hombre en los ataques del medio. Al ejecutar copias de seguridad con wget a través de redes de confianza, que
debe utilizar HTTPS con un certificado que puede ser verificado por wget.
Para una HTTPS enrutador que ejecuta con un certificado con firma personal, el comando sería algo como este:

**#wget-q - no-check-certificado - post-data 'Enviar descarga =' **
**https: / /*admin*:*pfSense@192.168.1.1*/ Diag_backup.php **
-O-config*nombre de host*- `Date +% Y% m% d% H% M% S` xml.

Para un router funcionamiento regular HTTP, el comando sería:

**#wget-q - post-data 'Enviar descarga =' **
**http://*admin*:*pfSense@192.168.1.1*/ Diag_backup.php **
-O-config*nombre de host*- `Date +% Y% m% d% H% M% S` xml.

En ambos casos, cambie el nombre de usuario y la contraseña con la suya, y la dirección IP sería lo que la dirección IP es accesible desde el sistema de realización de la copia de seguridad. El sistema realizar la copia de seguridad también tendrá acceso a la WebGUI, por lo que modifica las reglas de firewall en consecuencia. La ejecución de este sobre la WAN no se recomienda, como mínimo se debe utilizar HTTPS, y restringir el acceso a la WebGUI de confianza a un conjunto de direcciones IP públicas. Es preferible hacer esto a través de VPN.

5.4.2. Empuje con SCP

La configuración también puede ser empujado en el cuadro de pfSense a otro sistema UNIX con scp. Usando scp para empujar una copia de seguridad de una sola vez con la mano puede ser útil, pero su utilización en un sistema automatizado la moda tiene sus riesgos. La línea de comandos para scp variará mucho dependiendo de su sistema configuración, pero puede verse como:

**#scp / cf / conf / config.xml **
***usuario@backuphost*: Backups/config- `hostname` - `date +% Y% m% d% H% M% S` xml.**

Con el fin de impulsar la configuración de una manera automatizada que tendría que generar un SSH clave sin contraseña. Debido a la naturaleza insegura de una clave sin contraseña, lo que genera como una llave se deja como ejercicio para el lector. Esto añade cierto grado de riesgo debido al hecho de que cualquier persona con acceso a ese archivo tiene acceso a la cuenta designada, sin embargo porque la clave es mantenerse en el servidor de seguridad donde el acceso está muy restringido, no es un riesgo considerable en la mayoría de escenarios. Si lo hace esto, garantizar que el usuario remoto está aislada y tiene poco o nada de privilegios en el sistema destino. Un un entorno chroot SCP puede ser conveniente en este caso. Ver la scponly shell disponibles para la mayoría de Plataformas UNIX que permite copias SCP archivo, pero niega las capacidades interactivas de acceso. Algunos versiones de OpenSSH tiene chroot apoyo incorporado para SFTP (Secure FTP). Estas medidas en gran medida limitar el riesgo de compromiso con respecto al servidor remoto, pero aún así salir de su copia de seguridad datos en peligro. Una vez que el acceso está configurado, una entrada de cron se podría añadir al sistema de pfSense invocar scp. Para obtener más información, visite la pfSense Wiki de documentación o de la búsqueda en los foros.

5.4.3. Básicas de copia de seguridad de SSH

Al igual que la copia de seguridad del SCP, hay otro método que el trabajo de un sistema UNIX otro. Este método no invoca el SCP / SFTP capa, que en algunos casos puede no funcionar correctamente si un sistema está ya en un estado fallido.

#ssh root *@192.168.1.1* cat / cf / conf / backup.xml> config.xml

Cuando se ejecuta, esta orden dará lugar a una archivo llamado `backup.xml` en el trabajo actual directorio que contiene la configuración del sistema de pfSense remoto. La automatización de este método que utiliza cron es también posible, pero este método requiere una clave SSH sin contraseña como en el host realizar la copia de seguridad. Esta clave permitirá el acceso administrativo a su servidor de seguridad, por lo que debe estar bien controlado. (Véase Sección 4.5.2, "Secure Shell (SSH)" para los detalles de configuración de SSH.)

5.5. La restauración de copias de seguridad

Copias de seguridad no le hará mucho bien sin los medios para recuperar los archivos, y, por extensión, ponerlos a prueba. pfSense ofrece varios medios para la restauración de configuraciones. Algunos son más complicados que otros, pero cada uno debe tener el mismo resultado final: un sistema en funcionamiento idéntico a lo que estaba allí cuando la copia de seguridad se hizo.

5.5.1. Restauración de la WebGUI

La forma más fácil para la mayoría de la gente para restaurar una configuración es utilizar la WebGUI. Navegar de Diagnóstico → Copia de seguridad / restauración, y ver la sección de configuración de restauración (Figura 5.2, "WebGUI Restaurar"). Para restaurar la copia de seguridad, seleccione el área de la restauración (normalmente **TODOS**), A continuación, haga clic en Examinar. Busque el archivo de copia de seguridad en su PC y, a continuación, haga clic en el botón Restaurar configuración. La configuración se aplicará, y el firewall se reiniciará con los valores obtenidos a partir de el archivo de copia de seguridad.

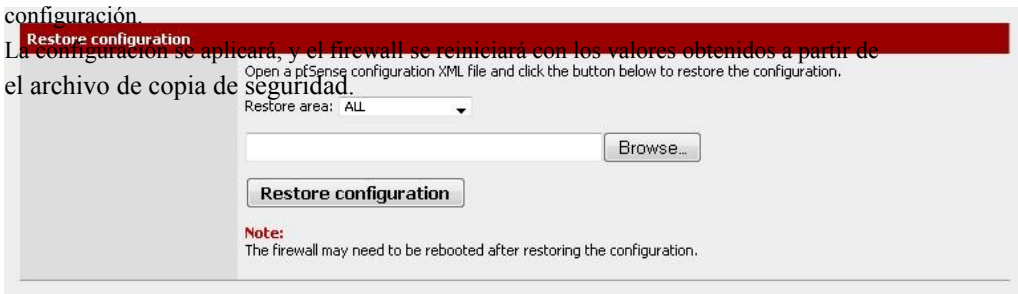


Figura 5.2. WebGUI restauración

Mientras que es fácil trabajar con, este método tiene una serie de condiciones cuando se trata de un completo restaurar a un nuevo sistema. En primer lugar, tendría que hacerse después de que el sistema de destino no es necesaria en instalado y funcionando. En segundo lugar, se requiere un PC adicional conectado a una red de trabajo (o cable cruzado) detrás del sistema de pfSense que está siendo restaurado.

5.5.2. La restauración de la Historia de configuración

En caso de problemas de menor importancia, una de las copias de seguridad interna pfSense puede ser la manera más fácil hacer una copia de un cambio. A partir de los diagnósticos → Copia de seguridad / Restaurar, haga clic en la ficha Historial de configuración (Figura 5.3, "Configuración de la Historia"). Los últimos 30 configuraciones se almacenan, junto con el actual Configuración en ejecución. Para cambiar a una de estas configuraciones anteriores, haga clic en el lado su entrada.

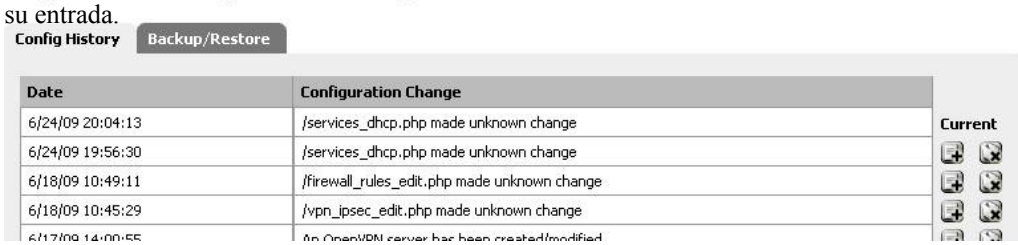


Figura 5.3. Configuración de la Historia

La configuración se puede cambiar, pero un reinicio no es automática cuando sea necesario. Cambios menores no requieren reiniciar el sistema, a pesar de revertir algunos cambios importantes. Para estar seguro, es posible que desee para reiniciar el router con la nueva configuración, vaya a Diagnósticos → Reinicie el sistema y haga clic en Sí.

configuraciones guardados anteriormente se pueden eliminar haciendo clic, pero no es necesario que los elimine por mano para ahorrar espacio, las copias de seguridad de configuración antiguos se eliminan automáticamente cuando los nuevos creado. Es posible que desee eliminar una copia de seguridad de un cambio en la configuración de malos conocidos para garantizar que no es accidental restaurado.

5.5.3. Restauración con un ISP

Cubierto en Sección 3.6, "Instalación de Recuperación", El instalador de Pre-Vuelo (PIF) se llevará a un archivo de configuración que se ha guardado en una unidad USB y restaurarla en el funcionamiento configuración durante el proceso de instalación. Este es probablemente el método más rápido para restaurar una configuración, como ocurre durante el proceso de instalación sin intervención manual en el pfSense caja. Arranca la primera vez con la nueva configuración, y usted no tendrá que preocuparse tener un PC de mano para realizar la restauración a través de la WebGUI.

5.5.4. La restauración de Montaje de la CF / HDD

Este método es popular entre los usuarios integrados. Si va a colocar la CF o disco duro del sistema de pfSense a un equipo que ejecuta FreeBSD se puede montar la unidad y copiar una nueva configuración directamente en un sistema instalado, o incluso copiar una configuración de un sistema fracasado.

Nota

También puede realizar esto en un sistema de pfSense separado en lugar de una computadora FreeBSD, pero no use un router producción activa para este fin.
En su lugar, utilizar un sistema de repuesto o un router de la prueba.

El archivo de configuración se guarda en `/ Cf / conf /` tanto para instala integrado y completo, pero la diferencia es
en el lugar donde reside este directorio. Para las instalaciones incrustadas, esto es en un segmento particular, tales como `ad0s3` si la unidad está `ad0`. Gracias a GEOM (marco de almacenamiento modular) las etiquetas en los últimos versiones de FreeBSD y en uso en sistemas de archivos incrustados NanoBSD basado en este segmento también puede tener acceso, independientemente del nombre del dispositivo utilizando la etiqueta `/ Dev / ufs / cf`. Para las instalaciones nuevas,
es parte de la división de raíz (normalmente `ad0s1a`). Los nombres de las unidades puede variar dependiendo del tipo y posición en el sistema.

5.5.4.1. Ejemplo incrustado

En primer lugar, conectar la CF a un lector de tarjetas USB en un sistema FreeBSD u otro pfSense inactivos sistema (véase la nota en la sección anterior). Para la mayoría, que se mostrará como `da0`. Usted también debe ver mensajes de la consola que refleja el nombre del dispositivo, y las etiquetas GEOM recientemente disponible.

Ahora montar la partición de configuración:

#mount-t ufs / def / ufs / cf / mnt

Si por alguna razón usted no puede usar las etiquetas GEOM, utilice el dispositivo directamente como `/ dev/da0s3`.

Ahora, una copia de configuración en la tarjeta:

**#cp / usr/backups/pfSense/config-alix.example.com-20090606185703.xml **
/ Mnt / conf / config.xml

A continuación, asegúrese de desmontar la partición de configuración:

#umount / mnt

Desconecte la tarjeta, vuelva a introducirla en el router y vuelva a encenderlo. El router debe estar en ejecución con la configuración anterior. Si desea copiar la configuración de la tarjeta, el proceso de es el mismo, pero los argumentos para el comando cp se invierten.

5.5.5. Rescate de configuración durante la instalación

También se tratan en Sección 3.6, "Instalación de Recuperación", este proceso se vuelva a instalar pfSense en un disco duro, pero mantener la configuración que está presente en esa unidad. Esto se utiliza cuando el contenidos del sistema están dañados de alguna manera, pero el archivo de configuración está intacto.

5.6. Los archivos de copia de seguridad y directorios con la copia de seguridad

Paquete

El paquete de copia de seguridad le permitirá hacer copias de seguridad y restaurar cualquier conjunto de archivos / carpetas en el
del sistema. Para la mayoría, esto no es necesario, pero puede ser útil para realizar copias de seguridad o para la RRD paquetes como FreeSwitch que pueden tener los archivos que desea guardar (por ejemplo, mensajes de voz.)
Para instalar el paquete, vaya a Sistema → Paquetes, y encuentra respaldo en la lista, y haga clic.
Una vez instalado, está disponible a partir de diagnósticos → Los archivos de copia de seguridad / Dir. Es bastante simple de usar,
como se muestra en el ejemplo siguiente.

5.6.1. Copia de seguridad de datos RRD

El uso de este paquete de copia de seguridad debe ser muy fácil de hacer una copia de seguridad de sus datos gráfico RRD (Véase el Sección 22.5, "RRD gráficos").

En primer lugar, vaya a Diagnósticos → Los archivos de copia de seguridad / Dir. Haga clic para añadir una nueva ubicación para el conjunto de copia de seguridad.
En el campo Nombre, introduzca **RRD de datos**. En el campo Ruta, escriba **/ Var / db / RRD**. Establecer Enabled
Verdadero, Y para la Descripción, escriba **Gráfico de datos RRD**. Haga clic en Guardar.

En la pantalla de copia de seguridad principal, haga clic en el botón Copia de seguridad y, a continuación se le presentará con un
el archivo a descargar que deberá contener los datos RRD junto con los otros directorios en el grupo de respaldo. Guardar en un lugar seguro, y considerar el mantenimiento de múltiples copias si los datos es muy importante para usted.

5.6.2. Restauración de datos RRD

Diagnóstico de → Copia de seguridad de archivos / Dir, haga clic en Examinar y busque un archivo de copia de seguridad que se
previamente descargados. Haga clic en Cargar, y los archivos deben ser restaurados. Debido a que la RRD archivos

sólo se tocó cuando se actualiza una vez cada 60 segundos, usted no debería tener que reiniciar el sistema o reiniciar
cualquiera de los servicios una vez los archivos se restauran.

5.7. Advertencias y Gotchas

Mientras que el archivo XML de configuración guardado por pfSense incluye todos los ajustes, lo hace
No incluye las modificaciones que se han realizado en el sistema a mano, tales como el manual de
modificaciones del código fuente. Además, algunos paquetes requieren métodos adicionales de copia de seguridad de sus datos.

El archivo de configuración pueden contener información confidencial, como claves VPN o certificados, y
contraseñas (que no sea la contraseña de administrador) en texto sin formato en algunos casos. Algunas contraseñas deben estará disponible en formato de texto en tiempo de ejecución, por lo que seguro hash de las contraseñas imposible.
Cualquier confusión sería trivial de invertir para cualquier persona con acceso al código fuente - es decir,
todo el mundo. Una decisión consciente de diseño se hizo en m0n0wall, y continuó en pfSense, a
dejar las contraseñas en claro para que sea sumamente claro que el archivo contiene contenido delicado
y deben ser protegidas como tales. Por lo tanto usted debe proteger las copias de seguridad de estos archivos en algunos manera. Si los almacena en un medio extraíble, tenga cuidado con la seguridad física de que los medios de comunicación y /
o cifrar la unidad.
Si tiene que usar la WebGUI través de la WAN sin una conexión VPN, debe por lo menos
el uso de HTTPS. De lo contrario, una copia de seguridad se transmite en claro, incluyendo cualquier información confidencial
dentro de ese archivo de copia de seguridad. Es muy recomendable que utilice un vínculo de confianza o encriptados conexión.

Capítulo 6. Servidor de seguridad

Una de las principales funciones de pfSense con independencia de la función en la que se implementa es el filtrado
tráfico. Este capítulo cubre los fundamentos de los cortafuegos, las mejores prácticas, y la información que necesidad de configurar reglas de firewall que sea necesario para su entorno.

6.1. Fundamentos de cortafuegos

Esta sección trata principalmente con los conceptos de servidor de seguridad de introducción y sienta las bases para ayudar a entender la mejor manera de configurar correctamente las reglas del firewall en pfSense.

6.1.1. Terminología básica

Regla y conjunto de reglas son dos términos utilizados en este capítulo. Norma se refiere a una sola entrada en su firewall → Reglas pantalla. Una norma es una configuración o una acción para saber cómo mirar o manejar tráfico de la red. Conjunto de reglas se refiere a todas las reglas de firewall en su conjunto. Esta es la suma de todos los usuarios
configurado y se añaden automáticamente las normas, que están cubiertos más largo de este capítulo.

En pfSense, conjuntos de reglas se evalúan en base primer partido. Esto significa que si usted lee el conjunto de reglas para una interfaz de arriba a abajo, la primera regla que coincida será el que se utiliza. Procesamiento se detiene después de llegar a este partido y luego la acción especificada por esa regla se toma. Mantenga siempre Teniendo esto en cuenta al crear nuevas reglas, especialmente cuando se están elaborando normas para restringir el tráfico. Las reglas más permisivas siempre debe ser hacia la parte inferior de la lista, por lo que las restricciones o se pueden hacer excepciones por encima de ellos.

6.1.2. Filtrado con estado

pfSense es un firewall. Esto significa que sólo permiten el tráfico en la interfaz donde el el tráfico se inicia. Cuando se inicia una conexión que coincidan con una regla de paso en el cortafuegos, una entrada se crea en el cuadro del estado del cortafuegos, donde la información sobre las conexiones activas a través de la servidor de seguridad se mantiene. El tráfico de respuesta a las conexiones iniciadas dentro de su red de forma automática le permitió volver a su red por la tabla de estado. Esto incluye todo el tráfico relacionado con un
protocolo diferente, como el control de los mensajes ICMP que se pueden proporcionar en respuesta a una red TCP, UDP, o con otros.

Ver Sección 4.5.9, "Advanced Traffic Shaper y Firewall" y Sección 6.6.10, "Tipo de Estado"
sobre las opciones de Estado y de los tipos.

6.1.2.1. Estado tamaño de la tabla

La tabla de estado de servidor de seguridad tiene un tamaño máximo, para evitar que el agotamiento de la memoria. Cada estado tiene aproximadamente 1 KB de memoria RAM. (Véase Sección 2.4.2.1, "las tablas de estado grande" Estado sobre las grandes tablas.) El estado por defecto tamaño de la tabla en pfSense es de 10,000. Esto significa que si usted tiene activos 10000 conexiones que atraviesan el cortafuegos, conexiones adicionales será dado de baja. Este límite puede se incrementará en la navegación con el sistema → Página de avanzada, y desplazarse hacia abajo en el tráfico Shaper y Firewall avanzado (Figura 6.1, "Aumento del tamaño de estado de la tabla a 50.000"). Introduzca el número necesario para Servidor de seguridad de Estados máximo, o deje la casilla en blanco para el valor predeterminado de 10.000. Usted puede ver el uso de su estado histórico en Estado → RRD gráficos. En la ficha Sistema, seleccione **Estados** En los gráficos desplegables.

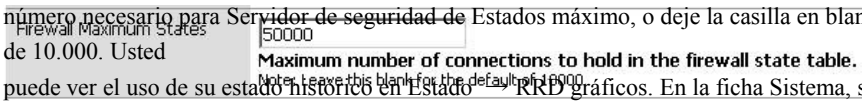


Figura 6.1. Aumento del tamaño de estado de la tabla a 50.000

6.1.3. El filtrado de entrada

El filtrado de entrada se refiere al cortafuegos de tráfico que llega a la red de Internet. En las implementaciones con multi-WAN que tienen múltiples puntos de entrada. Las condiciones de entrada por defecto en pfSense es bloquear todo el tráfico, ya que no hay reglas de permiso de WAN de forma predeterminada. Respuestas al tráfico inició desde el interior de la red, se permite automáticamente a través de la tabla de estado.

6.1.4. El filtrado de salida

El filtrado de salida se refiere al filtrado de tráfico iniciado dentro de la red destinada a la Internet o cualquier otra interfaz en el firewall. pfSense, como casi todos los comerciales y similares soluciones de código abierto, viene con una regla de LAN que permite todo, desde la salida a la LAN De Internet. Esta no es la mejor manera de operar, sin embargo. Se ha convertido en el valor predeterminado de facto en la mayoría de soluciones de servidor de seguridad, ya que es simplemente lo que más deseo de la gente. El error común es creer nada en la red interna es "digno de confianza", por lo que ¿por qué preocuparse de filtrado?

6.1.4.1. ¿Por qué debo emplear filtrado de salida?

Desde mi experiencia de trabajo con un sinnúmero de servidores de seguridad de numerosos vendedores a través de

muchas
diferentes organizaciones, empresas más pequeñas y las redes domésticas no utilizan salida

filtrado. Se puede aumentar la carga administrativa, ya que cada nueva aplicación o servicio puede requieren la apertura de puertos o protocolos adicionales en el firewall. En algunos entornos, es difícil porque los administradores no sabemos realmente lo que está sucediendo en la red, y no se atreven para romper las cosas. En otros, es imposible por razones de política laboral. Pero usted debe esforzarse para permitir sólo el tráfico mínimo requerido para salir de la red, siempre que sea posible. Estrecha salida filtrado es importante por varias razones.

1. Limitar el impacto de un sistema comprometido - malware normalmente utiliza los puertos y protocolos que no son necesarios en muchas redes. Muchos robots se basan en conexiones IRC para llamar a casa y recibir instrucciones. Algunos se utilizan puertos más comunes, como el puerto TCP 80 (normalmente HTTP) para evadir el filtrado de salida, pero muchos no lo hacen. Si no permiten el puerto TCP 6667, el habitual puerto de IRC, que puede paralizar los robots que se basan en el IRC para funcionar.

   Otro ejemplo que he visto es el caso de que la interfaz en el interior de una instalación pfSense se viendo 50 a 60 Mbps de tráfico, mientras que la WAN tenían menos de 1 Mbps de rendimiento. No se no otras interfaces en el firewall. Algunos investigación puso de manifiesto la causa como un peligro sistema en la LAN utilizando un robot que participan en una denegación de servicio distribuido (DDoS) contra un sitio web de juegos de azar chino. Se utiliza el puerto UDP 80, probablemente por un par de razones. En primer lugar,

   UDP permite enviar grandes paquetes sin completar un protocolo de enlace TCP. Con con estado servidores de seguridad son la norma, los grandes paquetes TCP no pasará hasta que el apretón de manos con éxito completado, lo que limita la eficacia de los ataques DDoS. En segundo lugar, aquellos que empleen salida filtrado son comúnmente demasiado permisiva, lo que permite TCP y UDP, TCP, donde sólo se requiere, como en el caso de HTTP. En esta red, el puerto UDP 80 no fue permitido por el conjunto de reglas de salida, por lo que todos los DDoS estaba realizando estaba golpeando la interfaz interna del servidor de seguridad con el tráfico que se estaba caído. Estaba buscando en el servidor de seguridad de una razón no relacionada y encontré esto, sino que era feliz avanzaba a sin degradación del rendimiento y el administrador de la red no sabía lo que estaba sucediendo.

   SMTP saliente es otro ejemplo. Sólo se debería permitir SMTP, el puerto TCP 25, para dejar la red de su servidor de correo. O si tu servidor de correo alojadas en servidores externos, sólo permiten sus sistemas internos para hablar con ese sistema específicos no incluidos en el puerto TCP 25. Esto evita que cualquier otro sistema en la red se utilice como un zombie de spam, ya que su SMTP el tráfico se redujo. Esto tiene la ventaja evidente de hacer su parte para limitar el spam, y también evita que su red se agreguen a las numerosas listas de negro a través de Internet que le impide el envío de correo electrónico legítimo muchos servidores de correo.

   La solución correcta es evitar que este tipo de cosas suceda en primer lugar, pero filtrado de salida proporciona otra capa que puede ayudar a limitar el impacto si otras medidas no.

2. Prevenir un compromiso - en algunas circunstancias, filtrado de salida puede impedir que sus sistemas no se vean comprometidas. Algunas explotaciones y gusanos requieren el acceso de salida para tener éxito. Un

ejemplo más viejo pero bueno de esto es el gusano Code Red a partir de 2001. El exploit causado afectados sistemas para tirar de un archivo ejecutable a través de TFTP (Trivial File Transfer Protocol) y luego ejecutar que. Su servidor web, casi seguro que no es necesario para utilizar el protocolo TFTP, y el bloqueo TFTP a través de filtrado de salida prevenir la infección por Code Red, incluso en los servidores no actualizados. Este es en gran medida sólo es útil para detener totalmente los ataques automatizados y gusanos, como un humano real atacante se encuentra todos los agujeros que existen en el filtrado de salida y usarlos a su favor.

Una vez más, la solución correcta para la prevención de compromiso es corregir las vulnerabilidades de su red, Sin embargo filtrado de salida puede ayudar.

3. Limite el uso de aplicaciones no autorizadas - muchas aplicaciones, tales como clientes VPN, peer-to-peer software, programas de mensajería instantánea y más confían en los puertos o protocolos atípica para su funcionamiento. Mientras que un
número creciente de peer-to-peer y mensajería instantánea hop será el puerto hasta encontrar algo les permite salir de la red, muchos se verá impedido de funcionar por una salida restrictivas conjunto de reglas, y este es un medio eficaz para limitar muchos tipos de conectividad VPN.

4. Prevenir IP spoofing - esta es una razón comúnmente citada para el empleo de filtrado de salida, pero pfSense bloquea automáticamente el tráfico a través de la funcionalidad falsa antispoof PF, por lo que no es
aplicable en este caso.

5. prevenir fugas de información - ciertos protocolos no se debe permitir que salgan de su red. Ejemplos específicos pueden variar de un entorno a otro. Microsoft RPC (Remote Procedure Call) en el puerto TCP 135, NetBIOS sobre TCP y los puertos UDP 137 a 139, y SMB / CIFS (Server Message Block / Common Internet File System) de TCP y UDP 445 son ejemplos comunes de los servicios que no se debe permitir que salgan de su red. Esto puede evitar que la información sobre su red interna de fugas en la Internet, y evitará que sus sistemas de iniciar los intentos de autenticación con servidores de Internet. Estos protocolos también se incluyen en "limitar el impacto de un sistema comprometido", como se indicó anteriormente, ya que muchos gusanos se han basado en estos protocolos para funcionar en el pasado. Otros protocolos que pueden ser relevantes en su entorno se syslog, SNMP y traps SNMP. La restricción de este tráfico prevenir mal configurados los dispositivos de red de envío de registro y otros potencialmente a la información sensible en Internet. En lugar de preocuparse por lo que podría protocolos a fuga de información de la red y deben ser bloqueados, sólo permiten el tráfico que se requiere.

6.1.4.2. Enfoques para la aplicación de filtrado de salida

En una red que, históricamente, no ha empleado filtrado de salida, puede ser difícil saber lo que el tráfico es realmente necesario. En esta sección se describen algunos enfoques para la aplicación de egreso filtrado en la red.

6.1.4.2.1. Deje que lo que conocemos, bloquear el resto, y el trabajo a través de la lluvia

Un enfoque es agregar reglas de firewall para el tráfico que usted conoce necesita estar permitido. Comience con hacer una lista de cosas que sabemos que son necesarios, como en Tabla 6.1, "tráfico de la salida necesaria".

Descripción	IP de origen	IP de destino	Puerto de destino
HTTP y HTTPS de todos los hosts	cualquier	cualquier	TCP 80 y 443
SMTP de correo	IP del servidor de correo	cualquier	TCP 25
Recursiva DNS consultas de los internos Servidores DNS	IP del servidor DNS	cualquier	TCP y UDP 53

Tabla 6.1. Salida de tráfico necesarios

A continuación, configure las reglas de firewall en consecuencia, y dejó caer todo lo demás.

6.1.4.2.2. el tráfico de registro y análisis de los registros

Otra alternativa es habilitar el registro en las reglas de su pase, y enviar los logs a un servidor syslog, donde se puede analizar para ver lo que el tráfico se salga de su red. Dos análisis de registros paquetes con soporte para formato de registro PF son fwanalog[1] y Hacha[2]. Usted puede encontrar más fácil de analizar los registros con un script personalizado, si usted tiene experiencia con el análisis de archivos de texto. Este ayudará a crear el conjunto de reglas necesarias con menos consecuencias que debe tener una mejor idea de lo que el tráfico es necesario en la red.

6.1.5. Bloque vs Rechazar

Hay dos maneras de no permitir el tráfico en las reglas del cortafuegos pfSense - bloquear y rechazar. El bloque Marco silencio gotas de tráfico. Este es el comportamiento por defecto de la regla de denegación de pfSense, por lo tanto, en un configuración por defecto, todo el tráfico iniciado desde Internet se redujo en silencio.

Rechazar envía una respuesta al negar tráfico TCP y UDP, dejando que el host que inició el tráfico Sabemos que la conexión fue rechazada. Rechazado el tráfico TCP recibe un TCP RST (reset) en respuesta, y rechazó el tráfico UDP recibe un mensaje ICMP inalcanzable en respuesta. Aunque usted puede especificar rechazo de cualquier regla de firewall, los protocolos IP que no sean TCP y UDP no son capaces de ser rechazado -

1
2

estas normas en silencio caerá otros protocolos IP. Esto se debe a que no existe un estándar para rechazar otros protocolos.

6.1.5.1. ¿Debo usar el bloque o rechazar?

Ha habido mucho debate entre los profesionales de la seguridad en los últimos años en cuanto al valor de bloque frente a rechazar. Algunos argumentan que el uso de bloque tiene más sentido, alegando que "ralentiza" atacantes de exploración de Internet. Cuando se utiliza rechazar, una respuesta se envía de nuevo inmediatamente que el puerto está cerrado, mientras que el bloque silenciosamente descarta el tráfico, haciendo que el escáner del atacante puerto
esperar una respuesta. Este argumento en realidad no tienen agua porque cada lector buen puerto
puede escanear cientos o miles de hosts al mismo tiempo, y no está allí sentado esperando un
respuesta de los puertos cerrados. Hay una diferencia mínima en el consumo de recursos y
velocidad de exploración, pero tan leve que no debe ser una consideración. Si bloquea todo el tráfico de la Internet, hay una diferencia notable entre el bloque y rechazar - nadie sabe su sistema es
realmente en línea. Si usted tiene incluso un único puerto abierto, el valor es mínimo porque el atacante sabe que se encuentra en línea, y también saber qué puertos están abiertos o no rechace bloqueado conexiones. Si bien no es un valor importante en el bloque más de rechazar, le recomiendo siempre utilizando el bloque de las reglas de la WAN.
Para conocer las reglas en las interfaces internas, le recomiendo usar rechazar en la mayoría de las situaciones. Cuando un host intenta
para acceder a algo que no está permitido en las reglas de su firewall, la aplicación puede acceder a él
cuelgue hasta que el cabo con el tiempo. Con el rechazo, ya que la conexión es inmediatamente rechazado, evita estas paradas. Esto es por lo general no es más que una molestia, pero en general siguen siendo
recomendamos el uso de rechazo, para evitar posibles problemas de aplicación que en silencio dejando caer el tráfico dentro de su red podría inducir. No es un efecto secundario de esto que puede ser un factor en su
elección de bloquear o rechazar. Si utiliza rechazar, se hace más fácil para las personas dentro de su red de determinar sus políticas de filtrado de salida como el servidor de seguridad, que ellos sepan lo que está bloqueando. Aún es posible para los usuarios internos para asignar las reglas de salida cuando se utiliza el bloque, sólo se necesita una poco más de tiempo y esfuerzo.

6.2. Introducción a la pantalla de Reglas de cortafuegos

Esta sección incluye una introducción y una visión general de la pantalla Reglas de cortafuegos. En primer lugar, ver para Firewall → Normas. Con ello se abre el conjunto de reglas WAN, que por defecto no tiene otras entradas que los de las redes privadas y redes de Bloque Bloque Bogon si habilitó ellos, como se muestra en Figura 6.2, "Reglas predeterminadas WAN". Si hace clic en el a la derecha de las redes privadas de bloques o Bloque redes Bogon normas, que le llevará a la página de configuración de interfaz WAN, donde estas opciones pueden ser activadas o desactivadas. (Véase Sección 6.5.1.3, "Bloque Redes Privadas" y Sección 6.5.1.4, "Redes Bloque Bogon" para más información sobre el bloqueo privado y Bogon redes.)

Figura 6.2. Predeterminado

WAN normas

Haga clic en la ficha Conexión para ver las reglas de LAN. De forma predeterminada, esto es sólo el **LAN por defecto -> cualquier** regla como se ve en Figura 6.3, "Reglas predeterminadas de LAN".

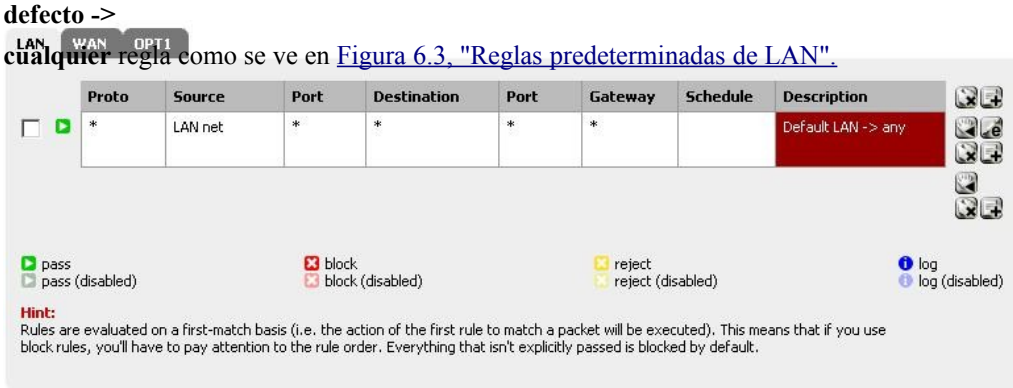


Figura 6.3. Por defecto de LAN normas

Normas para otras interfaces se pueden ver haciendo clic en sus fichas respectivas. OPT interfaces aparecen con sus nombres descriptivos, por lo que si usted designó a su OPT1 interfaz DMZ, a continuación, la ficha de sus reglas también dicen DMZ.

A la izquierda de cada regla es un icono indicador que muestra la acción del Estado - pass, bloquear o rechazar. Si está habilitado el registro para la regla, el círculo azul que contiene un i se muestra allí. Lo mismo iconos se utilizan para las reglas de movilidad reducida, excepto en el icono, como la regla, será atenuada.

6.2.1. Adición de una regla de firewall

Haga clic en cualquiera de los botones del servidor de seguridad: Reglas de la pantalla para agregar una nueva regla. La parte superior e inferior botones, como se muestra en Figura 6.4, "Añadir opciones de la regla de LAN", añadirá una nueva regla. La parte superior agrega una regla a la parte superior del conjunto de reglas, mientras que la parte inferior agrega la regla en la parte inferior.

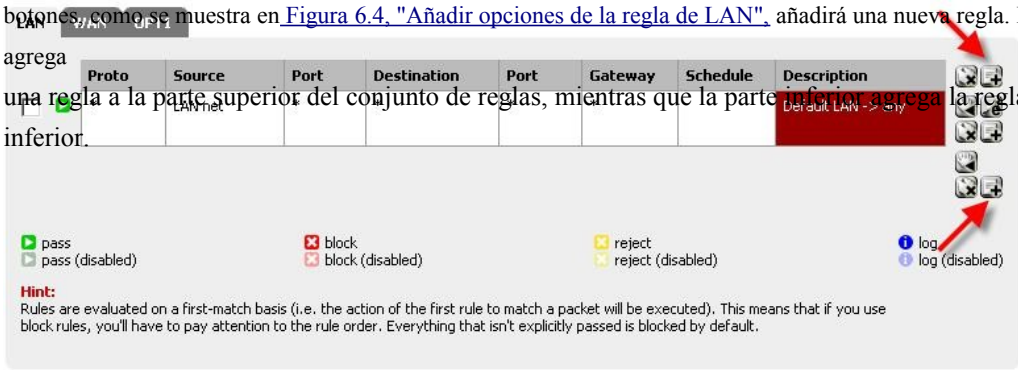


Figura 6.4. Añadir LAN opciones de la regla

Si desea hacer una nueva regla que es similar a una regla existente, haga clic en el en el final de la fila. La pantalla de edición aparecerá con la configuración de la regla existente precargada, lista ser ajustado. Para obtener más información acerca de cómo configurar la regla que se acaba de agregar, ver Sección 6.6, "Configuración de las reglas del cortafuegos".

6.2.2. Edición de reglas de firewall

Para editar una regla de firewall, haga clic en el a la derecha de la regla, o haga doble clic en cualquier parte del la línea. A continuación, será llevado a la pantalla de edición de esta norma, donde se puede hacer necesario ajustes. Ver Sección 6.6, "Configuración de las reglas del cortafuegos" Para obtener más información sobre las opciones disponible cuando se edita una regla.

6.2.3. Traslado de reglas de firewall

Las reglas pueden ser reordenados por su cuenta o en grupos. Para mover las reglas de la lista, marque la casilla a las normas que deben ser movidos, o un solo clic en la regla también se marca la casilla, a continuación, haga clic en el botón de la fila que debe estar por debajo de las normas reubicados. Cuando pasa el

más puntero del ratón una barra gruesa aparecerá para indicar que las normas se insertan. Después de hace clic en las normas y luego se introduce por encima de la fila elegida. También puede elegir las reglas de se mueven por un solo clic en cualquier lugar dentro de la fila que desee seleccionar.

6.2.4. Eliminación de reglas de firewall

Para eliminar una sola regla, haga clic a la derecha de la regla. Se le pedirá que confirme la eliminación, y si esto es lo que quería hacer, haga clic en Aceptar para eliminar realmente la regla.

Para eliminar varias reglas, marque la casilla al inicio de las filas que deben ser eliminados, a continuación, haga clic en el en la parte inferior de la lista. Las reglas también se pueden seleccionar haciendo clic en un solo lugar en su línea.

6.3. Alias

Alias le permiten a los puertos de grupo, los ejércitos, o las redes y se refieren a ellos por su nombre en el servidor de seguridad
normas, la configuración de NAT y la configuración de la talladora de tráfico. Esto le permite crear de manera significativa más corto y más manejables conjuntos de reglas. Cualquier cuadro en la interfaz web con un fondo rojo se alias ambiente.

Nota

Alias en este contexto no debe confundirse con la interfaz de alias IP, que son un medio de agregar direcciones IP adicionales para una interfaz de red.

6.3.1. Configuración de Alias

Para agregar un alias, vaya al servidor de seguridad → pantalla de Alias y haga clic en el botón. Los siguientes
secciones describen cada tipo de alias que se pueden utilizar.

En 1.2.x pfSense, cada alias está limitado a 299 miembros.

Para agregar nuevos miembros a un alias, haga clic en el en la parte inferior de la lista de entradas en el Firewall → Alias → Pantalla de edición.

6.3.1.1. Anfitrión Alias

alias de host permiten crear grupos de direcciones IP. Figura 6.5, "Ejemplo anfitriones alias" muestra un ejemplo de uso de un alias de hosts para contener una lista de servidores web públicos.

6.3.1.2. Red de Alias

alias de red le permite crear grupos de redes, o rangos de IP a través del uso de CIDR
resumen. sólo los servidores también pueden incluirse en los alias de red mediante la selección de un / 32 red
máscara. Figura 6.6, "Ejemplo de alias de red" muestra un ejemplo de un alias de red que se utiliza
más adelante en este capítulo.

6.3.1.3. Puerto Alias

Puerto alias permiten la agrupación de los puertos y rangos de puertos. El protocolo no se especifica en el
alias, más bien la regla de firewall en el que utiliza el alias definirá el protocolo como TCP, UDP, o
ambos. Figura 6.7, "Ejemplo puertos alias" muestra un ejemplo de un alias de los puertos.

6.3.2. Uso de alias

Cualquier cuadro con un fondo rojo aceptará un alias. Al escribir la primera letra de un alias
en cualquier cuadro de entrada como, una lista de alias de juego se muestra. Puede seleccionar el alias deseado,
o su escriba el nombre en su totalidad.

Nota

autocompletar Alias mayúsculas y minúsculas. Si usted tiene un alias llamado servidores web y
tipo de una minúscula "w", este alias no aparecerá. Una capital "W" se debe utilizar. Este
ya no será el caso en 2.0.

Figura 6.8, "Terminación automática de alias de los ejércitos" muestra cómo el alias configurados como servidores web
muestra en la Figura 6.5, "Ejemplo de alias de hosts" se pueden utilizar en el campo de destino cuando se añade o
edición de una regla de firewall. Seleccione "solo host o alias", a continuación, escriba la primera letra del alias que desee.
I
acaba de escribir **W** y el alias aparece como se muestra. Sólo alias del tipo adecuado se muestran. Por
campos que requieren una dirección IP o subred, único huésped y los alias de red se muestran. Para los campos
que requieren los puertos, los alias de los puertos sólo se muestran. Si hubiera varios alias a partir de
"W", la lista desplegable que aparece se muestran todos los alias correspondientes.

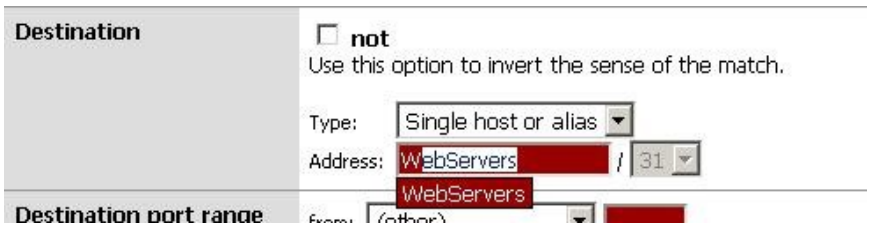


Figura 6.8. Terminación automática de alias de hosts

Figura 6.9, "Terminación automática de alias de los puertos" muestra la terminación automática de los alias de los puertos
configurado como se muestra en la Figura 6.7, "Ejemplo de alias puertos". De nuevo, si varios alias que coincida con el letra introducida, todos los alias que se pongan en venta en la lista. Puede hacer clic en el alias que desee para elegirlo.

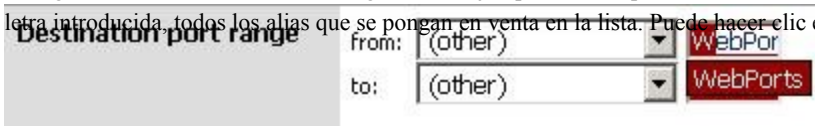
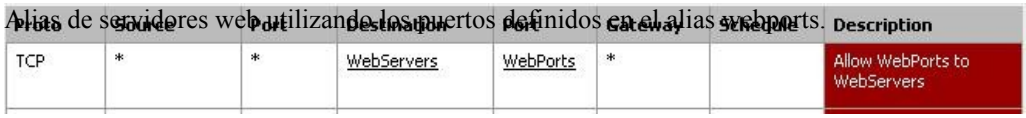


Figura 6.9. Terminación automática de alias de puertos

Figura 6.10, "Ejemplo de uso de la Regla Alias" muestra la regla que he creado con los servidores web y Webports alias. Esta regla se encuentra en la WAN, y permite a cualquier fuente para las direcciones IP se define en el Alias de servidores web utilizando los puertos definidos en el alias webports.



Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
TCP	*	*	WebServers	WebPorts	*		Allow WebPorts to WebServers

Figura 6.10. Ejemplo Artículo Uso de alias

Si pasas el ratón sobre un alias en el servidor de seguridad → Reglas de pantalla, aparece un cuadro que muestra el contenido de los alias con las descripciones incluidas en el alias. Figura 6.11, "Al pasar por muestra Ejércitos contenido " muestra esto para el alias de servidores web y Figura 6.12, "Al pasar muestra Puertos contenido " para el alias puertos.

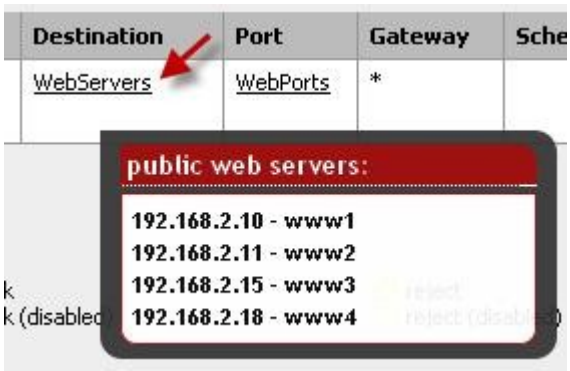


Figura 6.11. Al pasar muestra el contenido de los Ejércitos

Figura 6.12. Al pasar muestra el contenido de Puertos

6.3.3. Alias Mejoras en 2.0

pfSense 2.0 le permitirá a los alias nido dentro de otros alias, e incluirá la capacidad de introducir una dirección URL de un alias para su descarga.

pfSense 2.0 también incluye un administrador de usuario para OpenVPN, y la posibilidad de crear alias agrupación OpenVPN usuarios. Por ejemplo, los usuarios de TI pueden necesitar el acceso a su red interna, pero los demás usuarios sólo necesitan tener acceso a un pequeño subconjunto de la red. OpenVPN alias de usuario hacer tan fácil de lograr. OpenVPN se aborda con más detalle en Capítulo 15, OpenVPN.

6.4. Firewall de Mejores Prácticas artículo

Esta sección cubre algunas de las prácticas más generales a tener en cuenta a la hora de configurar el cortafuegos.

6.4.1. Denegar por defecto

Hay dos filosofías básicas de seguridad informática relacionados con control de acceso - por defecto permitir y denegar por defecto. Usted siempre debe seguir una estrategia de denegación predeterminada con el servidor de seguridad reglas. Configurar las reglas para permitir sólo el tráfico desnudo mínimo requerido para las necesidades de la red, y dejar que la caída de descanso con pfSense incorporado en su defecto regla de denegación. Al seguir esta metodología, el número de reglas de denegación en su conjunto de reglas debe ser mínima. Ellos todavía tienen un lugar para algunos usos, pero se reducirán al mínimo en la mayoría de entornos, siguiendo una estrategia de denegación predeterminada.

En una LAN predeterminado de la interfaz de configuración de dos y WAN, pfSense utiliza un defecto negar la filosofía en la WAN y permitir que un defecto en la LAN. Todo entrante desde Internet se le niega, y todo lo que a Internet desde la LAN está permitido. Todos los routers domésticos grado utilizar este metodología, al igual que todos los proyectos similares de código abierto y las ofertas comerciales más similares. Es lo que la mayoría de la gente quiere - por lo tanto, es la configuración por defecto. Sin embargo, no es la recomendada medio de la operación.

pfSense usuarios suelen preguntar "¿qué cosas malas tengo que bloquear? Esa es la pregunta equivocada, ya que se aplica a un defecto permiso de metodología. Tomó nota de la seguridad profesional Ranum Marcus incluye por defecto permiso de su "Seis ideas más tontos en Seguridad Informática" de papel, que se recomienda lectura para cualquier profesional de la seguridad.[3] Permita que sólo lo que necesita, y no dejar la por defecto que todos los pronunciarse sobre la LAN y la adición de reglas de bloqueo de "cosas malas" por encima del Estado lo permitan.

6.4.2. Que sea corto

Cuanto más corto sea el conjunto de reglas, más fácil es manejar. conjuntos de reglas largas son difíciles de trabajar, aumentar las posibilidades de error humano, tienden a ser demasiado permisiva, y mucho más difíciles de auditar. Utilizar alias para ayudar a mantener su conjunto de reglas lo más corto posible.

6.4.3. Revise su Reglamento

Usted debe revisar su manual de reglas de cortafuegos y la configuración NAT de forma periódica para asegurarse de que siguen coincidiendo con los requisitos mínimos de su entorno de red actual. La frecuencia recomendada de dicho control variarán de un entorno a otro. En

[3] http://ranum.com/security/computer_security/editorials/dumb/index.html

redes que no cambian con frecuencia, con un pequeño número de administradores del servidor de seguridad y las buenas
procedimientos de control de cambios, trimestral o semestral es generalmente adecuado. Para un rápido cambio de entornos o aquellos con pobre control de cambios y varias personas con acceso a servidor de seguridad, el configuración debe ser revisado al menos una vez al mes.

6.4.4. Documentar su configuración

En todos menos en las redes más pequeñas, puede ser difícil de recordar lo que se configura dónde y por qué.
El uso del campo Descripción de reglas de firewall y NAT es siempre recomendable. En mayor o implementaciones más complejas, también debe mantener un documento de configuración más detallada que describe la configuración de su pfSense entero. Al revisar la configuración en el futuro, esto debería ayudar a determinar qué normas son necesarias y por qué están allí. Esto también se aplica a cualquier otra área de la configuración.
También es importante tener este documento hasta la fecha. Al realizar su periódico Reseñas de configuración, es una buena idea revisar también este documento para asegurar se mantenga hasta la fecha con su configuración actual. Debe asegurarse de este documento se actualiza cada vez los cambios de configuración se realizan.

6.4.5. Reducción del ruido de registro

El registro está habilitado por defecto en la regla de denegación de pfSense de forma predeterminada. Esto significa que

todo el ruido
se bloqueen de Internet se va a registrar. A veces no se ve mucho ruido, pero en muchos ambientes se encuentra algo incesantemente correo basura a sus registros. Con conexiones con grandes dominios de difusión - una práctica comúnmente empleada por cable ISP - esto es más a menudo se transmite de NetBIOS de personas deficientes pista-que se conectan Máquinas con Windows directamente a sus conexiones de banda ancha. Estas máquinas constantemente bombear solicitudes de difusión para la navegación de la red, entre otras cosas. También puede ver el protocolo de enrutamiento del ISP, o los protocolos de redundancia de router como VRRP o HSRP. En la co-localización entornos como centros de datos, a veces se ve una combinación de todas esas cosas.
Porque no hay ningún valor en conocer el firewall bloquea 14 millones en emisiones de NetBIOS del día de ayer, y que el ruido podría encubrir los registros que son importantes, es una buena idea añadir una regla de bloqueo en la interfaz WAN para el ruido del tráfico repetido. Al añadir una regla de bloqueo sin el registro habilitado en la interfaz WAN, este tráfico seguirá siendo bloqueada, pero ya no llenan su registros.
La regla se muestra en la Figura 6.13, "las reglas de firewall para prevenir emisiones de registro" es que tengo configurado en uno de los sistemas de mi prueba, donde el "WAN" está en una LAN. Para deshacerse del registro ruido para que pueda ver las cosas de interés, he añadido esta regla para bloquear, pero no registra nada con la destino de la dirección de difusión de la subred.

Figura 6.13. Las reglas de firewall para prevenir emisiones de registro

Se deben agregar las normas similares, se pongan en venta los detalles de cualquier ruido de registro que está viendo en su
el medio ambiente. Compruebe los registros del cortafuegos en Estado → Sistema de Registros → ficha Firewall para ver qué
tipo de tráfico que son el bloqueo y la revisión de su frecuencia. Si el tráfico particular es consistente
que se registran más de 5 veces por minuto, probablemente debería añadir una regla de bloque para que reduzca el registro de ruido.

6.4.6. Registro de Prácticas

Fuera de la caja, pfSense no registra todo el tráfico pasa y registra todo el tráfico se redujo. Este es el comportamiento por defecto típico de fuente abierta y casi todos los cortafuegos comerciales. Es más prácticos, como la tala todo el tráfico pasa rara vez se debe hacer debido a los niveles de carga y registro generados. Sin embargo, esta metodología es en realidad un poco hacia atrás. el tráfico bloqueado no puede hacer daño por lo
su valor de registro es limitado, mientras que el tráfico que se pasa puede ser muy importante la información de registro haber si un sistema está en peligro. Después de eliminar cualquier ruido de bloque inútil como se describe en el sección anterior, el resto es de algún valor para fines de análisis de tendencias. Si usted está viendo significativamente mayor o menor volumen de registro de lo habitual, es probablemente bueno para investigar por qué. OSSEC, un código abierto sistema de intrusiones basado en host de detección (IDS), es un sistema que puede registros de recopilación de pfSense a través de syslog y alerta de que inicie sesión anomalías volumen.[4]

6.5. Regla Metodología

Reglas de pfSense se aplican sobre una base por interfaz, siempre en la dirección de entrada en el que interfaz. Esto significa iniciados desde la LAN se filtra utilizando las reglas de la interfaz LAN. Tráfico inicia desde el Internet se filtra a las normas de interfaz WAN. Debido a que todas las reglas de pfSense son de estado por defecto, una entrada de tabla de estado se crea cuando el tráfico coincide con una regla. Todo el tráfico de respuesta es automática permitido por esta entrada de la tabla de estado.

En este momento, no hay manera de adaptarse a las normas de salida en cualquier interfaz. De salida normas no son necesarios, porque se aplica el filtrado de la dirección de entrada de cada interfaz.
En algunas circunstancias limitadas, tales como un firewall con numerosas interfaces internas, que tienen

4http://www.ossec.net

disponibles puede reducir significativamente el número de reglas de firewall necesarias. En tal caso, podría aplicar las reglas de salida para el tráfico de Internet como las normas de salida en la WAN para evitar tener que duplicarlos para cada interfaz interna. El uso de entrada y de salida de filtrado hace cosas más complejas y más propenso a errores del usuario, pero entendemos que puede ser deseable y Esperamos dar cabida a esta de alguna manera en el futuro.

6.5.1. Se agregan automáticamente reglas de firewall

pfSense agrega automáticamente algunas reglas de firewall para una variedad de razones. En esta sección se describe toda norma agrega automáticamente y su propósito.

6.5.1.1. Anti-bloqueo de la Regla

Para evitar el bloqueo a ti mismo de la interfaz web, pfSense permite una de las reglas anti-bloqueo de por defecto. Esto se puede configurar en el sistema → Avanzada la página en WebGUI de Lucha contra el cierre patronal. Este automáticamente la regla permite el tráfico agregado de cualquier fuente dentro de la red de cualquier protocolo escuchando en la IP LAN.

En los entornos preocupados por la seguridad, debe desactivar esta regla, y configurar las reglas de LAN por lo que sólo un alias de hosts de confianza pueden tener acceso a las interfaces de administración del servidor de seguridad.

6.5.1.1.1. Restringir el acceso a la interfaz de administración de LAN

Primero tendrá que configurar las reglas del firewall si lo desea restringir el acceso a la gestión interfaces. Voy a caminar a través de un ejemplo de cómo suele configurar esto. Puedo utilizar SSH y HTTPS para la administración, por lo que crear un alias de ManagementPorts contiene estos puertos (Figura 6.14, "Alias para los puertos de gestión").

Entonces puedo crear un alias para las máquinas y / o redes que tendrán acceso a la gestión interfaces (Figura 6.15, "Alias de los ejércitos de gestión").

Los alias resultantes se muestran en la Figura 6.16, "lista Alias".

A continuación, las reglas del firewall LAN debe estar configurado para permitir el acceso a los previamente definidos los ejércitos, y denegar el acceso a todo lo demás. Hay muchas maneras que usted puede lograr esto, dependiendo sobre aspectos específicos de su entorno y cómo manejar filtrado de salida. Figura 6.17, "Ejemplo Restringido normas de gestión de LAN "y la Figura 6.18," restringido las normas de gestión de LAN - ejemplo alternativo "muestran dos ejemplos. La primera permite que las consultas DNS a la IP LAN, que es necesario si usted está utilizando el agente de DNS, y también permite a los hosts de LAN hacer ping a la IP de la LAN. A continuación, rechaza el resto del tráfico. El segundo ejemplo se permite el acceso desde la gestión de los ejércitos a los puertos de gestión, a continuación, rechaza el resto del tráfico a los puertos de gestión. Elija el

metodología que mejor se adapte a su entorno. Recuerde que el puerto de origen no es el mismo que el puerto de destino.

Una vez que las reglas del firewall se configuran, es necesario deshabilitar la regla WebGUI anti-bloqueo de el Sistema → página Avanzadas (Figura 6.19, "las reglas anti-bloqueo con discapacidad"). Marque la casilla y haga clic en Guardar.

Nota

Si ya no se puede acceder a la interfaz de administración después de desactivar el anti- regla de bloqueo, no se ha configurado las reglas de firewall adecuadamente. Se puede volver a habilitar la regla anti-bloqueo mediante el uso de la opción IP de LAN en el menú de la consola. Sólo tienes que configurar su IP actual, y el Estado automáticamente se vuelve a habilitar.

6.5.1.2. Anti-spoofing Reglamento

pfSense utiliza la función PF antispoof para bloquear el tráfico falso. Esto proporciona Unicast Invertir trazado Forwarding (uRPF) funcionalidad tal como se define en RFC 3704 [Http://www.ietf.org/rfc/rfc3704.txt].
El servidor de seguridad comprueba cada paquete contra su tabla de enrutamiento, y si un intento de conexión viene de una dirección IP de origen en una interfaz donde el servidor de seguridad de la red sabe que no reside, se ha caído.
Por ejemplo, algo que viene de la WAN con una IP de origen de una red interna se ha caído.
Todo inició en la red interna con una dirección IP de origen que no residen en el interior la red se cae.

6.5.1.3. Bloque de redes privadas

La opción Bloquear las redes privadas en la interfaz WAN pone automáticamente en una regla de bloque para RFC 1918 subredes. A menos que tenga un espacio IP privado de la WAN, se debe permitir esto. Este sólo se aplica al tráfico iniciado en el lado WAN. Puede acceder a los hosts de redes privadas desde el interior. Esta opción no está disponible para el TPP interfaces WAN de pfSense 1.2.x, pero es en 2.0. Puede agregar manualmente una regla para bloquear redes privadas en el territorio palestino ocupado interfaces WAN
la creación de un alias que contiene el RFC 1918 subredes y la adición de una regla de firewall en la parte superior de su OPT normas de interfaz WAN para bloquear el tráfico con una fuente de juego ese alias. (Véase Sección 1.7.1.1, "Direcciones IP privada" Para obtener más información acerca de direcciones IP privadas.)

6.5.1.4. Bloque Redes Bogon

redes Bogon son los que nunca debe ser visto en Internet, incluidos los reservados y sin asignar espacio de direcciones IP. Estas redes no debe ser visto como IP de origen en Internet,

e indicar ya sea el tráfico falso, o una subred no utilizados que ha sido secuestrado por un uso malicioso. pfSense proporciona una lista bogons que se actualiza según sea necesario. Si usted tiene redes Bloque Bogon habilitado, el servidor de seguridad obtendrá una lista actualizada bogons el primer día de cada mes a partir de `files.pfsense.org`. El guión corre a las 3:00 am hora local, y duerme una cantidad aleatoria de tiempo hasta 12 horas antes de realizar la actualización. Esta lista no cambia con mucha frecuencia, y nuevas asignaciones de IP se quitan de la lista bogons meses antes de que sean realmente utilizadas, por lo que la actualización mensual es suficiente. Asegúrese de que su firewall puede resolver nombres de host DNS, de lo contrario la actualización fallará. Para asegurarse de que puede resolver DNS, vaya a Diagnósticos → Ping, y tratar de hacer ping **files.pfsense.org** como se demuestra en Figura 6.20, "Prueba de resolución de nombres para actualizaciones Bogon ".

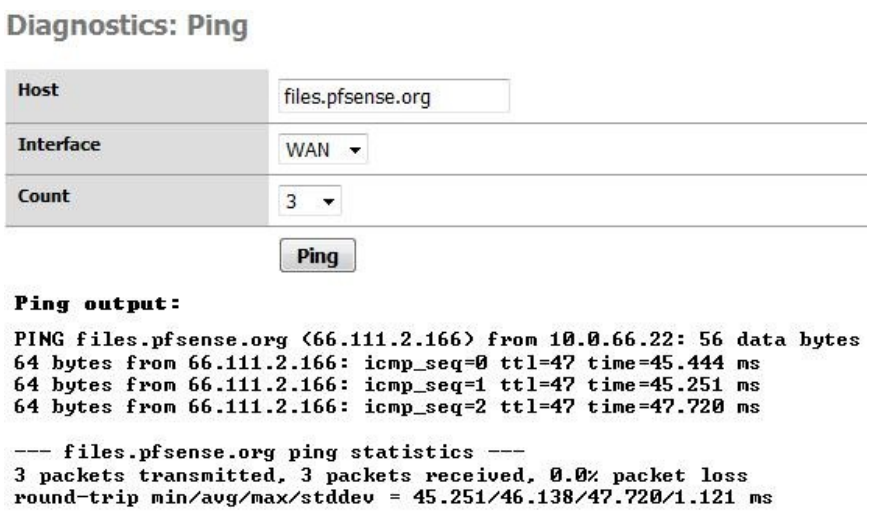


Figura 6.20. Prueba de la resolución de nombres para las actualizaciones Bogon

6.5.1.4.1. Forzar una actualización bogons

Con los cambios relativamente frecuentes a la lista bogons, y previo aviso de los nuevos IP pública asignaciones, la actualización bogons mensual es suficiente. Sin embargo puede haber situaciones en las que desea forzar manualmente una actualización Bogon, como si las actualizaciones han estado fallando Bogon debido a una incorrecta configuración de DNS. Puede ejecutar una actualización a través de la interfaz web Diagnóstico → pantalla de comandos, ejecutando / etc / rc.update_bogons.sh ahora. El argumento ahora siguiendo el guión es importante porque le dice a la secuencia de comandos para ejecutar de inmediato y el sueño no.

6.5.1.5. IPsec

Cuando se habilita un sitio a sitio de conexión IPsec, las reglas se agregan automáticamente permitiendo que el extremo remoto del túnel dirección IP de acceso al puerto UDP 500 y el protocolo ESP en la WAN dirección IP utilizada para la conexión. Cuando los clientes móviles de IPsec es activado, el puerto UDP 500 y tráfico ESP se permite a partir de cualquier fuente.

Debido a la política de manera de enrutamiento obras, el tráfico que coincide con una regla que especifica una puerta de enlace se verán obligados a Internet y evitar el procesamiento IPsec. Cuando usted tiene una regla de especificar una puerta de enlace en la interfaz que contiene dentro de la subred utilizada por la conexión IPsec, y el destino de la regla es "todo", por regla general se añade automáticamente a negar la política de enrutamiento para el tráfico destinado a la subred remota VPN.

Agrega automáticamente reglas de IPsec se discuten en mayor profundidad en Capítulo 13, IPsec.

6.5.1.6. PPTP

Cuando se habilita el servidor PPTP, reglas ocultas se agregan automáticamente permitiendo que el puerto TCP 1723 y el GRE (Generic Routing Encapsulation) protocolo para la dirección IP de WAN de cualquier dirección IP de origen. Más información acerca de estas normas se pueden encontrar en Sección 12.3, "VPNs y Reglas de cortafuegos ".

6.5.1.7. Denegar por defecto el artículo

Normas que no coinciden con ninguna de las reglas definidas por el usuario ni ninguna de las otras reglas se agregan automáticamente silencio bloqueada por la regla de denegación por defecto (como se explica en Sección 6.4.1, "Denegar por defecto").

6.6. Configuración de reglas de firewall

Esta sección cubre cada opción individual disponibles en el servidor de seguridad → Reglas → Pantalla de edición la hora de configurar reglas de firewall.

6.6.1. Acción

Aquí es donde puede especificar si el Estado va a pasar, bloquear o rechazar el tráfico. Cada uno de ellos es cubiertos anteriormente en este capítulo.

6.6.2. Personas de movilidad reducida

Si desea desactivar una regla sin eliminarla de la lista de reglas, marque esta casilla. Todavía se mostrar en su pantalla de reglas de firewall, pero en gris para indicar su estado de discapacidad.

6.6.3. Interfaz

La caída de la interfaz de abajo especifica la interfaz en la que se aplicará la regla. Recuerde que el tráfico sólo es filtrada en la interfaz donde se inicia el tráfico. Tráfico inicia desde su LAN destinados a la Internet o cualquier otra interfaz en el servidor de seguridad es filtrada por el conjunto de reglas de LAN.

6.6.4. Protocolo

Aquí es donde se especifica el protocolo de esta regla partido. La mayoría de estas opciones son auto-explicativo. TCP / UDP coincidirá con el tráfico TCP y UDP. Especificación de ICMP hará otra lista desplegable aparece donde puede seleccionar el tipo de ICMP. Varios otros comunes protocolos están también disponibles.

6.6.5. Fuente

Aquí es donde se especifica la dirección IP de origen, subred, o alias que coincida con esta regla. Usted También puede marcar la casilla no para negar el partido.

Para el tipo que señale: Cualquiera, que coincidirá con cualquier dirección; solo host o alias, que coincidirá con una única dirección IP / nombre de host o nombre de alias, o de redes, que se llevará a la vez un dirección IP y la máscara de subred para que coincida con un rango de direcciones. Por último, hay varios disponibles presets que pueden ser muy útiles en lugar de entrar en estas direcciones a mano: Dirección de WAN, LAN dirección de subred LAN, los clientes PPTP, PPPoE y usuarios.

Para conocer las reglas a través de TCP y / o UDP, también puede especificar el puerto de origen aquí haciendo clic en el El botón Avanzado. El puerto de origen se oculta detrás del botón Opciones avanzadas, ya que se normalmente quiere dejar el puerto de origen en "cualquier", como las conexiones TCP y UDP son de origen desde un puerto aleatorio en el intervalo de puerto efímero (entre 1024 a 65535, el rango exacto utiliza variables dependiendo del sistema operativo y versión del sistema operativo que inicia la conexión). La fuente puerto casi nunca es el mismo que el puerto de destino, y no se lo debe configurar como tal a menos que sepa la aplicación que está utilizando emplea este comportamiento atípico. También es seguro que definir su puerto de origen en un rango de 1024 a 65535.

6.6.6. Fuente OS

Una de las características más singulares de la PF y, por tanto pfSense es la posibilidad de filtrar por el sistema operativo iniciar la conexión. Para conocer las reglas del PCT, pf permite al sistema operativo pasiva toma de huellas digitales que le permite crear reglas basadas en el sistema operativo de iniciar el protocolo TCP conexión. La característica p0f de pf determina el sistema operativo en uso mediante la comparación de las características de la
TCP SYN paquete que inicia las conexiones TCP con un archivo de huellas dactilares. Tenga en cuenta que es posible

cambiar la huella digital de su sistema operativo para parecerse a otro sistema operativo, especialmente en abierto
sistemas operativos de código como la BSD y Linux. Esto no es fácil, pero si usted tiene técnico
usuarios de dominio con el administrador o el acceso de root a los sistemas, es posible.

6.6.7. Destino

Aquí es donde se especifica la dirección IP de destino, subred, o alias que coincida con esta regla.

Véase la descripción de la opción Fuente de Sección 6.6.5, "Fuente" para más detalles. Al igual que con la Marco Dirección de origen, usted puede comprobar, no para negar el partido.

Para reglas que especifican TCP y / o UDP, el puerto de destino, rango de puertos, o alias se especifica también aquí.

6.6.8. Registrarse

Esta casilla determina si los paquetes que coincidan con esta regla se registra en el registro del cortafuegos.
El registro es discutido en más detalle en Sección 6.4.6, "Registro de Prácticas".

6.6.9. Opciones avanzadas

Esta sección le permite configurar las capacidades de gran alcance pf de limitar los estados servidor de seguridad en función de cada regla.

De forma predeterminada, no hay límites establecidos para cualquiera de estos parámetros.

6.6.9.1. límite de conexiones de cliente simultáneas

Esta opción especifica el número de entradas total del estado puedan existir para esta regla. Si esto se establece en 10, y hay 10 conexiones que coincidan con la regla, el 11 será dado de baja. Podría ser de 10 diferentes
los ejércitos, o 9 conexiones en un host y una en otra, es el total que importa.

6.6.9.2. Máxima de las entradas del estado por host

Si prefiere límite basado en conexiones por host, este valor es lo que quieres. El uso de este configuración, puede limitar la regla a 10 conexiones por host de origen, en lugar de 10 conexiones totales.

6.6.9.3. Máximo nuevas conexiones / por segundo

Este método de limitación de velocidad puede ayudar a asegurar que una tasa de conexión de alta no sobrecargar un servidor o su tabla de estado. Por ejemplo, los límites se pueden colocar en las conexiones entrantes a un correo servidor para reducir la carga de ser sobrecargado por contra spam bots. También se puede utilizar en salida las normas de tráfico para establecer límites que impidan a cualquier máquina de una sola carga de su tabla de estado

o hacer conexiones rápidas demasiados, los comportamientos que son comunes con los virus. Usted puede establecer
una conexión de cantidad y un número de segundos para el período de tiempo. Cualquier dirección IP superior
que el número de conexiones dentro del plazo establecido serán bloqueadas durante una hora. Detrás de la escenas, esto es manejado por el cuadro virusprot, llamado así por su finalidad típica de la protección antivirus.

6.6.9.4. Estado de tiempo de espera en segundos

Aquí se puede definir un tiempo de espera de estado para el tráfico que coincidan con esta regla, anulando por defecto del sistema
estado de tiempo de espera. Las conexiones inactivas se cerrará cuando la conexión ha estado inactivo durante
esta cantidad de tiempo. El tiempo de espera de estado por defecto depende del algoritmo de optimización del servidor de seguridad en
uso. Las opciones de optimización se tratan en Sección 4.5.9.3, "Opciones de Firewall de optimización"

6.6.10. Estado Tipo

Hay tres opciones para el seguimiento del estado en pfSense que se pueden especificar para cada regla.

6.6.10.1. mantener el estado

Este es el valor predeterminado, y lo que debe casi siempre uso.

6.6.10.2. Estado synproxy

Esta opción hace que pfSense para poder conexiones TCP entrantes. conexiones TCP comenzar con un apretón de manos de tres vías. El primer paquete de una conexión TCP es un SYN de la fuente, que provoca una respuesta SYN ACK del destino. Esto ayuda a proteger contra un tipo de negación Servicio de ataque, inundaciones SYN. Esto es típicamente utilizado con las normas en las interfaces WAN. Este tipo de ataque no es muy común hoy en día, e incluye todos los principales sistemas operativos modernos capacidad de manejar esto por sí solo. Podría ser útil al abrir los puertos TCP a los anfitriones que no se ocupan de abuso de la red también.

6.6.10.3. ninguno

Esta opción no mantener el estado de esta regla. Esto sólo es necesario en algunos altamente especializados escenarios avanzados, ninguno de los cuales se tratan en este libro, ya que son extremadamente raros. Nunca debería haber una necesidad para el uso de esta opción.

6.6.11. N Sync XML-RPC

Al marcar esta casilla impide que esta norma a partir de la sincronización con otros miembros de la CARP. Esto es cubiertos en Capítulo 20, Firewall de redundancia / alta disponibilidad.

6.6.12. Lista

Aquí puede seleccionar un programa que especifica los días y horas esta norma estará en vigor. Selección de "Ninguno", la regla siempre se activará. Para obtener más información, consulte Sección 6.9, "Tiempo Reglas de base " más adelante en este capítulo.

6.6.13. Gateway

Gateway le permite especificar una interfaz WAN o en la piscina equilibrador de carga para el tráfico que coincidan con esta regla para su uso. Esto se trata en Capítulo 11, Múltiples conexiones WAN.

6.6.14. Descripción

Escriba una descripción aquí para su consulta. Esto es opcional, y no afecta a la funcionalidad de la regla. Usted debe entrar en algo aquí que describe el propósito de la regla. El máximo longitud es de 52 caracteres.

6.7. Métodos de utilización de direcciones IP públicas adicionales

Si sólo tiene una única dirección IP pública, puede pasar a la siguiente sección. Los métodos de el despliegue de más direcciones IP públicas puede variar dependiendo de cómo se asignan, como muchos le han asignado, y los objetivos de su entorno de red. Para uso público adicional IPs con NAT, es necesario configurar direcciones IP virtuales. También tiene dos opciones para asignar directamente IPs públicas a los anfitriones con el enrutamiento y subredes IP pública puente.

6.7.1. Elegir entre rutas, puentes, y NAT

Usted puede usar su IP pública adicional directamente a la asignación de los sistemas que se uso de ellos, o mediante el uso de NAT.

6.7.1.1. Direcciones IP adicionales a través de DHCP

Algunos proveedores le obligan a obtener las direcciones IP adicionales a través de DHCP. Esto ofrece una flexibilidad limitada en lo que puede hacer con estas direcciones, dejándote con dos opciones viables.

6.7.1.1.1. Puente

Si quiere que el IP adicionales asignados directamente a los sistemas que los utilizan, es puente su única opción. Utilice una interfaz OPT puente con WAN para estos sistemas.

6.7.1.1.2. Pseudo multi-WAN

Su única opción para tener el firewall tire estas direcciones como arrendamientos es una pseudo multi-WAN implementación. Instale una interfaz de red por IP pública, y configurarlos para DHCP. Enchufe todos los las interfaces en un interruptor entre el cortafuegos y el módem o router. Puesto que usted tiene múltiples interfaces de compartir un único dominio de difusión, tendrá que marcar la casilla a "Esto ARP suprimir mensajes cuando interfaces de compartir la misma red física" en el Sistema de → Página de avanzada para eliminar ARP advertencias en sus registros que son normales en este tipo de la implementación.

El único uso de múltiples direcciones IP pública asignada de esta forma es para el reenvío de puertos. Usted puede configurar el puerto hacia delante en cada interfaz WAN que se utiliza la dirección IP asignada a la interfaz por su proveedor de Internet del servidor DHCP. Salida NAT para el territorio palestino ocupado WAN no funcionará debido a la limitación de que cada WAN debe tener una puerta de enlace IP única a cabo adecuadamente el tráfico directo de que WAN. Esto se discute más en Capítulo 11, Múltiples conexiones WAN.

6.7.1.2. Adicional direcciones IP estáticas

Métodos de utilización de direcciones IP adicionales estáticos públicos pueden variar según el tipo de cesión. Cada uno de los escenarios comunes que se describe aquí.

6.7.1.2.1. Única subred IP

Con una subred IP pública única, una de las IPs públicas será en el router arriba, comúnmente que pertenecen a su ISP, con una de las direcciones IP asignadas a la IP WAN de pfSense. El resto de direcciones IP se puede utilizar con NAT, tendiendo un puente o una combinación de los dos. Para usarlos con NAT, agregue ARP proxy o carpa VIP. Para asignar direcciones IP pública directamente a las máquinas detrás del firewall, se le necesidad de una interfaz dedicada para los anfitriones que se enlaza a WAN. Cuando se utiliza con puente, el hosts con la IP pública directamente afectados deberán utilizar la puerta de enlace predeterminada mismo que el de la WAN cortafuegos, el router del ISP aguas arriba. Esto creará dificultades si los hosts con direcciones IP públicas deben iniciar las conexiones a las máquinas detrás de otras interfaces de su servidor de seguridad, ya que la puerta de enlace ISP no la ruta de tráfico para las subredes internas de nuevo a su servidor de seguridad. Figura 6.21, "público múltiple IPs en uso - solo bloque de IP "se muestra un ejemplo del uso de múltiples direcciones IP públicas en un solo bloque con una combinación de NAT y puente. Para información sobre la configuración, NAT se discute más en Capítulo 7, Network Address Translation, y reducir en Capítulo 9, Puente.

6.7.1.2.2. Pequeña subred IP WAN con mayor LAN subred IP

Algunos ISP le dará una pequeña subred IP que el "WAN" cesión, y una ruta más grande "Dentro" de subred para la final de la subred de la WAN. Comúnmente se trata de un 30 / de la WAN, y

un / 29 o mayor para el interior. router del proveedor se le asigna uno de los extremos de la / 30, por lo general la
más bajo de propiedad intelectual, y el servidor de seguridad se le asigna la propiedad intelectual más alto. El proveedor entonces las rutas de la subred LAN
al teléfono IP de la WAN. Puede utilizar las direcciones IP adicionales en una interfaz de enrutado con IPs públicas directamente
asignado a los hosts, o con NAT con otras personalidades, o una combinación de los dos. Dado que los proyectos de investigación
se dirigen a usted, ARP no es necesaria, y no necesita ninguna de las entradas VIP para el uso con 1:1 NAT.
Debido a pfSense es la entrada en el segmento de OPT1, enrutamiento de OPT1 anfitriones a LAN es mucho
más fácil que en el escenario de un puente necesario cuando se utiliza un único bloque IP pública. Figura 6.22, "Múltiples IPs públicas en el uso - a dos cuadras de propiedad intelectual" se muestra un ejemplo que combina un enrutado IP
bloque y NAT. Enrutamiento IP pública se trata en Sección 8.2, "Enrutamiento IP Pública", Y NAT
en Capítulo 7, Network Address Translation.
Si está utilizando CARP, la subred WAN tendrá que ser un / 29, de manera que cada servidor de seguridad tiene su propio IP de la WAN, y usted tiene una dirección IP CARP donde el proveedor más grande dentro de la ruta del bloque. La
dentro de la subred IP debe ser enviado a una dirección IP que está siempre disponible, independientemente de que servidor de seguridad
se ha terminado, y el más pequeño de subred se puede usar con la carpa es un 29 /. Esta configuración con la carpa es el mismo
como se ilustra arriba, con la puerta de entrada OPT1 ser una IP CARP, y el proveedor de enrutamiento a un
CARP IP en vez de la IP WAN. CARP se trata en Capítulo 20, Firewall de redundancia y Alto Disponibilidad.

6.7.1.2.3. Múltiples subredes IP

En otros casos, puede tener varias subredes IP de su ISP. Por lo general se inicia con uno de
las dos modalidades anteriormente descritas, y más tarde, cuando se solicite IPs adicionales que se
siempre con un adicional de subred IP. Esta subred adicional debe ser enviado a usted por su
ISP, ya sea para su WAN IP en el caso de un único servidor de seguridad, o para una dirección IP cuando se utiliza CARP CARP.
Si su proveedor se niega a la ruta de la subred IP para usted, sino más bien las rutas a su router y los usos
una de las direcciones IP de la subred como puerta de enlace IP, usted tendrá que usar proxy ARP para la VIP
subred adicional. Si es posible, su proveedor, la ruta si la subred IP para usted, ya que hace
es más fácil trabajar con independencia de su servidor de seguridad de la elección.
En caso de la subred IP se dirige a usted, el escenario descrito en Sección 6.7.1.2.2, "WAN pequeñas Subred IP con mayor LAN subred IP " se aplica, sólo para una subred dentro adicionales. Usted puede asignar
a una interfaz nueva OPT, usarlo con NAT, o una combinación de los dos.

6.8. Virtual IP

pfSense permite el uso de múltiples direcciones IP públicas en relación con el NAT a través de Virtual
IP (VIP).

Hay tres tipos de direcciones IP virtuales disponibles en pfSense: Proxy ARP, la carpa, y otros. Cada uno es útil en situaciones diferentes. En la mayoría de circunstancias, pfSense tendrá que proporcionar ARP en su

VIP por lo que debe usar proxy ARP o CARP. En situaciones en las ARP no es necesario, como cuando más direcciones IP públicas son dirigidas por el proveedor de la WAN IP, utilice otras personalidades tipo.

6.8.1. Proxy ARP

Proxy ARP funciones estrictamente en la capa 2, ofrecer respuestas ARP para la dirección IP CIDR o rango de direcciones IP. Esto permite que pfSense para reenviar el tráfico destinado a esa dirección de acuerdo a la configuración de NAT. La dirección o rango de direcciones no están asignados a ninguna interfaz en pfSense, porque no tienen que ser. Esto significa que no hay servicios en pfSense se puede responder a estas direcciones IP. Esto generalmente se considera un beneficio, ya que su IP pública adicional sólo debe ser usado para los propósitos NAT.

6.8.2. CARP

CARPA VIP se utilizan sobre todo con las implementaciones redundantes utilizando CARP. Para obtener información sobre utilizando CARPA VIP, consulte Capítulo 20, Firewall de redundancia / alta disponibilidad sobre el hardware redundancia.

Algunas personas prefieren utilizar VIP CARP incluso cuando se emplea sólo un único servidor de seguridad. Esto es por lo general pfSense porque responde a los pings en la carpa VIP, si las reglas de su cortafuegos permite este tráfico (Las reglas por defecto no lo hace, para VIPs en WAN). Otra situación en la CARPA VIP se debe utilizar es para cualquier personalidades que será el anfitrión de un servidor FTP. El proxy FTP en pfSense debe ser capaz de unirse a el VIP para funcionar, y sólo CARPA VIP permite.

pfSense no responde a los pings destinados a Proxy ARP y otras personalidades, independientemente de su configuración de reglas de firewall. Con Proxy ARP y otras personalidades, debe configurar NAT para un host interno de ping para funcionar. Ver Capítulo 7, Network Address Translation para más de la información.

6.8.3. Otros

"Otros" VIP permiten definir direcciones IP adicionales para su uso cuando las respuestas ARP para la dirección IP no son necesarios. La única función de la adición de un Otro VIP está haciendo que la dirección disponible en las pantallas de configuración de NAT. Esto es útil cuando se tiene un bloque IP pública dirigida a su dirección IP WAN o un VIP CARP.

6.9. Tiempo base de reglas

normas basadas en el tiempo le permiten aplicar reglas de firewall sólo en los días especificados y / o márgenes de tiempo. normas basadas en el tiempo se implementan en 1.2.x con el ipfw filtro, porque las dificultades con el estado

mantenimiento en el momento esta funcionalidad fue escrito significaba esta era la única posibilidad de adecuada
desconectar sesiones activas cuando el calendario de vencimiento. Nueva funcionalidad en pfSense 2.0 permite que se trata de integrarse con el PF de filtro, permitiendo que el tiempo basado en normas para funcionar igual que cualquier otra
regla. Por el momento, hay algunas advertencias a usar el tiempo basado en normas, y la lógica de estos normas es un poco diferente. En esta sección se analizará cómo el uso del tiempo basado en normas, y las diferencias entre ellos y otras normas de firewall.

6.9.1. Tiempo Reglas lógica basada

Cuando se trate de normas basadas en el tiempo, el programa determina el momento de aplicar la acción especificada en la regla de firewall. Cuando la hora actual o la fecha no está cubierto por el programa, la acción de
la regla se invierte. Por ejemplo, una regla que pasa el tráfico de los sábados lo bloqueará todos los demás día, independientemente de las reglas definidas más adelante en el firewall. Las reglas son transformados a base de la parte superior-
abajo, lo mismo que las reglas del cortafuegos otros. El primer partido se utiliza, y una vez se encontró coincidencia, que que se tomen medidas y no otras reglas son evaluados. Si está trabajando con una regla de transmitir una cierta calendario, por ejemplo sábado y domingo, y que no tiene el efecto deseado, entonces podría
en lugar de tratar una regla de bloqueo de lunes a viernes.
Es importante recordar siempre que el uso horario que la norma tendrá un efecto
si está dentro de la hora programada o no. La norma no sólo se omiten debido a que el momento actual no se encuentra dentro de la hora programada. Tenga esto en cuenta para asegurarse de que no accidentalmente permitir un acceso más de lo previsto con una regla programada. Tome este otro ejemplo:
Si usted tiene una política restrictiva de la salida para el tráfico HTTP, y desea programar el tráfico HTTP reglas, entonces usted tendrá que programar las normas restrictivas, y no sólo tiene un bloque programado regla para el tráfico HTTP. En este caso el bloque programado regla general, cuando fuera de la hora programada, se convertirá en una regla general pasan HTTP y HTTP ignorar las normas más restrictivas de la salida.

6.9.2. Tiempo Advertencias basada en reglas

Porque el tiempo de las reglas basadas en el uso ipfw en lugar de fondos de pensiones, que son incompatibles con el portal

cautivo. Por
la misma razón, multi-WAN y algunas de las otras capacidades avanzadas de firewall regla también se disponible con el tiempo basado en normas.

6.9.3. Configuración de los horarios de tiempo basada en reglas

Los horarios se definen en firewall → Horarios y calendario de cada uno puede contener múltiples tiempo rangos. Una vez que un programa se define, entonces se puede utilizar para una regla de firewall. En el siguiente ejemplo, una empresa quiere negar el acceso a HTTP durante el horario laboral, y permita que todos los demás veces.

6.9.3.1. Definición de los tiempos de la Lista

Para agregar un programa de servidor de seguridad → Listas, haga clic en. Esto debería abrir el calendario pantalla de edición, como se ve en la Figura 6.23, "Adición de un rango de tiempo". El primer campo en esta pantalla
es para el nombre de Lista. Este valor es el nombre que aparecerá en la lista de selección para su uso en las reglas del cortafuegos. Al igual que los nombres de alias, este nombre sólo puede contener letras y dígitos, y no espacios. Para este ejemplo, vamos a poner en **BusinessHours**. Siguiente en el cuadro Descripción, escriba una ya de forma libre descripción de este horario, como **Horario Normal**. Desde un programación se compone de una o más definiciones de intervalo de tiempo, lo próximo debe definir un rango de tiempo antes de poder guardar la programación.
Un programa se puede aplicar a días específicos, tales como 02 de septiembre 2009, o los días de la semana, como de lunes a miércoles. Para seleccionar un día cualquiera en el próximo año, elegir el mes de la lista desplegable, a continuación, haga clic en el día o días específicos en el calendario. Para seleccionar un día de la semana, haga clic en su nombre en los encabezados de columna. Para nuestro ejemplo, haga clic en L, M, X, J, y Vie. Esto hará que el programa activo para cualquier lunes a viernes, con independencia del mes. Ahora seleccionar el tiempo en que este programa debe ser activa, en formato de 24 horas. Nuestro horario de atención será **09:00** a **17:00** (17:00). Todas las horas se dan en la zona horaria local. Ahora entrar en un tiempo Descripción del área de distribución, como **Semana laboral**, A continuación, haga clic en Agregar Tiempo. Una vez que el intervalo de tiempo se ha definido, aparecerá en la lista en la parte inferior de la programación pantalla de edición, como en la Figura 6.24, "Alta Gama de tiempo".

Si hay más tiempo para definir, repita el proceso hasta que esté satisfecho con los resultados. Por ejemplo, para ampliar este programa de instalación, puede ser un medio día del sábado para definir, o tal vez el tienda abre a última hora del lunes. En ese caso, definir un rango de tiempo para los días idénticos, y luego otro rango para cada día con diferentes tiempos. Esta colección de rangos de tiempo será el pleno horario. Cuando todos los rangos de tiempo necesarios han sido definidos, haga clic en Guardar. A continuación, se volver a la lista de lo previsto, y el nuevo calendario aparecerá, como en Figura 6.25, "Calendario de la lista después de agregar ". Este programa estará disponible para su uso en las reglas del cortafuegos.

Figura 6.25. Lista la lista después de agregar

6.9.3.2. Uso de la Lista en una regla de firewall

Para crear una regla de firewall que utilizan este programa, debe agregar una regla en la interfaz deseada. Ver Sección 6.2.1, "Adición de una regla de firewall" y Sección 6.6, "Configuración de las reglas del cortafuegos" de

más información sobre cómo agregar y las normas de edición. Para nuestro ejemplo, agregar una regla para bloquear el TCP
tráfico en la interfaz LAN de la subred LAN, a cualquier destino en el puerto HTTP. Cuando
llegar a la Lista Marco elegir el horario que acabamos de definir, **BusinessHours**, Como en Figura 6.26, "Elección de una lista de reglas de firewall".

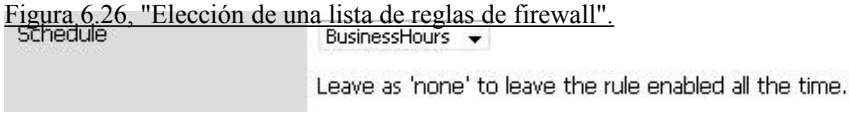


Figura 6.26. Elegir un horario para una regla de firewall

Después de guardar la regla, el programa aparecerá en la lista de reglas de firewall, junto con una indicación de estado activo de la programación. Como se puede ver en Figura 6.27, "Firewall lista de reglas con el cuadro", esta es una regla de bloqueo, pero la columna de horario es lo que indica que el Estado no está en sus activos estado de bloqueo, ya que se está viendo en un momento en que se encuentra fuera del rango programado. Si Pase el ratón sobre el nombre del programa, se mostrará el tiempo definido para ese horario. Si pasa más de el indicador de estado de programa, le dirá descriptivamente cómo el Estado se está comportando en ese punto en el tiempo. Como se trata de que se está viendo fuera de los tiempos definidos en nuestro programa BusinessHours, este va a decir "Tráfico coinciden con esta regla se está permitido". Si hubiéramos usado una regla de pase, lo contrario sería cierto.

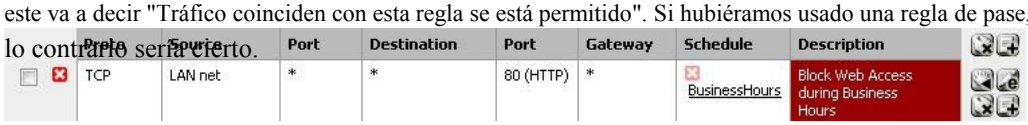


Figura 6.27. Firewall de lista de reglas con el cuadro

Ahora que el Estado se define, asegúrese de probar tanto dentro como fuera de las horas programadas para garantizar que el comportamiento deseado es promulgada. También hay que tener el tiempo de advertencias basadas en reglas (Sección 6.9.2, "Advertencias basada en el tiempo Reglamento") en cuenta el momento de elaborar estas normas.

6.10. Visualización de los registros del firewall

Para cada regla que se establece para iniciar la sesión, y por defecto la regla de denegación, una entrada de registro que se haga. Hay varios
formas de ver estas entradas de registro, con diferentes niveles de detalle, y no hay una clara "mejor" método.

Al igual que otros registros en pfSense, los registros del firewall sólo mantienen un cierto número de registros. Si las necesidades
de su organización requieren que usted mantenga un registro permanente de los registros del firewall para una mayor período de tiempo, ver Sección 22.1, "Sistema de Registros" para obtener información relativa a la copia estas entradas de registro
a un servidor syslog a medida que ocurren.

6.10.1. Viendo en la WebGUI

Los registros del firewall es visible desde el WebGUI, y puede ser encontrado en estado de → Registros del sistema,
en la pestaña Firewall. Usted puede ver o analizar los registros, que son más fáciles de leer, o los registros de la materia prima,
que tienen más detalles si usted entiende formato de registro PF. También hay un escenario de la
los registros del sistema que se muestran estas entradas en adelante o para atrás. Si no está seguro en el que
Para las entradas del registro se muestran, compruebe la fecha y hora de la primera y la última, o visite
Sección 22.1, "Sistema de Registros" para obtener información sobre cómo ver y cambiar esta configuración.

El WebGUI analiza los registros, se ve en Figura 6.28, "Ejemplo de entradas del registro se ve desde la WebGUI",
en 6 columnas: Acción, Tiempo, Interfaz, Origen, Destino, y el Protocolo. Acción muestra lo que
pasó con el paquete que genera la entrada de registro, ya sea pasar, bloquear o rechazar. El tiempo es el
momento en que llegó el paquete. La interfaz es en el paquete entró en pfSense. Fuente es la fuente
Dirección IP y el puerto. Destino es la dirección IP de destino y el puerto. El protocolo es el protocolo
del paquete, ya sea ICMP, TCP, UDP, etc.

Act	Time	If	Source	Destination	Proto
	Jul 16 20:54:05	WAN	0.0.0.0:68	255.255.255.255:67	UDP
	Jul 16 20:56:05	WAN	0.0.0.0:68	255.255.255.255:67	UDP
	Jul 16 21:05:05	WAN	0.0.0.0:68	255.255.255.255:67	UDP
	Jul 16 21:06:05	WAN	0.0.0.0:68	255.255.255.255:67	UDP

Figura 6.28. Ejemplo de entradas del registro se ve desde la WebGUI

El icono de acción es un vínculo que las operaciones de búsqueda y mostrar la regla que provocó la entrada del registro.

Más información

A menudo, esto simplemente dice "Denegar por defecto", pero cuando la solución de problemas regla que puede ayudar reducir el número de sospechosos.

Si el protocolo es TCP, también verá campos adicionales aquí que representan las banderas TCP en la
paquete. Éstos indican diversos estados de conexión o los atributos de paquetes. Algunos de los más comunes
cuáles son:

S - SYN	Sincronizar números de secuencia. Indica una nueva conexión intento cuando sólo SYN está fijado.
A - ACK	Indica aceptación de los datos. Como se señaló anteriormente, estas son las respuestas para que el remitente saber datos se han recibido en Aceptar.
F - FIN	Indica que no hay más datos del remitente, el cierre de una conexión.

R - RST	Restablecimiento de la conexión. Esta bandera se fija al responder a una solicitud de abrir una conexión en un puerto que no tiene ningún demonio de escucha. También se puede ajustar por el software de servidor de seguridad para la espalda no deseados conexiones.

Hay varios otros indicadores, y su significado se resume en muchos materiales de el protocolo TCP. Como es habitual, el Artículo Wikipedia sobre TCP [Http://en.wikipedia.org/wiki/Transmission_Control_Protocol # TCP_segment_structure] Tiene más información.

6.10.2. Viendo desde el menú Consola

Los troncos se pueden ver en tiempo real directamente desde la interfaz de registro PF mediante la opción **10** desde el menú de la consola. Un ejemplo sencillo es una entrada de registro como la que se ve arriba en Figura 6.28, "Ejemplo de entradas del registro se ve desde la WebGUI":

Esto demuestra que el artículo 54 se emparejó, que dio lugar a una acción de bloqueo en la `vr1` interfaz. Las direcciones IP de origen y de destino se muestran a continuación. Los paquetes de otros protocolos pueden mostrar de datos mucho más.

6.10.3. Para ver imágenes de la Shell

Cuando se utiliza la cáscara sea de SSH o desde la consola, hay numerosas opciones disponibles para ver el filtro de registros.

Cuando se mira directamente a los contenidos del archivo de obstruir, las entradas de registro pueden ser muy complejas y detallado. Debería ser relativamente fácil de seleccionar los distintos campos, pero dependiendo del contexto del partido, puede ser más difícil.

6.10.3.1. Viendo el contenido actual del archivo de registro

El registro de filtro, como se explica en la apertura de este capítulo, está contenido en un registro circular binario por lo que no puede utilizar las herramientas tradicionales como el gato, grep, etc en el archivo directamente. El registro debe ser leído de nuevo con el programa de obstruir, y entonces puede ser conducido a través de cualquier programa que desee.

Para ver el contenido actual del archivo de registro, ejecute el siguiente comando:

#obstruir / var / log / filter.log

Todo el contenido del archivo de registro se mostrará. Si usted está interesado sólo en los últimos años líneas, se pueden canalizar a través de la cola de este modo:

#obstruir / var / log / filter.log | tail

6.10.3.2. Tras la salida del registro en tiempo real

Para "seguir" a la salida del archivo de obstruir, debe utilizar el `-F` parámetro para tapar. Este es el equivalente de tail-f para aquellos acostumbrados a trabajar con los archivos de registro normal en los sistemas UNIX.

#obstruir-f / var / log / filter.log

Esta es la salida todo el contenido del archivo de registro, pero no dejar de fumar después. En su lugar, se espera para obtener más entradas e imprimirlos a medida que ocurren.

6.10.3.3. Viendo el registro de salida analizado en el depósito

No es un analizador de registro simple escrito en PHP que puede ser utilizado de la cáscara para producir reducida de salida en lugar del registro de primas por completo. Para ver el contenido analizado de la sesión actual, ejecute:

#obstruir / var / log / filter.log | php / usr / local / www / filterparser.php

Podrás ver el registro de las entradas de salida por línea, con salida simplificada de este modo:

```
17 de julio 00:06:05 bloque vr1 UDP 0.0.0.0:68 255.255.255.255:67
```

6.10.3.4. Encontrar la regla que provocó una entrada de registro

Al ver uno de los formatos de registro sin procesar, el número de la regla para una entrada en la pantalla. Usted puede
utilizar este número de la regla para encontrar la regla que causó el partido. En el siguiente ejemplo, estamos tratando de averiguar qué norma se numera *54*.

#pfctl-vvsr | grep ^ '@*54* '

```
@ 54 caída de bloques en el registro rápido todo el sello "regla de
denegación por defecto"
```

Como puede ver, esta fue la regla de denegación por defecto.

6.10.4. ¿Por qué a veces veo bloqueado las entradas del registro de conexiones legítimas?

A veces podrás ver las entradas de registro que, si bien etiquetados con el "Default negar" la regla, se parecen a pertenecen al tráfico legítimo. El ejemplo más común es ver una conexión bloqueada
participación de un servidor web.

Es probable que esto suceda cuando un paquete TCP FIN, que normalmente se cierra la conexión, llega después de que el estado de la conexión se ha quitado. Esto sucede porque en ocasiones un paquete

se perderán, y la retransmite serán bloqueados por el cortafuegos ha cerrado ya la conexión.

Es inofensivo, y no indica una conexión real bloqueado. Todos los firewalls ello, aunque algunos no generan mensajes de registro para este tráfico bloqueado incluso si se registra todos los bloqueados tráfico.

Usted verá esto en ocasiones incluso si ha permitir que todas las normas en todas sus interfaces, ya que todos los para las conexiones TCP sólo permite paquetes TCP SYN. El resto de tráfico TCP o será parte de un estado que existen en la tabla de estado, o se imitan los paquetes con las banderas TCP.

6.11. Solución de problemas de reglas de firewall

En esta sección se ofrece orientación sobre qué hacer si las reglas de firewall no se comportan como deseo o esperar.

6.11.1. Revise sus registros

El primer paso para solucionar problemas de tráfico sospechoso debe ser bloqueado para revisar sus cortafuegos los registros (de estado → Registros del sistema, en la pestaña Firewall). Recuerde que pfSense por defecto de registro todo el tráfico se redujo y no se registra ningún tráfico que pasa. A menos que se añada el bloque o rechazar las reglas que no utilice el registro, todo el tráfico bloqueado siempre podrá ingresar. Si no ve el tráfico con un X roja junto a él en su registros de cortafuegos, pfSense no va a abandonar el tráfico.

6.11.2. Revisión de parámetros de la regla

Modificar la norma en cuestión y la revisión de los parámetros que haya especificado para cada campo. Para TCP y el tráfico UDP, recuerda el puerto de origen casi nunca es el mismo que el puerto de destino, y por lo general se debe establecer en cualquier. Si la regla de denegación por defecto es el culpable, puede ser necesario para elaborar una nueva pasar regla que coincide con el tráfico que debe ser permitido.

6.11.3. Revisión del estado de pedido

Recuerde que la primera regla que coincida gana - sin otras normas que se evalúan.

6.11.4. Normas e interfaces

Asegúrese de que sus normas se encuentran en la interfaz correcta para funcionar según lo previsto. Recuerde que el tráfico se filtra sólo por el conjunto de reglas configuradas en la interfaz donde se inicia el tráfico. El tráfico proveniente de

un sistema de la LAN con destino a un sistema en cualquier otra interfaz se filtra sólo por la LAN reglas. Lo mismo es cierto para todas las otras interfaces.

6.11.5. Activar la regla de registro

Puede ser útil para determinar qué regla se pongan en venta el tráfico en cuestión. Al habilitar el registro en las reglas de su pase, puede ver los registros del firewall y haga clic en una entrada individual para determinar que aprobó la norma de tráfico.

6.11.6. Solución de problemas con la captura de paquetes

captura de paquetes puede ser muy valiosa para la solución de problemas y la depuración de los problemas de tráfico.

Usted puede decir
si el tráfico está llegando a la interfaz externa en absoluto, o salir de la interfaz en el interior, entre otras muchas otros usos. Ver Capítulo 25, Captura de paquetes para más detalles sobre la solución de problemas con el paquete
captura y tcpdump.

Capítulo 7. Network Address Translation

En su uso más común, Network Address Translation (NAT) le permite conectar múltiples ordenadores a Internet mediante una única dirección IP pública. pfSense permite que estos simples implementaciones, pero también tiene capacidad para mucho más avanzadas y complejas configuraciones de NAT necesaria en redes con múltiples direcciones IP públicas.

NAT se configura en dos direcciones - entrada y de salida. Salida NAT define cómo el tráfico que sale de la red destinado a Internet se traduce. Entrada NAT se refiere al tráfico ingresen a su red desde Internet. El tipo más común de NAT entrante y uno de los la mayoría está familiarizado con el puerto es hacia delante.

7.1. Configuración por defecto NAT

En esta sección se describe la configuración de NAT por defecto de pfSense. El más adecuado configuración de NAT se genera automáticamente. En algunos ambientes se desea modificar esta configuración, y pfSense plenamente le permite hacerlo - todo desde la interfaz web. Esto es un contraste de muchas otras distribuciones de código abierto cortafuegos, que no permiten la capacidades, son necesarios en todos los mas pequeños, simples redes.

7.1.1. Configuración por defecto NAT Saliente

La configuración de NAT por defecto en pfSense con una interfaz LAN y el despliegue de dos WAN traduce automáticamente el tráfico de Internet enlazado a la dirección IP de la WAN. Cuando múltiples WAN interfaces se configuran, el tráfico de dejar cualquier interfaz WAN se traduce automáticamente a la dirección de la interfaz WAN que se utiliza.

puerto estático se configura automáticamente para IKE (parte de IPsec) y SIP (VoIP) de tráfico. Estáticas de puertos se aborda con más detalle en Sección 7.6, "NAT Saliente" sobre la salida NAT.

7.1.2. Configuración por defecto NAT entrantes

De forma predeterminada, no está permitido en el de Internet. Si tiene que permitir el tráfico iniciado en la Internet a un host en la red interna, debe configurar el puerto hacia delante o NAT 1:1. Este se trata en las secciones próximas.

7.2. Puerto Delanteros

delante del puerto le permiten abrir un puerto específico, rango de puerto o protocolo de una empresa privada dirigida
dispositivo en su red interna. El nombre de "puerto hacia adelante" fue elegido porque es lo que más
la gente entiende, y pasó a llamarse de la técnicamente más adecuado "NAT entrantes"
después de innumerables quejas de los usuarios confundidos. Sin embargo, es un poco de un nombre poco apropiado, como se puede
reorientar el GRE y protocolos de pesetas, además de los puertos TCP y UDP. Esto es más común
utiliza cuando servidores de alojamiento, o el uso de aplicaciones que requieren conexiones de entrada de la
De Internet.

7.2.1. Los riesgos de redireccionamiento de puertos

En una configuración por defecto, pfSense no permite en ningún tráfico iniciado en Internet. Este
proporciona la protección de cualquier persona de exploración de Internet en busca de los sistemas de ataque. Cuando se agregar un puerto para la conexión, pfSense permitirá ningún tráfico que coincide con la regla de firewall correspondiente. Es
no sabe la diferencia de un paquete con una carga maliciosa y que es benigno. Si
coincide con la regla de firewall, es permitido. Tienes que confiar en los controles basado en host para asegurar que ninguna
los servicios permitidos a través del firewall.

7.2.2. El reenvío de puertos y servicios locales

Puerto delanteros tienen prioridad sobre los servicios que se ejecutan localmente en el servidor de seguridad, tales como la web
interfaz, SSH, y cualquier otros servicios que se estén ejecutando. Por ejemplo, esto significa que si usted permite que Web remoto acceder a la interfaz de la WAN mediante HTTPS en el puerto TCP 443, si se añade un puerto
avanzar en la WAN para que el puerto TCP 443 hacia adelante va a funcionar y el acceso de la interfaz web de WAN ya no funciona. Esto no afecta el acceso a otras interfaces, sólo la interfaz
que contiene el puerto para la conexión.

7.2.3. Agregar Delanteros Puerto

Delanteros Puerto se gestionan a cortafuegos → NAT, en la ficha Avance del puerto. Las reglas en esta pantalla
se gestionan de la misma manera que las reglas del cortafuegos (véase Sección 6.2, "Introducción al servidor de seguridad pantalla Reglamento ").

Para empezar a agregar tus puerto para la conexión, haga clic en el botón en la parte superior o inferior de la lista, según lo indicado por Figura 7.1, "Agregar Puerto Adelante".

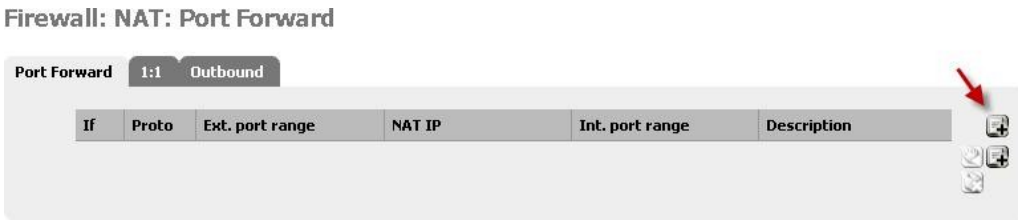


Figura 7.1. Añadir Adelante Puerto

Ahora va a estar mirando a la pantalla de edición de Puerto Adelante, se muestra en la Figura 7.2, "Puerto Adelante Ejemplo ", con las opciones por defecto elegido. En primer lugar, seleccionar la interfaz en la que el puerto que se va transmitió reside. En la mayoría de los casos esto se WAN, pero si usted tiene un vínculo WAN OPT, o si este Será un local de redirección, puede ser otra interfaz.

La dirección externa en la mayoría de los casos se debe establecer en **Dirección de interfaz** o una disposición IP virtual (véase Sección 6.8, "IPs virtuales"), a menos que se trata de un local de redirección.

El Protocolo y el rango de puerto externo se debe establecer en consecuencia para el servicio que se transmitió. Por ejemplo, que transmita VNC[1] se establecería Protocolo **TCP** y el rango de puertos externos para **5900**. (Como se trata de un puerto comúnmente transmitido, que también está disponible en la lista desplegable para selección de puerto.)

La IP NAT debe ser la dirección IP local a la que este puerto exteriores situados por delante la voluntad y el local puerto es donde el rango de puertos remitido comenzará. Si va a reenviar un rango de puertos, por ejemplo 19000-19100, sólo tiene que especificar un punto de partida local ya que los puertos deben coincidir una a uno. Este campo le permite abrir un puerto diferente en el exterior de la sede en el interior está escuchando, por ejemplo el puerto externo 8888 podrá remitir al puerto local 80 para HTTP en un servidor interno.

El campo de descripción, como en otras partes de pfSense, está disponible para una breve frase acerca de lo que el puerto se invoque o por qué existe.

Si no está utilizando un clúster de conmutación por error CARP, saltar sobre el n XML-RPC opción de sincronización. Si son, a continuación, marcar esta casilla, evitará que esta regla de ser sincronizado con los demás miembros de un clúster de conmutación por error (ver Capítulo 20, Firewall de redundancia / alta disponibilidad), Que suele ser indeseables.

La última opción es muy importante. Si marca Auto-añadir una regla de firewall para permitir el tráfico a través de esta regla NAT, entonces una regla de firewall se creará automáticamente para usted que le permita el tráfico

[1] Virtual Network Computing, una computadora de escritorio multiplataforma protocolo de uso compartido con muchos libres / implementaciones de código abierto, como UltraVNC (http://www.uvnc.com/)

para llegar al puerto de destino. Normalmente es mejor dejar esta marcada, y modificar entonces la regla de firewall
después, si es necesario. Haga clic en Guardar cuando haya terminado, a continuación, en Aplicar cambios.

En Figura 7.2, "Ejemplo de Avance del puerto" hay un ejemplo de la pantalla hacia adelante edición de puerto completado con la configuración adecuada que transmita la VNC para un sistema local.

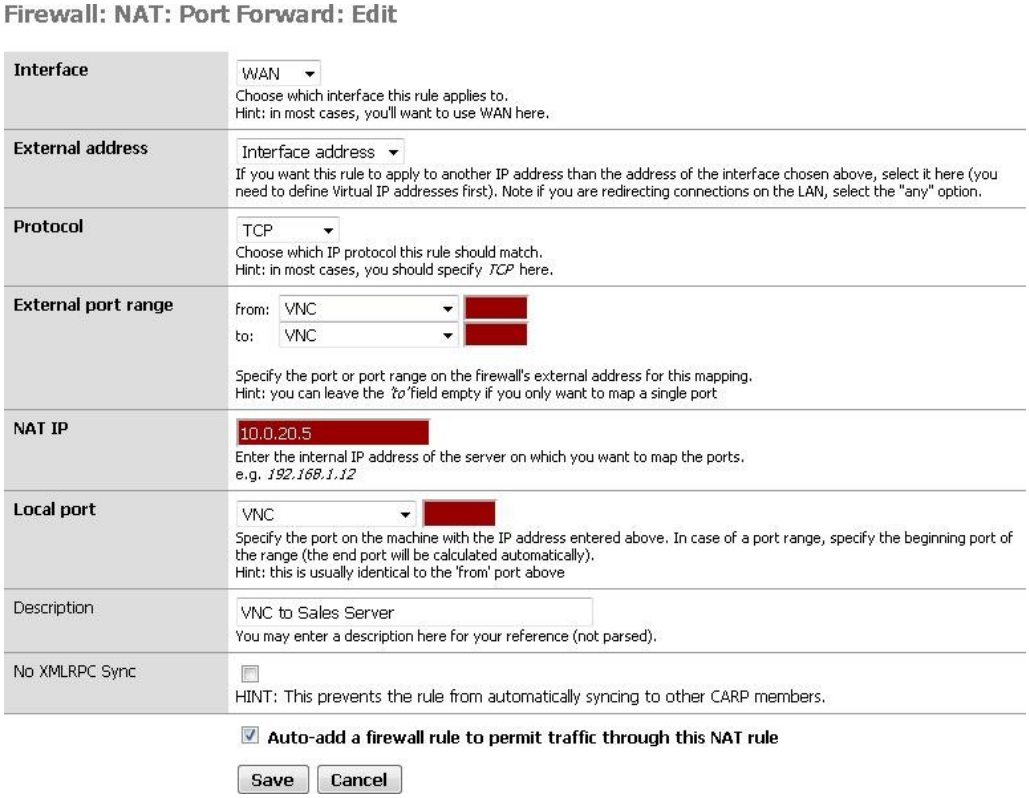


Figura 7.2. Puerto Ejemplo Adelante

Después de hacer clic en Guardar, se le llevará de nuevo a la lista de reenviar el puerto, y verás la nueva entrada creados como en Figura 7.3, "Listado de puertos".

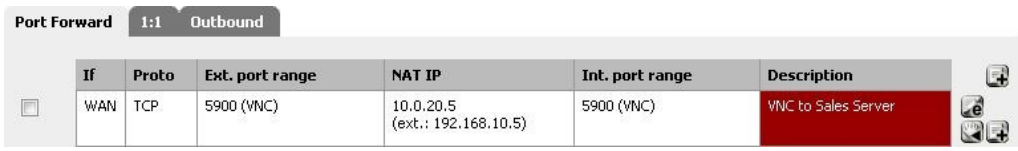


Figura 7.3. Listado de Puerto

Si lo desea, para corroborar la regla de firewall, como se ve en firewall → Reglas en la ficha de la interfaz en la que el puerto hacia adelante se ha creado. Se mostrará que el tráfico se permitirá en el período de investigación NAT en el puerto adecuado, como se muestra en Figura 7.4, "Adelante Puerto reglas de firewall".

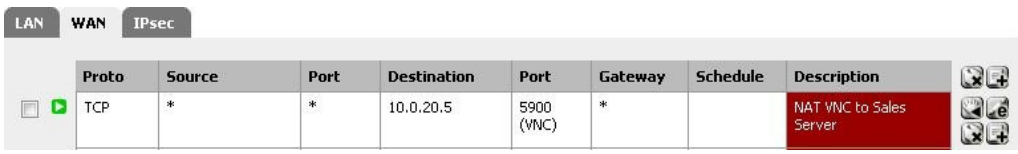


Figura 7.4. Adelante Puerto de reglas de cortafuegos

Usted tendrá que restringir el **Fuente** de la norma genera automáticamente cuando sea posible. Por cosas tales como servidores de correo que deben ser ampliamente accesibles, esto no es práctico, pero para el VNC ejemplo, es probable que sólo hay un pequeño número de máquinas que deben ser capaces de conectarse a través de VNC en un servidor de a través de Internet. Creación de un alias de hosts autorizados, y el cambio la fuente de la **cualquier** al alias es mucho más seguro que salir de la fuente abierta a toda la De Internet. Es posible que desee probar primero con la fuente sin restricciones, y tras comprobar que funciona como deseada, restringir la fuente si lo desea.

Si todo está correcto, el puerto para la conexión debería funcionar en las pruebas fuera de su red. Si algo salió mal, consulte Sección 7.9.1, "Puerto Adelante Solución de problemas" más adelante en este capítulo.

7.2.4. Limitaciones del puerto hacia adelante

Sólo se puede presentar un solo puerto a un host interno para cada dirección IP pública que ha disponible. Por ejemplo, si sólo tiene una dirección IP pública, sólo puede tener una servidor web interno que utiliza el puerto TCP 80 para el tráfico web. Cualquier servidor adicional necesario utilizar puertos alternativos, tales como 8080. Si usted tiene cinco direcciones IP públicas disponibles configurado como Virtual IP, usted podría tener cinco servidores web internos a través del puerto 80. Ver Sección 6.8, "Virtual IPs " para más información sobre las direcciones IP virtuales.

Para que remite el puerto WAN en las direcciones que sean accesibles por medio de su respectiva IP WAN dirección de la residencia de cara interfaces, tendrá que configurar NAT reflexión que se describe en Sección 7.5, "Reflexión NAT". Usted siempre debe probar su puerto hacia adelante de un sistema de otra conexión a Internet, y no desde el interior de la red.

7.2.5. Servicio de Auto-configuración con UPnP

Algunos programas ahora son compatibles con Universal Plug-and-Play (UPnP) para configurar automáticamente NAT delante del puerto y las reglas del cortafuegos. Aún más los problemas de seguridad se aplique en ellos, pero en la casa de utilizar el
beneficios superan a menudo las preocupaciones potenciales. Ver Sección 21.6, "UPnP" para más información sobre la configuración y el uso de UPnP.

7.2.6. El desvío del tráfico con Delanteros Puerto

Otro uso de los forwards puerto es para redireccionar de forma transparente el tráfico de su red interna. Adelante Puerto especificar la interfaz LAN u otra interfaz interna se redirigirá el tráfico
coincida con el avance hacia el destino especificado. Este es el más comúnmente usado para transparencia proxy el tráfico HTTP a un servidor proxy o redirigir todos los salientes de SMTP a un servidor.

Nota

El sistema que está dirigiendo el tráfico a esta debe residir en una interfaz diferente de el servidor de seguridad. De lo contrario su propio tráfico de red se redirige a sí mismo. En el caso de un servidor proxy HTTP con un puerto para la conexión de redirección de la LAN, por su propio solicitudes nunca será capaz de salir de la red a menos que el servidor reside en una interfaz de territorio palestino ocupado. No hay manera de negar un puerto para la conexión en una interfaz interna en
1.2.x pfSense, aunque hay una solicitud abierta en función de eso y se puede incluir en 2.0.

La entrada NAT se muestra en la Figura 7.5, "Ejemplo de redirección del puerto hacia adelante" es un ejemplo de un configuración que va a redirigir todo el tráfico HTTP que llegan a la interfaz LAN de Calamar (puerto 3129) en el host 172.30.50.10.

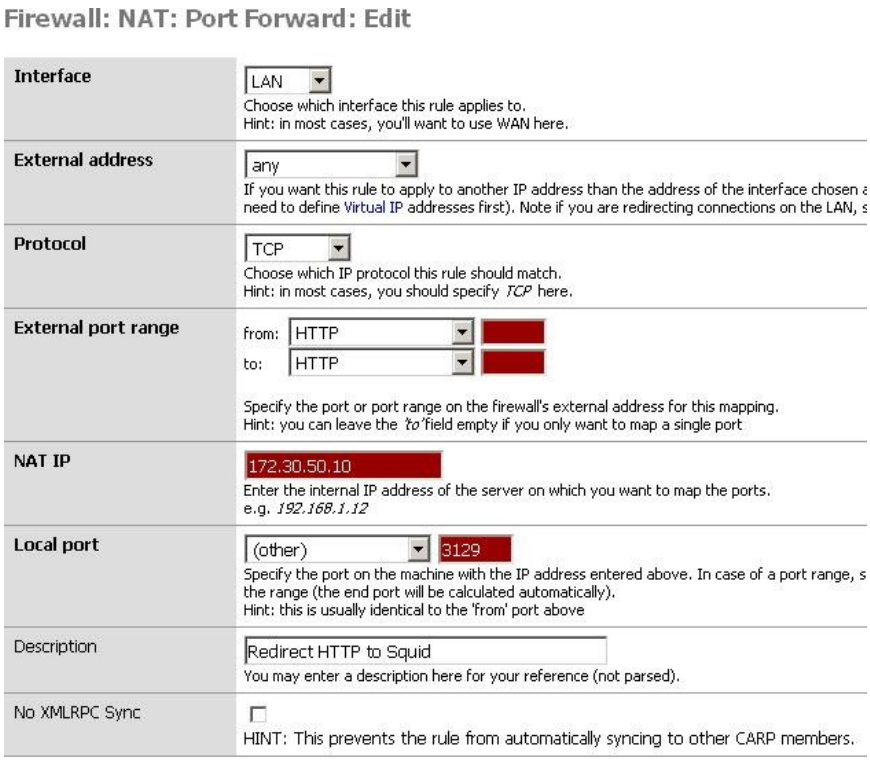


Figura 7.5. Ejemplo redirigir puerto para la conexión

Recuerde que el servidor está redirigiendo a debe residir en una interfaz diferente que el utilizado en el puerto para la conexión, como se describió anteriormente.

7.3. 01:01 NAT

01:01 (se pronuncia uno a uno) los mapas de NAT una IP pública a una IP privada. Todo el tráfico de esa IP privada a Internet será asignado a la dirección IP pública se define en la asignación de NAT 1:1, reemplazar la configuración de NAT de salida. Todo el tráfico iniciado en Internet destinado a especifica la dirección IP pública se traducirá a la IP privada, y luego evaluados por el firewall WAN conjunto de reglas. Si el tráfico es permitido por las reglas de su firewall, será pasado al host interno.

7.3.1. Los riesgos de NAT 01:01

Los riesgos de 1:1 NAT son en gran medida el mismo que transmite el puerto, si se permite el tráfico a que alojan en su WAN reglas de firewall. Cada vez que permitir el tráfico, que se permita el tráfico potencialmente dañinos en su red. Hay un riesgo añadido ligero utilizando las 01:01 NAT en que los errores reglas del firewall puede tener consecuencias más graves. Con las entradas del puerto hacia adelante, que están limitando el tráfico que se se permite dentro de la regla de NAT, así como la regla de firewall. Si el puerto hacia adelante el puerto TCP 80, a continuación, agregue una regla de permitir que todos en la WAN, sólo TCP 80 en que host interno será accesible. Si está utilizando NAT 1:1 y añade que todos los pronunciarse sobre WAN, todo lo que en ese host interno será accesible desde Internet. Errores de configuración son siempre un peligro potencial, y esto por lo general no debe considerarse como una razón para evitar 1:01 NAT. Hemos de tener en cuenta este hecho cuando configurar las reglas de firewall, y como siempre, que permita evitar cualquier cosa que no es necesario.

7.3.2. Configuración de NAT 01:01

Para configurar NAT 01:01, primero agregar una dirección IP virtual para el período de investigación pública que se utiliza para la entrada NAT 01:01 como se describe en Sección 6.8, "IPs virtuales". A continuación vaya al servidor de seguridad → NAT y haga clic en el 1:01 ficha. Haga clic para añadir una entrada de 1:1.

7.3.2.1. 01:01 Los campos de entrada NAT

Firewall: NAT: 1:1: Edit

Figura 7.6, "1:01 NAT pantalla Editar" muestra la pantalla de edición de NAT 01:01, a continuación, cada campo se detallarán.

Interface	WAN Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.
External subnet	/ 32 Enter the external (WAN) subnet for the 1:1 mapping. You may map single IP addresses by specifying a /32 subnet.
Internal subnet	Enter the internal (LAN) subnet for the 1:1 mapping. The subnet size specified for the external subnet also applies to the internal subnet (they have to be the same).
Description	You may enter a description here for your reference (not parsed).

Figura 7.6. 01:01 NAT pantalla Editar

7.3.2.1.1. Interfaz

La caja de interfaz le permite seleccionar la ubicación de la subred externa. Esto es casi siempre la WAN, o una interfaz WAN OPT en implementaciones multi-WAN.

7.3.2.1.2. Exteriores de subred

La subred externa es donde se define la dirección IP pública o rango de direcciones IP para las 01:01 cartografía. Esto puede ser una única dirección IP mediante la especificación de un / 32 máscara, o un rango CIDR mediante la selección de
otra máscara.

7.3.2.1.3. Interior de subred

La subred interna es donde se especifica la dirección IP interna o rango de direcciones IP para la 1:01 cartografía. Esta dirección IP o el intervalo debe ser alcanzable en una de sus interfaces internas, ya sea en una subred conectados directamente, o accesible a través de una ruta estática.

7.3.2.1.4. Descripción

Este es un campo opcional que no afecta el comportamiento de la entrada NAT 1:1. Rellene algo que le permitirá identificar fácilmente a esta entrada cuando se trabaja con el servidor de seguridad en el futuro.

7.3.2.2. Ejemplo de configuración de IP única 01:01

En esta sección se mostrará cómo configurar una entrada NAT 1:1 con un solo interno y externo IP. En este ejemplo, 10.0.0.5 es una dirección IP virtual en la WAN. En la mayoría de las implementaciones de este se sustituido con uno de sus direcciones IP públicas. El servidor de correo está configurado para este los mapas se encuentra en un segmento de la DMZ con IP interna 192.168.2.5. 01:01 La entrada NAT para mapear 10.0.0.5 a 192.168.2.5 se muestra en la Figura 7.7, "La entrada NAT 1:1". Un diagrama que representa este configuración en la Figura 7.8, "Ejemplo de NAT 01:01 - único en el interior y fuera de IP".

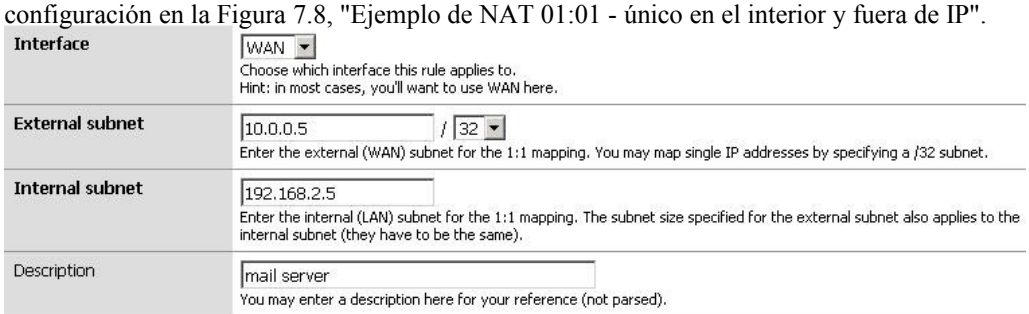


Figura 7.7. Entrada NAT 01:01

7.3.2.3. Ejemplo de configuración IP de gama 01:01

01:01 NAT se puede configurar para múltiples IPs públicas mediante el uso de rangos CIDR. CIDR resumen se trata en Sección 1.7.5, "de resumen CIDR". Esta sección cubre la configuración de 1:1 NAT para una amplia CIDR / 30 de los PI.

IP externa	Interior IP
10.0.0.64/30	192.168.2.64/30
10.0.0.64	192.168.2.64
10.0.0.65	192.168.2.65
10.0.0.66	192.168.2.66
10.0.0.67	192.168.2.67

Tabla 7.1. / 30 CIDR mapeo - octeto final se pongan en venta

El último octeto de las direcciones IP no tiene por qué ser el mismo en el interior y el exterior, pero recomendamos que hacerlo siempre que sea posible. Por ejemplo, Tabla 7.2, "/ 30 mapas CIDR - no se pongan en venta final octeto " también sería válida.

IP externa	Interior IP
10.0.0.64/30	192.168.2.200/30
10.0.0.64	192.168.2.200
10.0.0.65	192.168.2.201
10.0.0.66	192.168.2.202
10.0.0.67	192.168.2.203

Tabla 7.2. / 30 CIDR mapeo - octeto final no se pongan en venta

Recomiendo elegir un esquema de direccionamiento en el último octeto partidos, porque hace la red más fácil de entender y por lo tanto mantener. Figura 7.9, "la entrada de 01:01 NAT / 30 CIDR amplia "muestra cómo configurar NAT 01:01 para lograr la asignación enumerados en el Tabla 7.1, "/ 30 CIDR mapas - octeto final se pongan en venta ".

7.3.3. 01:01 NAT en la WAN IP, también conocido como "zona de distensión" en Linksys

Algunos routers de consumo como los de Linksys tienen lo que llaman una "zona de distensión", característica que se adelante todos los puertos y protocolos destinados a la dirección IP de la WAN a un sistema en la LAN. En

efecto, esto es de 1:1 NAT entre la dirección IP de la WAN y la dirección IP del sistema interno.
"Zona de distensión" en ese contexto, sin embargo, no tiene nada que ver con lo que una verdadera red DMZ es en tiempo real
la creación de redes de terminología. De hecho, es casi todo lo contrario. Un host en una verdadera zona de distensión se encuentra en una
aislado de la red lejos de los anfitriones otra LAN, aseguró fuera de la Internet y los host LAN
por igual. Por el contrario, una "zona desmilitarizada" de acogida en el sentido de Linksys no es sólo en la misma red que el
hosts de LAN, pero completamente expuestos al tráfico entrante con ninguna protección.

En pfSense, no se puede tener 01:01 NAT activo en la IP WAN. El WebGUI no permitir que dicho
configuración, ya que se rompería la conectividad para otras máquinas en la red. En su lugar, debe
sólo hacia delante de los protocolos y puertos necesarios para el servidor o aplicación, y restringir su
el uso de reglas de firewall que sea posible. Que técnicamente se puede lograr lo mismo mediante el envío de
Los puertos TCP y UDP del 1 al 65535 y el GRE y protocolos de pesetas, pero esto es muy fuerte
desalentados, ya que tiene consecuencias graves de seguridad.

7.4. Pedido de procesamiento de NAT y Firewall

Comprender el orden en que los cortafuegos y NAT se produce es importante en la configuración
NAT y las reglas del cortafuegos. La Figura 7.10, "Realización de pedidos de NAT y Firewall de procesamiento", ilustra
este ordenamiento. También muestra que los lazos de tcpdump, ya que su uso como herramienta de solución de problemas se
se describirá más adelante en este libro (véase Capítulo 25, Captura de paquetes).

Cada capa no siempre tiene éxito. Figura 7.11, "LAN a la WAN de procesamiento" y Figura 7.12, "WAN
a la LAN de procesamiento " muestran que las capas se aplican para el tráfico iniciado desde la LAN va a la
WAN, y también para el tráfico iniciado en la WAN va a LAN (por ejemplo cuando el tráfico está permitido).

Para el tráfico de LAN a WAN, en primer lugar las reglas del firewall que se evalúan, el NAT de salida
se aplica si el tráfico está permitido. El NAT WAN y las reglas del firewall no se aplican al tráfico
inició en la LAN.

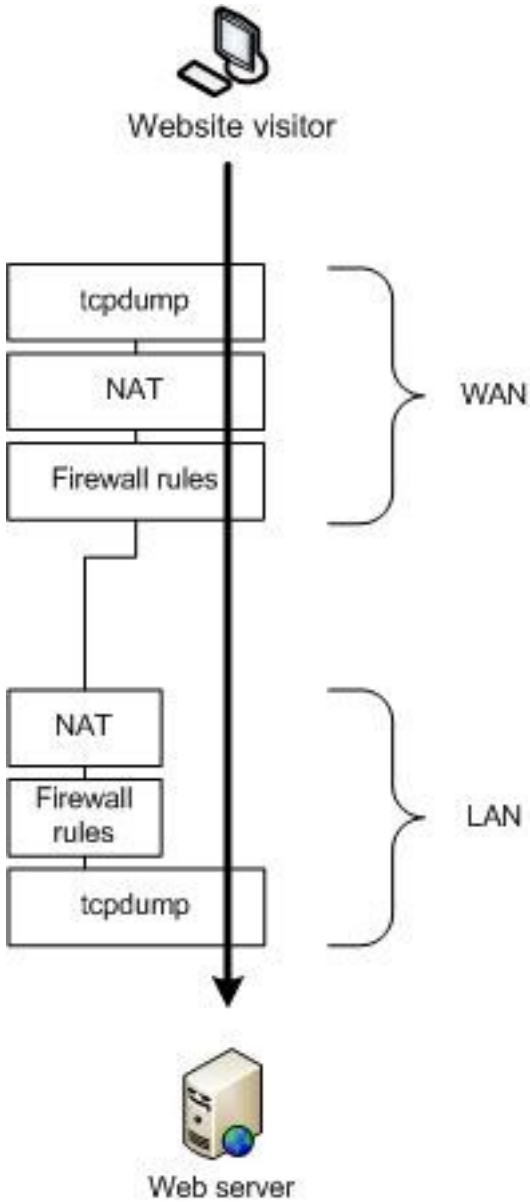


Figura 7.12. Procesamiento de WAN a LAN

Para el tráfico iniciado en la WAN, NAT se aplica en primer lugar, a continuación, las reglas del firewall.

Tenga en cuenta que tcpdump es siempre lo primero y el último en ver el tráfico - por primera vez en la

interfaz de entrada,
antes de cualquier procesamiento de firewall y NAT, y el último en la interfaz de salida. Esto demuestra lo que está en
el cable. (Véase Capítulo 25, Captura de paquetes)

7.4.1. Extrapolando a interfaces adicionales

Los diagramas anteriores sólo ilustran un básico de dos interfaz LAN y WAN de implementación. Cuando
trabajar con servidores de seguridad con OPT e interfaces WAN OPT, aplican las mismas reglas. Todos los territorios palestinos ocupados
interfaces se comportan de la misma LAN, y todas las interfaces WAN OPT se comportan de la misma como WAN.
El tráfico entre dos interfaces internas se comporta de la misma LAN a la WAN de tráfico, aunque la
reglas predeterminadas NAT no traducen el tráfico entre las interfaces internas por lo que la capa de NAT
no hacer nada en esos casos. Si define las reglas de NAT de salida que coincidan con el tráfico entre
interfaces internas, se aplicará tal como se muestra.

7.4.2. Reglas para NAT

Para conocer las reglas de la WAN o interfaces WAN OPT, porque NAT traduce la dirección IP de destino de la
tráfico antes de las reglas del firewall que evaluar, las reglas de firewall WAN siempre debe especificar el
dirección IP privada como destino. Por ejemplo, al agregar un puerto para la conexión para el puerto TCP 80
en la WAN, y comprobar la Auto-Añade una caja de servidor de seguridad general, esta es la regla de firewall que resulta en la WAN.

TCP	*	*	192.168.1.5	80 (HTTP)	*		NAT forward HTTP

El período de investigación interna en el puerto de avanzar es 192.168.1.5. Ya sea que utilice el puerto hacia delante o NAT 1:1,
reglas de firewall en todas las interfaces WAN debe utilizar la dirección IP interna como la dirección de destino. Consulte a Figura 7.13, "las reglas de firewall para el puerto hacia adelante a la LAN de host" para un ejemplo de cómo un regla debe aparecer.

Figura 7.13. Las reglas de firewall para el puerto hacia adelante a la LAN de host

7.5. NAT Reflexión

NAT reflexión se refiere a la capacidad de acceder a los servicios externos de la red interna
IP pública, lo mismo que usted haría si estuviera en Internet. Muchos de origen comercial y abierta
cortafuegos no admite esta funcionalidad en todos. pfSense tiene algo limitado el apoyo a NAT
reflexión, aunque algunos ambientes se requiere una infraestructura DNS dividida para dar cabida a
esta funcionalidad. Dividir el DNS está cubierta en Sección 7.5.2, "Split DNS".

7.5.1. Configuración y uso de Reflexión NAT

Para habilitar la reflexión NAT, vaya al Sistema → Página de avanzada. Desplácese hacia abajo en Traducción de direcciones de red y desactive la casilla de Deshabilitar NAT reflexión como se muestra en Figura 7.14, "Activar NAT Reflexión". Haga clic en Guardar y, a la reflexión NAT se activará. N una configuración adicional que se necesita, inmediatamente va a funcionar.

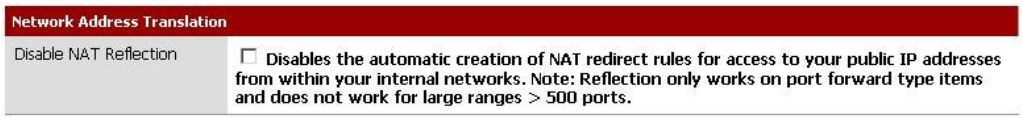


Figura 7.14. Habilitar NAT Reflexión

7.5.1.1. NAT Advertencias Reflexión

reflexión NAT es siempre un poco de un truco, ya que los bucles de tráfico a través del firewall. Debido a la pf opciones limitadas prevé la adaptación estos escenarios, hay algunas limitaciones en el aplicación pfSense reflexión NAT. Puerto rangos de más de 500 puertos no tienen NAT reflexión activa, y 1:1 NAT no es compatible. Dividir el DNS es el único medio de hacer frente grandes rangos de puertos y NAT 1:1. Me encantaría decirle a esta situación mejorará en pfSense 2.0, pero que es poco probable debido a los desafíos del manejo de este dados los límites de la subyacente software. El mantenimiento de una infraestructura DNS dividida es requerido por muchos de los firewalls comerciales, incluso,
y por lo general no es un problema.

7.5.2. Dividir el DNS

Una alternativa preferible a la reflexión NAT es implementar una infraestructura DNS dividida. Dividir el DNS hace referencia a una configuración de DNS, donde su público DNS de Internet resuelve a su IP pública, y DNS en la red interna se resuelve en la IP privada interna. Los medios para conseguir esto variará dependiendo de las características específicas de su infraestructura de DNS, pero es el resultado final de la mismo. Se omite la necesidad de reflexionar NAT mediante la resolución de nombres de host a la IP privada en el interior su red.

7.5.2.1. Invalida DNS Forwarder

Si utiliza pfSense como su servidor DNS para los hosts internos, puede utilizar anula DNS reenviador para llevar a cabo una implementación de DNS dividida. Para agregar un reemplazo para el agente de DNS, vaya a los servicios → Reenviador DNS y haga clic en la sección "Usted puede entrar en los registros que anulan

los resultados de los agentes de abajo ", como se indica en la Figura 7.15," Add DNS Forwarder Reemplazar ".

El resultado será el promotor de DNS: pantalla de edición de acogida. La Figura 7.16, "Add Forwarder DNS Aumento al presupuesto para example.com "y la Figura 7.17," DNS reenviador anulación de www.example.com " muestran ejemplos de anulaciones DNS para example.com y www.example.com.

Usted tendrá que añadir un aumento al presupuesto para cada nombre de host en el uso de detrás de su firewall.

7.5.2.2. Interior servidores DNS

Si utiliza otros servidores DNS en su red interna, como es común cuando se utiliza Microsoft Active Directory, usted tendrá que crear zonas para que todos los dominios de acogida dentro de su red, junto con todos los demás registros de los dominios (A, CNAME, MX, etc.)

En entornos que utilizan el servidor DNS de BIND DNS donde el público se encuentra alojado en el mismo servidor DNS como el privado, cuentan con puntos de vista de BIND se utiliza para resolver DNS diferente de la residencia
los ejércitos que las externas. Si está usando un servidor DNS diferente, es posible que un apoyo similar funcionalidad. Compruebe su documentación para obtener información.

7.6. Salida NAT

Salida NAT controla cómo el tráfico que sale de la red serán traducidos. Para configurarlo, visite el Firewall → Página de NAT y elegir la pestaña de salida. Hay dos de configuración opciones para la salida NAT en pfSense, generación automática de salida regla de NAT y el Manual generación de salida NAT (Advanced salida NAT (AON)). En las redes con un público único dirección IP por la WAN, por lo general hay ninguna razón para que AON. En entornos con múltiples direcciones IP públicas, puede ser deseable. Para entornos con CARP, es importante NAT el tráfico de salida a una dirección IP CARP, como se explica en Capítulo 20, Firewall de redundancia y Alto Disponibilidad.

7.6.1. Por defecto Reglas NAT Saliente

Al usar el NAT por defecto automático de salida, pfSense automáticamente crear reglas NAT el tráfico de traducir dejar la red interna a la dirección IP de la interfaz WAN que el tráfico de hojas.

7.6.2. Puerto estático

De forma predeterminada, pfSense vuelve a escribir el puerto de origen en todos los paquetes salientes.

Muchos sistemas operativos no
un mal trabajo de la aleatorización de puerto de origen, si lo hacen en absoluto. Esto hace más fácil la suplantación de IP, y permite a los hosts de huellas digitales detrás de su servidor de seguridad de su tráfico saliente. Reescritura el puerto de origen elimina estos posibles (aunque poco probable) vulnerabilidades de seguridad.

Sin embargo, esto rompe algunas aplicaciones. No se construyen en las reglas cuando avanzadas de salida NAT es con discapacidad que no lo hace para UDP 500 (IKE para el tráfico VPN) y 5060 (SIP), porque estos tipos de tráfico, casi siempre se rompe por reescribir el puerto de origen. El resto del tráfico se ha el puerto de origen reescrito de forma predeterminada.

Usted puede utilizar otros protocolos, como algunos juegos entre otras cosas, que no funcionan correctamente cuando el puerto de origen se reescribe. Para desactivar esta funcionalidad, deberá utilizar la estática opción de puerto. Haga clic en Firewall → NAT, y la ficha de salida. Haga clic en Manual de salida regla NAT
generación (Advanced salida NAT (AON)) y haga clic en Guardar. A continuación verá una regla en el parte inferior de la página etiquetada Auto creado regla para LAN. Haga clic en el botón a la derecha de la regla para editarlo. Marque la casilla de puerto estático en la página y haga clic en Guardar. Aplicar cambios. Después de hacer ese cambio, el puerto de origen en el tráfico de salida se mantendrá.

7.6.3. Deshabilitar NAT Saliente

Si está utilizando direcciones IP públicas en las interfaces locales, y por lo tanto no es necesario aplicar NAT el tráfico que pasa a través del firewall, debe desactivar NAT para esa interfaz. Con el fin de hacer esto, primero debe cambiar la configuración de NAT de salida en Manual de salida NAT, y luego Guardar. Después de hacer ese cambio, una o más reglas que aparecen en la lista en la pantalla de salida NAT. Eliminar la regla o reglas para el público en subredes IP haciendo clic en cada línea una vez (o marcar la casilla de el inicio de la línea) y, a continuación, haga clic en el botón en la parte inferior de la lista. Haga clic en Aplicar cambios para completar el proceso.

Una vez que todas las reglas se han eliminado, de salida NAT ya no se activa para los
direcciones y pfSense entonces las direcciones IP vía pública sin necesidad de traducción.

Para desactivar completamente NAT saliente, eliminar todas las reglas que están presentes cuando se utiliza manual NAT de salida.

7.7. Elegir una configuración de NAT

Su opción de configuración de NAT depende principalmente del número de IPs públicas que han y el número de sistemas que requieren el acceso de entrada desde Internet.

7.7.1. IP único público por la WAN

Cuando sólo tiene una única IP pública por la WAN, las opciones de NAT son limitados. Sólo se puede utilizar 01:01 NAT con Virtual IP, no con cualquier IP WAN. En este caso, sólo se puede usar hacia delante del puerto.

7.7.2. Múltiples direcciones IP públicas por WAN

Con múltiples direcciones IP públicas por la WAN, que tiene numerosas opciones para su entrada y de salida configuración de NAT. delante del puerto, NAT 1:1, y Avanzado de salida NAT todo puede ser deseable en algunas circunstancias.

7.8. NAT y compatibilidad de Protocolo

Algunos protocolos no funcionan bien y otras no en todos con NAT. Algunos protocolos de integrar IP Las direcciones dentro de los paquetes, algunos no funcionan correctamente si el puerto de origen se reescribe, y algunos son difíciles debido a las limitaciones de la FEP. Esta sección trata de los protocolos que tienen dificultades con NAT en pfSense, y cómo evitar estos problemas cuando sea posible.

7.8.1. FTP

FTP plantea problemas tanto con NAT y firewalls debido al diseño del protocolo. FTP fue diseñado inicialmente en la década de 1970, y el nivel actual de definición de las especificaciones de la protocolo fue escrita en 1985. Desde FTP se creó más de una década antes de la NAT, y largo antes de servidores de seguridad son comunes, que hace algunas cosas que son muy NAT y cortafuegos hostil. pfSense utiliza dos diferentes aplicaciones proxy FTP, pftpx y ftpsesame. pftpx se utiliza para todos escenarios de NAT, mientras acomoda ftpsesame puente y de enrutamiento de direcciones IP públicas.

7.8.1.1. FTP Limitaciones

Debido a pf carece de la capacidad para manejar adecuadamente el tráfico FTP sin un proxy, y el pfSense FTP aplicación proxy es algo falta, hay algunas restricciones en el uso de FTP.[2]

7.8.1.1.1. Conexiones de cliente FTP a Internet

conexiones FTP cliente siempre usará la interfaz WAN primario y no se puede utilizar cualquier OPT interfaces WAN. Más información sobre esto puede encontrarse en Capítulo 11, Múltiples WAN Conexiones

[2] En pfSense 2.0, el servidor proxy FTP y auxiliares relacionadas han sido eliminados y toda esta funcionalidad se maneja a la perfección en un más manera robusta en el interior del núcleo.

7.8.1.1.2. Servidores FTP detrás de NAT

servidores FTP detrás de NAT debe utilizar el puerto 21, ya que el proxy FTP sólo se iniciará cuando el puerto

21 es
especificado.

7.8.1.2. FTP modos

7.8.1.2.1. Modo Activo

Con FTP en modo activo, cuando una transferencia de archivos se solicita, el cliente escucha en un puerto local, y a continuación, indica al servidor la dirección IP del cliente y el puerto. El servidor se conectará de nuevo a que la propiedad intelectual
dirección y el puerto con el fin de transferir los datos. Este es un problema para los servidores de seguridad porque el puerto está
normalmente al azar, aunque los clientes modernos permiten limitar el alcance que se utiliza. Como es posible que han adivinado, en el caso de un cliente detrás de NAT, la dirección IP determinada sería una dirección local, inalcanzable desde el servidor. No sólo eso, sino una regla de firewall que hay que añadir y un puerto hacia adelante para permitir el tráfico en este puerto.
Cuando el proxy FTP está en uso, se trata de hacer tres cosas importantes. En primer lugar, se volverá a escribir el FTP PUERTO comandos para que la dirección IP es la dirección IP WAN del servidor de seguridad, y al azar un elegido el puerto en esa dirección IP. A continuación, se añade un puerto para la conexión que conecta la traducción de direcciones IP y el puerto a la dirección IP original y el puerto especificado por el cliente FTP. Por último, se permite el tráfico desde el servidor FTP para conectarse a ese "público" del puerto.

Cuando todo está funcionando como debería, todo esto sucede de manera transparente. El servidor nunca se sabe se está hablando con un cliente detrás de NAT, y el cliente no sabe que el servidor no se conecta directamente.

En el caso de un servidor detrás de NAT, esto no suele ser un problema ya que el servidor sólo se Música para las conexiones en el estándar de los puertos FTP y luego hacer las conexiones de salida de nuevo a los clientes.

7.8.1.2.2. Modo pasivo

Modo pasivo (PASV) actúa un poco a la inversa. Para los clientes, es más NAT y firewalls
ya que el servidor escucha en un puerto cuando una transferencia de archivos se solicita, no el cliente. Por lo general, el modo PASV trabajará para los clientes FTP detrás de NAT sin usar proxy o un tratamiento especial en absoluto.

Si un servidor está detrás de NAT, sin embargo, el tráfico debe ser proxy a la inversa, cuando a sus clientes intento de utilizar el modo PASV. El proxy FTP puede manejar esta situación, pero todas las llamadas entrantes FTP las solicitudes se parecen provenir del sistema de pfSense en lugar de los clientes. Al igual que el
situación en la sección anterior, cuando un cliente solicita el modo PASV el servidor tendrá que dar

su dirección IP y un puerto aleatorio para el cual el cliente puede intentar conectarse. Ya que el servidor es en una red privada, que la dirección IP y el puerto tendrá que ser traducido y permite a través de el servidor de seguridad.

7.8.1.2.3. Extendido modo pasivo

Extendido modo pasivo (EPSV) funciona de forma similar al modo PASV pero hace concesiones para el uso en IPv6. Cuando un cliente solicita una transferencia, el servidor responde con el puerto al que el cliente debe conectar. Las mismas advertencias para los servidores en modo PASV se aplican aquí.

7.8.1.3. Servidores FTP y reenvíos Puerto

Para garantizar el proxy FTP funciona correctamente para el puerto hacia delante

- IP pública debe ser IP de la interfaz WAN o de un tipo de carpas VIP, porque el proxy FTP debe para escuchar en la IP pública, y ARP Proxy y otras personalidades de tipo no permiten esto.
- ayudante de FTP debe estar habilitado en la interfaz WAN en el puerto hacia adelante reside.
- El servidor debe estar usando el puerto 21.

7.8.1.4. Servidores FTP y NAT 01:01

Al alojar un servidor FTP usando 01:01 NAT, debe hacer tres cosas para garantizar el proxy FTP funcionará, lo que permite FTP para que funcione correctamente.

- Utilice CARPA VIP tipo

  Debido a que el proxy FTP debe ser capaz de escuchar en el VIP, y Proxy ARP y otras personalidades de tipo no permitir esto, debe utilizar CARPA VIP con ninguna de las entradas 01:01 NAT alojamiento de servidores FTP.

- Habilitar el ayudante de FTP en la red WAN, donde la entrada se configura 01:01

  Vaya a la interfaz donde la subred externa 01:01 resida, en el menú de interfaces. En un solo despliegue de WAN, se trata de interfaces → WAN. Bajo FTP ayudante, asegúrese de desactivar la espacio de usuario de aplicación proxy FTP está marcada.

- Añadir una entrada al puerto para la conexión de TCP 21

  Esto no es precisamente sencillo, pero la forma de activar la ayuda de FTP para escuchar en una relación 1:1 NAT IP es mediante la adición de una entrada de puerto para la conexión con la misma IP internas y externas y el puerto TCP 21. Esto en realidad no agregar la configuración de NAT se especifica, como el sistema reconoce su

01:01 entrada NAT, y simplemente lanza el proxy FTP en que la propiedad intelectual. Esto puede ser más recta
adelante en pfSense 2.0, pero el comportamiento existentes se mantendrán para la compatibilidad hacia atrás.

7.8.2. TFTP

Norma tráfico TCP y UDP iniciar conexiones a hosts remotos usando un puerto de origen al azar en el rango de puertos efímeros (rango varía según el sistema operativo, pero entra dentro 1024-65535), y el puerto de destino del protocolo en uso. Las respuestas del servidor al cliente que revertir - la fuente puerto es el puerto del cliente de destino y el puerto de destino es el puerto del cliente de origen. Así es como asociados pf el tráfico de respuesta a las conexiones iniciadas desde el interior de la red.

TFTP (Trivial File Transfer Protocol) no se sigue de esto, sin embargo. El estándar que define TFTP, RFC 1350, especifica la respuesta del servidor TFTP al cliente se obtienen de un pseudo-número de puerto aleatorio. Su cliente TFTP puede elegir un puerto de origen de los 10.325 (como ejemplo) y utilizar el puerto de destino para TFTP, puerto 69. El servidor para otros protocolos entonces enviar el respuesta a través de puerto de origen 69 y puerto de destino 10325. Desde TFTP en su lugar utiliza un pseudo-aleatorios puerto de origen, el tráfico de respuesta no coincide con el pf Estado ha creado para este tráfico. De ahí que la respuestas serán bloqueados debido a que parecen ser el tráfico no solicitado a través de Internet.

TFTP no es un protocolo de uso general a través de Internet. La única situación que en ocasiones surge cuando se trata de un problema es con algunos teléfonos IP que se conectan al exterior de los proveedores de VoIP a través de Internet usando TFTP para tirar de configuración y otra información. La mayoría de los proveedores de VoIP no lo requieren.

No hay forma de solucionar esta limitación en este momento - TFTP no funcionará a través de pfSense 1.2. pfSense 2.0 incluye un proxy TFTP que elimina esta limitación.

7.8.3. PPTP / GRE

Las limitaciones con PPTP en pfSense son causados por las limitaciones en la capacidad de pf de NAT el GRE protocolo. Por lo tanto, las limitaciones se aplican a cualquier uso del protocolo GRE, sin embargo es el PPTP uso más común del GRE en la mayoría de las redes actuales.

El estado del código de seguimiento en pf para el protocolo GRE sólo puede seguir una sola sesión por IP pública por un servidor externo. Esto significa que si usted utiliza conexiones VPN PPTP, sólo una máquina interna se pueden conectar simultáneamente a un servidor PPTP en Internet. Un millar de máquinas se pueden conectar simultáneamente a un millar de diferentes servidores PPTP, pero a una sola vez una sola servidor. Un solo cliente también puede conectarse a un número ilimitado de servidores fuera de PPTP.

El único trabajo disponible todo es el uso de múltiples direcciones IP públicas en el servidor de seguridad, uno por cada cliente a través de
NAT de salida o 1:1, o utilizar múltiples direcciones IP pública externa en el servidor PPTP. Esto no es un problema con otros tipos de conexiones VPN.

Debido a las mismas limitaciones GRE se mencionó anteriormente, si activas el servidor PPTP en pfSense, no se puede conectar a cualquier servidor PPTP en Internet de los clientes NAT a la IP WAN pfSense. El trabajo alrededor de esto también requiere el uso de más de una dirección IP pública. Puede NAT clientes internos a otra IP pública, y sólo se sujeta a los mismos por públicos restricciones de propiedad intelectual antes mencionados.

Desde que en gran medida dependen de la funcionalidad del sistema subyacente, y simplemente envolver una interfaz gráfica de usuario en torno a esa funcionalidad, este es un problema difícil de resolver para nosotros. En el momento de escribir este artículo estamos investigando las posibles soluciones para este problema en pfSense 2.0, pero no tienen todavía un solución.

7.8.4. Juegos online

Juegos normalmente son NAT ambiente aparte de un par de advertencias. Esta sección se refiere a los juegos de PC con capacidades en línea, así como sistemas de consola de juegos con opciones online. En esta sección proporciona una visión general de las experiencias de numerosos usuarios pfSense. Recomiendo visitar el En el tablero de juego pfSense foro [http://forum.pfsense.org] para encontrar más información.

7.8.4.1. Puerto estático

Algunos juegos no funcionan correctamente a menos que se habilite el puerto estático. Si usted está teniendo problemas con un juego, lo mejor que probar primero es que permite puerto estático. Vea la sección de puerto estático al principio de este capítulo para obtener más información.

7.8.4.2. Múltiples jugadores o equipos detrás de un dispositivo NAT

Algunos juegos tienen problemas donde los jugadores múltiples o dispositivos están detrás de un dispositivo NAT sola. Estos problemas parecen ser específicos a NAT, no pfSense, ya que los usuarios que han probado otros servidores de seguridad experimentan los mismos problemas con ellos. Buscar en el tablero de juego en el foro de pfSense para el juego o el sistema que está utilizando y es probable que encontrar información de otros con experiencias similares en el pasado.

7.8.4.3. Superar los problemas con NAT UPnP

Muchos sistemas de juego modernos soportan Universal Plug-and-Play (UPnP) para que automáticamente configurar alguna necesidad especial en términos de los delanteros de puertos NAT y las reglas del cortafuegos. Usted puede encontrar que habilitar UPnP en su sistema pfSense le permitirá fácilmente juegos para trabajar con poca o ninguna intervención. Ver Sección 21.6, "UPnP" Para obtener más información sobre la configuración y el uso de UPnP.

7.9. Solución de problemas

NAT puede ser un animal complejo, y en todos menos en los ambientes más básica, es inevitable que haber algunos problemas de conseguir una buena configuración de trabajo. En esta sección se repasará algunos comunes problemas y algunas sugerencias sobre cómo podrían resolverse.

7.9.1. Puerto Adelante Solución de problemas

delante del puerto, en particular, puede ser difícil, ya que hay muchas cosas que van mal, muchos de los cuales podría estar en la configuración del cliente y no pfSense. La mayoría de los problemas encontrados por nuestros usuarios ha resuelto mediante una o varias de las siguientes sugerencias.

7.9.1.1. Puerta de entrada hacia delante incorrecta

Antes de cualquier tarea de solución de problemas, asegúrese que las configuraciones para el puerto hacia adelante son correctos.

Ir sobre el proceso de Sección 7.2.3, "Añadir Delanteros Puerto" otra vez, y vuelva a comprobar que el los valores son correctos. Recuerde, si usted cambia la IP NAT o los puertos, también se tendrá que ajustar la regla de firewall se pongan en venta. Las cosas comunes para verificar:

- Corregir la interfaz (por lo general WAN, o dondequiera que el tráfico va a ingresar en el cuadro de pfSense).
- Corregir NAT IP, que debe ser accesible desde una interfaz en el router pfSense.
- Corregir rango de puertos, que debe corresponder al servicio que están tratando de avanzar.

7.9.1.2. Falta o regla de firewall incorrecta

Después de comprobar la configuración de puerto para la conexión, verifique que la regla de firewall tiene la adecuada ajustes. Una regla de servidor de seguridad incorrecto también sería evidente al ver los registros del firewall (Sección 6.10, "Visualización de los registros del firewall"). Recuerde, que el destino del servidor de seguridad regla debe ser la dirección IP interna del sistema de destino y no la dirección de la interfaz que contiene el puerto para la conexión. Ver Sección 7.4.2, "Normas para NAT" para más detalles.

7.9.1.3. Firewall está habilitado en el equipo de destino

Otra cosa a considerar es que pfSense puede reenviar el puerto correctamente, pero un servidor de seguridad en el equipo de destino puede estar bloqueando el tráfico. Si hay un firewall en el sistema objetivo, tendrá que comprobar sus registros y configuración para confirmar si el tráfico está siendo bloqueado en ese punto.

7.9.1.4. pfSense no es puerta de entrada del sistema de destino

Con el fin de pfSense que transmita correctamente un puerto para un sistema local, pfSense debe ser el valor por defecto
puerta de entrada para el sistema de destino. Si pfSense no es la puerta de entrada, el sistema de destino intentará enviar las respuestas al tráfico portuario hacia adelante a cualquier sistema es la puerta, y luego uno de los dos las cosas van a suceder: embargo, se eliminará en ese momento ya no habría conexión correspondiente Estado en que el router - o - que habría que aplicar NAT del router y luego se redujo en el sistema que origina la solicitud ya la respuesta es de una dirección IP diferente de la de que la solicitud se envió inicialmente.

7.9.1.5. La máquina de destino no está escuchando en el puerto redirigido

Si, cuando la conexión se prueba, se rechaza la solicitud en lugar de tiempo de espera, con toda probabilidad pfSense es el reenvío de la conexión correcta y la conexión es rechazada por el sistema de destino. Esto puede ocurrir cuando el sistema de destino no tiene servicio de escucha en el puerto en cuestión, o si el puerto que está siendo enviado no coincide con el puerto en el que el sistema de destino está a la escucha.

Por ejemplo, si el sistema de destino se supone que es música para conexiones SSH, pero el puerto adelante se introdujo por el puerto 23 en lugar de 22, la petición lo más probable es que sea rechazada. Usted puede por lo general la diferencia al tratar de conectar con el puerto en cuestión a través de telnet. Un mensaje tales como Conexión rechazada indica algo, con frecuencia de acogida en el interior, se activa negarse la conexión.

7.9.1.6. ISP está bloqueando el puerto que está tratando de avanzar

En algunos casos, los ISP filtrar el tráfico entrante a los puertos conocidos. Revise los términos de su ISP de Servicio (TOS), y ver si hay una cláusula sobre la ejecución de los servidores. Estas restricciones son más comunes en las conexiones residenciales de conexiones comerciales. En caso de duda, una llamada a la ISP puede aclarar el asunto.

Si los puertos están siendo filtrados por su ISP, puede que tenga que mover sus servicios a un puerto diferente con el fin de evitar la filtración. Por ejemplo, si su ISP no permite servidores en el puerto 80, prueba 8080 o 8888.

Antes de tratar de evitar un filtro, consulte a su equipo de especialistas del ISP para asegurarse de que no está violando sus reglas.

7.9.1.7. Prueba del interior de su red en lugar de fuera de

De forma predeterminada, delante del puerto sólo funciona cuando las conexiones se realizan desde fuera de su red. Esto es un error muy común cuando se prueba delante del puerto.

Si necesita delante del puerto de trabajar internamente, véase Sección 7.5, "Reflexión NAT". Sin embargo, Dividir el DNS (Sección 7.5.2, "Split DNS") Es una solución más apropiada y elegante a este problema sin necesidad de depender de la reflexión NAT o hacia el puerto, y sería digno de su tiempo para aplicar en su lugar.

7.9.1.8. Es incorrecta o falta de direcciones IP virtuales

Al utilizar direcciones IP que no son los reales direcciones IP asignadas a una interfaz, debe uso de direcciones IP virtuales (VIP, consulte Sección 6.8, "IPs virtuales"). Si un puerto para la conexión de una dirección IP alternativa no funciona, puede que tenga que cambiar a un tipo diferente de VIP. Por ejemplo, es posible que necesite utilizar un tipo de proxy ARP en lugar de un "otro" tipo VIP.

Cuando la prueba, asegúrese también de que se está conectando a la adecuada VIP.

7.9.1.9. pfSense no es la frontera / router de frontera

En algunos casos, pfSense es un enrutador interno, y hay otros routers entre éste y el Internet también realizan NAT. En tal caso, un puerto para la conexión tendría que ser inscrito en la Edge Router reenvío del puerto de pfSense, que luego se utiliza otro puerto para la conexión a conseguirlo en el sistema local.

7.9.1.10. Además las pruebas necesarias

Si ninguna de estas soluciones le ayudó a obtener un puerto de trabajo hacia adelante, consulte Capítulo 25, Paquete Captura para obtener información sobre el uso de capturas de paquetes para diagnosticar problemas de reenvío de puerto.

7.9.2. NAT Reflexión Solución de problemas

NAT Reflexión (Sección 7.5, "Reflexión NAT") Es más de una chapuza que una solución, y como tal es propenso a no funcionar como se esperaba. No podemos recomendar lo suficiente que utilice Split DNS en su lugar (ver Sección 7.5.2, "Split DNS"). Si NAT La reflexión no está funcionando correctamente, asegúrese de que fue activado de la manera correcta, y asegurarse de que no son el reenvío de una amplia gama de puertos.

NAT normas de reflexión también se duplican para cada interfaz presente en el sistema, así que si usted tiene una gran cantidad de delanteros del puerto y las interfaces, el número de reflectores puede fácilmente superar los límites de la del sistema. Si esto ocurre, una entrada se imprime en los registros del sistema.

7.9.2.1. Web Access es roto con NAT habilitado Reflexión

Si usted tiene un mal especificado de puertos NAT hacia adelante, puede causar problemas cuando NAT La reflexión es permitido. La forma más común de este problema se plantea es cuando usted tiene una web local servidor y el puerto 80 es enviado allí con un mal especificado de direcciones externas.

Si NAT reflexión está habilitado y la dirección externa se establece en **cualquier**, Cualquier conexión que hacen
aparece como su propia página web. Para solucionar este problema, edite el NAT del puerto hacia adelante para el puerto de ofender,
y el cambio de direcciones externa a **Dirección de interfaz** en su lugar.

Si realmente necesita una dirección externa de **cualquier**, A continuación, NAT La reflexión no funciona para usted, y tendrá que emplear a Split DNS en su lugar.

7.9.3. Solución de problemas de salida NAT

Cuando haya activado NAT manual de salida, y hay varias subredes locales, un
entrada de NAT de salida será necesario para cada uno. Esto se aplica especialmente si va a tener tráfico
salir con NAT después de entrar en el router pfSense través de una conexión VPN como PPTP o OpenVPN.

Un indicio de una regla NAT saliente falta sería paquetes ver salir de la interfaz WAN
con una dirección de origen de una red privada. Ver Capítulo 25, Captura de paquetes para obtener más detalles en la obtención e interpretación de captura de paquetes.

Capítulo 8. Enrutamiento

Una de las principales funciones de un servidor de seguridad es de enrutamiento de tráfico, además de filtrar y realizar
NAT. Este capítulo se refiere a varios temas relacionados con la ruta, incluyendo las rutas estáticas, protocolos de enrutamiento,
enrutamiento de direcciones IP públicas, y mostrar la información de enrutamiento.

8.1. Rutas estáticas

Las rutas estáticas se utilizan cuando se han hosts o redes accesibles a través de un otro router que no sea su puerta de enlace predeterminada. Su firewall o router conoce las redes directamente unido a él, y
llega a todas las demás redes según las indicaciones de su tabla de enrutamiento. En las redes donde se tiene una interna
router conectar subredes internas adicionales, debe definir una ruta estática para que la red de
ser alcanzable.

8.1.1. Ejemplo de ruta estática

Figura 8.1, "ruta estática" ilustra un escenario en el que se requiere una ruta estática.

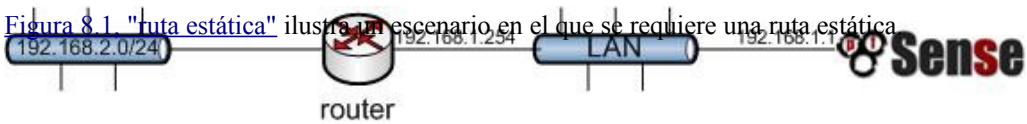


Figura 8.1. Ruta estática

Debido a que la red 192.168.2.0/24 en Figura 8.1, "ruta estática" no está en una relación directa
interfaz de pfSense, necesita una ruta estática para que sepa cómo llegar a esa red. Figura 8.2, "Configuración de rutas estáticas" muestra la ruta estática adecuado para el diagrama anterior.

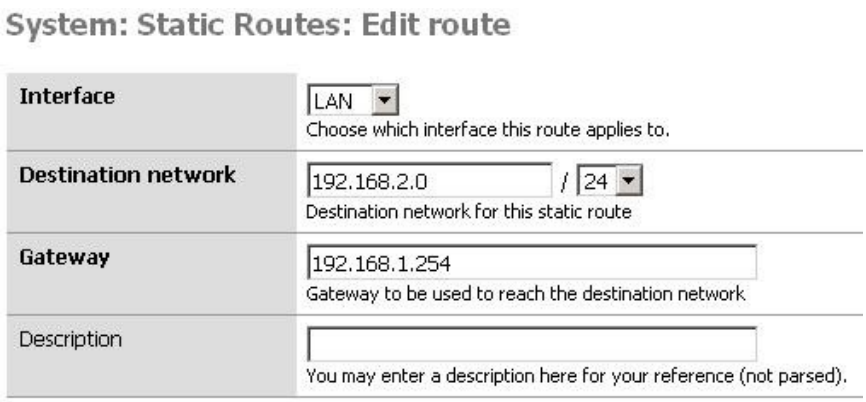


Figura 8.2. Configuración de rutas estáticas

La caja de interfaz define la interfaz, donde la puerta de enlace es accesible. La

Red de destino especifica la subred accesible a través de esta ruta. Puerta de enlace especifica el período de investigación la dirección del router en esta red es accesible. Esta debe ser una dirección IP dentro de la subred IP de la interfaz elegida. ajustes de servidor de seguridad regla también puede ser requerido. El valor por defecto LAN única regla permite el tráfico procedente de la subred LAN, por lo que si mantiene esa norma, que tendrá que abrir la red de origen para incluir también a las redes accesibles a través de rutas estáticas de la LAN. La siguiente sección describe un escenario común con rutas estáticas para que también vosotros revisión.

8.1.2. Bypass reglas de firewall para el tráfico en la misma interfaz

En muchos casos cuando se utiliza rutas estáticas se termina con el enrutamiento asimétrico. Esto significa que el tráfico en una dirección tomará un camino diferente del tráfico en la dirección opuesta. Tome Figura 8.3, "asimétrica de enrutamiento" por ejemplo.

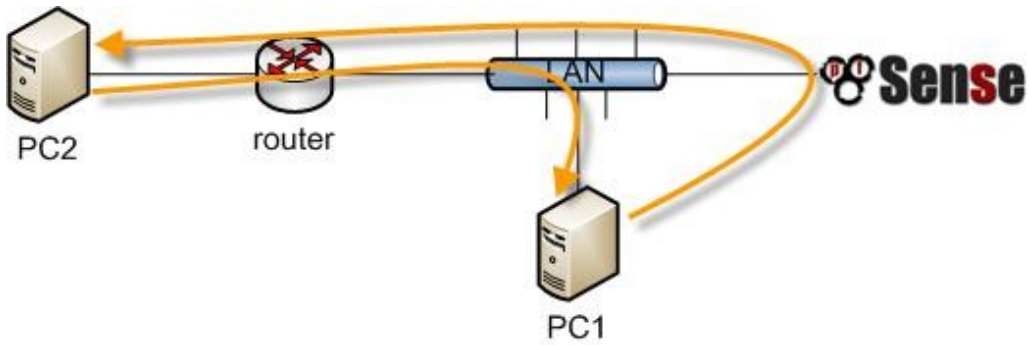


Figura 8.3. Enrutamiento asimétrico

El tráfico de PC1 a PC2 pasará por pfSense, ya que es PC1 de puerta de enlace predeterminada, pero el tráfico en
la dirección opuesta irán directamente desde el router a la PC1. Desde pfSense es un firewall,
debe velar por todos los de la conexión para poder filtrar el tráfico correctamente. Con el enrutamiento asimétrico
de esta manera, cualquier servidor de seguridad con estado acabará cayendo el tráfico de fiar porque no pueden mantener adecuadamente
estado sin ver el tráfico en ambas direcciones. Compruebe siempre las reglas del firewall de derivación para el tráfico en la caja misma interfaz en el Sistema → Avanzada la página en los escenarios de enrutamiento asimétrico para evitar el tráfico legítimo de ser retirados. Esto se suma reglas de firewall que permite todo el tráfico entre las redes se definen en las rutas estáticas con ninguna opción estado PF. Como alternativa, puede agregar las reglas del firewall se especifica **ninguno** como el tipo de Estado, el tráfico de correspondencia entre lo local y lo subredes remotas, pero que generalmente no se recomienda debido a la complejidad que puede presentar y la mayor probabilidad de errores. En caso de necesidad de filtrar el tráfico entre estáticamente enrutado subredes, se debe hacer en el router y no el servidor de seguridad desde el servidor de seguridad no está en condiciones de en la red donde se puede controlar el tráfico.

8.1.3. Redirecciones ICMP

Cuando un dispositivo envía un paquete a su puerta de enlace predeterminada, y la puerta de entrada sabe que el emisor puede llegar a la red de destino a través de una ruta más directa, se enviará un mensaje de redirección ICMP en respuesta y remitir el paquete tal como está configurado. La redirección ICMP causa una ruta para ese destino a se añadirá a la tabla de enrutamiento del dispositivo de envío, y el dispositivo que posteriormente utilizará ruta más directa para llegar a esa red. Esto no funcionará si su sistema operativo está configurado para no permitir Redirecciones ICMP, que no suele ser el caso por incumplimiento.

Redirecciones ICMP son comunes cuando se tiene una ruta estática que apunta a un enrutador en la misma interfaz de PC como cliente y otros dispositivos de red. El diagrama de enrutamiento asimétrico de la sección anterior es un ejemplo de esto.

Redirección ICMP en su mayoría han inmerecidamente recibido una mala reputación de algunos en la seguridad
comunidad debido a que permiten la modificación de la tabla de enrutamiento de un sistema. Sin embargo, no se el riesgo de que algunos suponen, como para ser aceptado, el mensaje de redirección ICMP debe incluir la primera 8 bytes de datos del datagrama original. Una gran cantidad en condiciones de ver que los datos y por lo tanto poder para forjar con éxito ilícito redirecciones ICMP se encuentra en una posición para lograr el mismo resultado final en varias otras maneras.

8.2. Enrutamiento IP Pública

Esta sección cubre la ruta de IPs públicas, donde hay un público subred IP asignada al
una interfaz interna, y las implementaciones de un solo servidor de seguridad. Si está utilizando CARP, consulte Sección 20.7,
"Proporcionar redundancia Sin NAT".

8.2.1. Asignación de IP

Usted necesita por lo menos dos subredes IP pública asignada por su ISP. Uno es para la WAN de su
servidor de seguridad, y uno para la interfaz en el interior. Este es comúnmente un / 30 de subred de la WAN, con un segunda subred asignada a la interfaz interna. En este ejemplo se utilizará un / 30 sobre la WAN, como se muestra en Tabla 8.1, "Block WAN IP" y un / 29 de subred pública en una interfaz OPT interno como se muestra en Tabla 8.2, "Dentro del bloque de IP".

11.50.75.64/30	
Dirección IP	Asignado a
11.50.75.65	router del ISP (pfSense puerta de enlace predeterminada IP)
11.50.75.66	pfSense interfaz WAN IP

Tabla 8.1. Bloque IP WAN

192.0.2.128/29	
Dirección IP	Asignado a
192.0.2.129	pfSense interfaz OPT
192.0.2.130	Interior anfitriones
192.0.2.131	
192.0.2.132	
192.0.2.133	

192.0.2.128/29	
Dirección IP	Asignado a
192.0.2.134	

Tabla 8.2. Dentro del bloque

IP

8.2.2. Interfaz de configuración

En primer lugar, configure las interfaces WAN y el territorio palestino ocupado. La interfaz LAN también se puede utilizar para IPs públicas
si lo desea. En este ejemplo, LAN es una organización privada de subred IP y OPT1 es el público de subred IP.

8.2.2.1. Configurar WAN

Agregue la dirección IP y puerta de enlace en consecuencia. Figura 8.4, "WAN IP y la configuración de puerta de enlace" muestra de la WAN se configura como se muestra en la Tabla 8.1, "Block WAN IP".

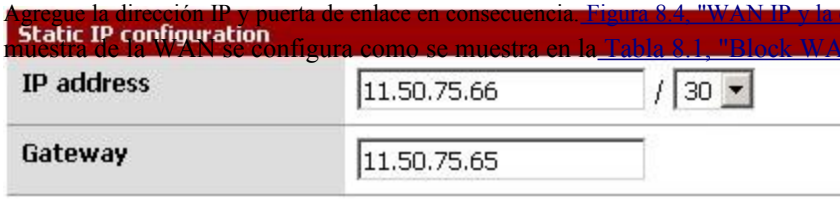


Figura 8.4. WAN IP y la configuración de puerta de enlace

8.2.2.2. Configurar OPT1

Ahora permiten OPT1, opcionalmente cambiar su nombre, y configurar la dirección IP y la máscara.
Figura 8.5, "Configuración de enrutamiento OPT1" muestra OPT1 configurado como se muestra en Tabla 8.2, "Dentro del bloque IP".

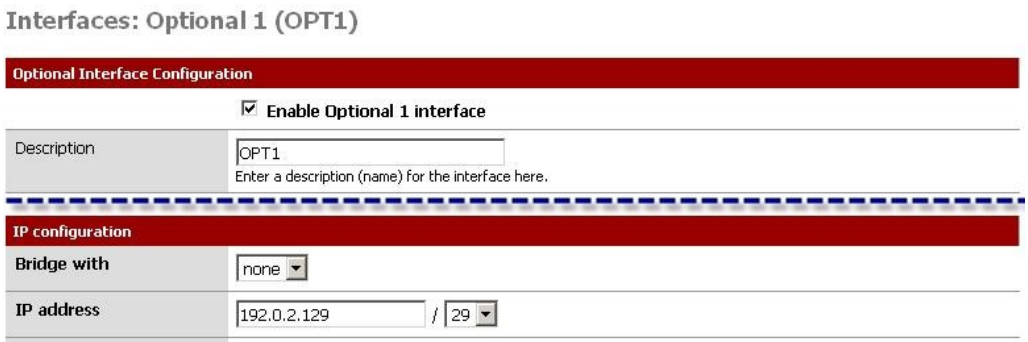


Figura 8.5. Configuración de enrutamiento OPT1

8.2.3. Configuración de NAT

El valor predeterminado de traducir el tráfico interno a la IP WAN debe ser anulado cuando se utiliza IPs públicas en una interfaz interna. Vaya a Servidor de seguridad → NAT, y haga clic en la ficha de salida. Seleccione Manual salida generación de reglas NAT y haga clic en Guardar. Esto generará una norma por defecto traducción de todo el tráfico de la subred LAN de salir de la interfaz WAN a la IP WAN, el valor predeterminado comportamiento de pfSense. Si su red contiene una subred privada como en este ejemplo, esta es la exacta configuración deseada. El tráfico procedente de la red 192.0.2.128/29 OPT1 es no traducidas porque la fuente se limita a 192.168.1.0/24. Esta configuración se muestra en la Figura 8.6, "Salida de configuración NAT". Si utiliza direcciones IP públicas en su LAN, eliminar automáticamente agregó entrada. A continuación, haga clic en Aplicar cambios.

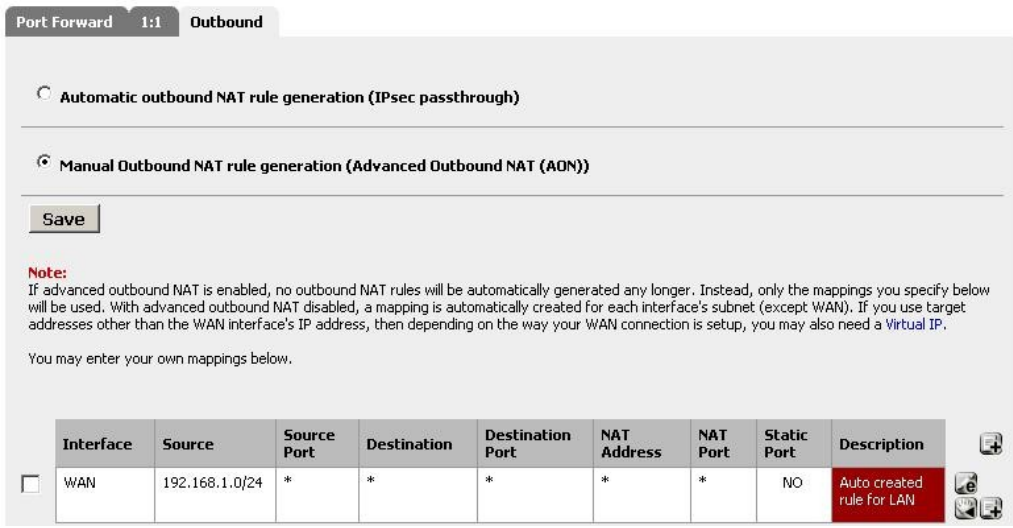


Figura 8.6. Salida de configuración NAT

8.2.4. Configuración del Firewall artículo

La configuración de NAT y el período se ha completado. Las reglas de firewall deberá añadirse a permitir el tráfico saliente y entrante. Figura 8.7, "OPT1 las reglas del cortafuegos" muestra una zona de despeje, como configuración, donde se rechaza todo el tráfico destinado a la subred LAN, DNS y pings a la OPT1 interfaz IP están permitidas, y se permite la salida HTTP.

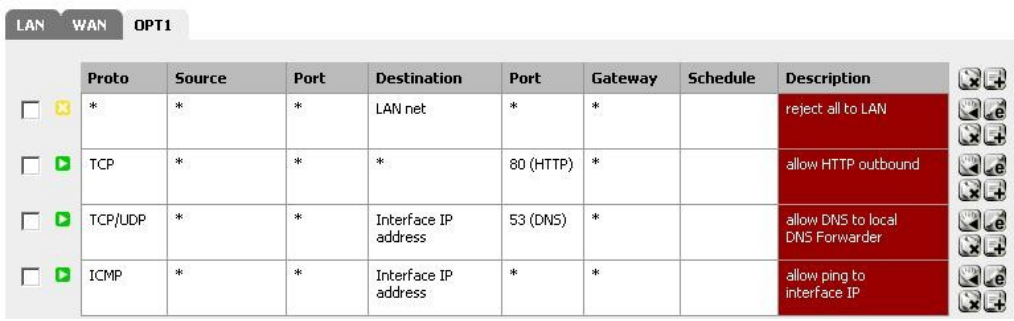


Figura 8.7. normas OPT1 cortafuegos

Para permitir el tráfico de Internet a las direcciones IP públicas en una interfaz interna, necesita añadir reglas en la WAN utilizando la IP pública como el destino. Figura 8.8, "las reglas del firewall WAN" muestra una regla que permite HTTP a 192.0.2.130, una de las IPs públicas en la interfaz interna, como se muestra en Tabla 8.2, "Dentro del bloque de IP".

Figura 8.8. WAN reglas de firewall

Después de configurar las reglas del firewall si lo desea, la configuración se ha completado.

8.3. Protocolos de enrutamiento

En el momento de escribir estas líneas, dos protocolos de enrutamiento son compatibles con pfSense, RIP (Routing Protocolo de información) y BGP (Border Gateway Protocolo). OSPF (Abrir primero la ruta más corta) es probable que se agregó como un paquete en algún momento. Esta sección es la luz en los detalles, y presume comprensión de los protocolos de enrutamiento, como requisito previo. Una discusión a fondo de enrutamiento protocolos está fuera del alcance de este libro.

8.3.1. RIP

RIP se puede configurar en Servicios → RIP. Para utilizarlo:

1. Compruebe la casilla Habilitar RIP
2. Seleccione las interfaces RIP escuchar y enviar actualizaciones de enrutamiento en
3. Seleccione su versión RIP
4. Cuando se usa RIPv2, introduzca una contraseña RIPv2 si se utiliza en la red.
5. Haga clic en Guardar

RIP de inmediato pondrá en marcha y empezar a enviar y recibir actualizaciones de enrutamiento en el especificado interfaces.

8.3.2. BGP

Un paquete BGP usando OpenBSD OpenBGPD [http://www.openbgpd.org] está disponible. Para instalarlo, visite System → Paquetes y haga clic en el signo más a la derecha de OpenBGPD. Haga clic en Aceptar para

instalar el paquete. A continuación, haga clic en el logotipo de pfSense en la parte superior izquierda, que le llevará a la página de inicio
y volver a cargar los menús. Usted encontrará OpenBGPD en el menú Servicios.

BGP es una complejo bestia, y describiendo que en detalle es fuera el ámbito de aplicación de esta libro. Configuración de pfSense de OpenBGPD es recta hacia adelante si que entender BGP. Durante desarrollo de esta paquete, que se basó en O'Reilly BGP libro [http://www.amazon.com/gp/product/0596002548? es decir, = UTF8 & tag = pfSense-20 y linkCode = AS2 y campo = 1789 = 9325 y creativa y creativeASIN = 0596002548]
y lo recomiendo para cualquiera que quiera implementar BGP.

8.4. Ruta Solución de problemas

Cuando el diagnóstico de problemas de flujo de tráfico, una de las primeras cosas que debe verificar son las rutas conocidas
pfSense.

8.4.1. Visualización de las rutas

Hay dos maneras de ver las rutas: A través de la WebGUI, ya través de la línea de comandos.

Para ver las rutas en la WebGUI, visita de diagnóstico → Rutas y podrás ver la salida como que se muestra en la Figura 8.9, "Mostrar ruta".

Destination	Gateway	Flags	Refs	Use	Mtu	Netif	Expire
Default	10.0.2.2	UGS	0	52	1500	le0	
10.0.2.0/24	link#1	UC	0	0	1500	le0	
10.0.2.2	52:54:00:12:35:02	UHLW	2	30	1500	le0	850
10.0.2.15	127.0.0.1	UGHS	0	0	16384	lo0	
127.0.0.1	127.0.0.1	UH	1	0	16384	lo0	
192.168.56.0/24	link#2	UC	0	0	1500	le1	
192.168.56.101	08:00:27:00:d4:84	UHLW	1	521	1500	le1	1160

Figura 8.9. Ruta de pantalla

La salida de la línea de comandos es similar a la observada en el WebGUI:

#netstat-rn
```
Las tablas de enrutamiento

Internet:
```

```
Destino Banderas Gateway Refs Use Netif Vencimiento
predeterminado 10.0.2.2 UGS 0 53 le0
link 10.0.2.0/24 # 1 de la UC 0 0 le0
10.0.2.2 52:54:00:12:35:02 UHLW 2 35 796 le0
10.0.2.15 127.0.0.1 UGHS 0 0 lo0
127.0.0.1 127.0.0.1 UH 1 0 lo0
enlace 192.168.56.0/24 # 2 de la UC 0 0 le1
192.168.56.101 08:00:27:00: d4: 84 UHLW 1 590 le1 1197
```

Las columnas aparecen en estas pantallas indicar diversas propiedades de las rutas, y se explican siguiente.

8.4.1.1. Destino

El host de destino o de la red. La ruta por defecto para el sistema es simplemente aparece como

"predeterminado".

De lo contrario, los anfitriones se enumeran por su dirección IP y las redes se muestran con una dirección IP y CIDR máscara de subred.

8.4.1.2. Gateway

Un gateway es el router que los paquetes que van a un destino específico necesario para ser enviados. Si este columna muestra un enlace, como el enlace # 1, luego de que la red es directamente accesible desde la interfaz y no especiales de encaminamiento es necesario. Si un host es visible con una dirección MAC, entonces es un local
de acogida puede llegar con una entrada en la tabla ARP, y los paquetes son enviados allí directamente.

8.4.1.3. Banderas

Hay un buen número de banderas de unos pocos, todos los cuales están cubiertos en la página del manual de FreeBSD		
`netstat (1)`, ~~reproduce en el Tabla 8.3, "Banderas tabla de rutas y significados" con algunas modificaciones.~~		
Carta	Bandera	168
1	RTF_PROTO1	
2	RTF_PROTO2	
3	RTF_PROTO3	

B	RTF_BLACKHOLE
b	RTF_BROADCAST

Significado	Protocolo específico bandera de enrutamiento # 2	Protocolo específico bandera de enrutamiento # 3
Protocolo específico bandera de enrutamiento # 1	Protocolo específico bandera	Descartar paquetes durante el actualizaciones
		Representa una dirección de broadcast

C	RTF_CLONING	Generar nuevas rutas en el uso
c	RTF_PRCLONING	Protocolo especificado por generar nuevas rutas en el uso
D	RTF_DYNAMIC	Creado dinámicamente por redirigir
G	RTF_GATEWAY	Destino requiere transmisión por intermediario
H	RTF_HOST	entrada de host (neto de otra manera)
L	RTF_LLINFO	protocolo válido para vincular la dirección traducción
M	RTF_MODIFIED	Modificados dinámicamente (por redirección)
R	RTF_REJECT	Host o una red inalcanzable
S	RTF_STATIC	Agregar manualmente
U	RTF_UP	Ruta útil
W	RTF_WASCLONED	Ruta se generó como resultado de la clonación
X	RTF_XRESOLVE	Externo se traduce demonio proto vincular la dirección

Tabla 8.3. Ruta de las banderas de mesa y de significados

Por ejemplo, una ruta marcada como UGS es una vía útil, los paquetes se envían a través de la puerta de entrada en la lista,
y es una ruta estática.

8.4.1.4. Refs

Esta columna cuenta el número actual de los usos activos de una ruta determinada.

8.4.1.5. Utilice

Este contador es el número total de paquetes enviados a través de esta ruta. Esto es útil para determinar si un ruta se está utilizando, ya que continuamente incremento en el flujo de paquetes si esta ruta se utilizó.

8.4.1.6. Netif

La interfaz de red utilizada para esta ruta.

8.4.1.7. Expirará

Para las entradas dinámicas, este campo muestra la duración de esta ruta hasta que caduca si no se utiliza de nuevo.

8.4.2. Usando traceroute

Traceroute es una herramienta útil para probar y verificar las rutas y la funcionalidad multi-WAN, entre otros usos. Esto le permitirá ver cada "salto" a lo largo de la ruta de un paquete a medida que viaja de un extremo a la otra, junto con la latencia encontrado en llegar a ese punto intermedio. En pfSense, puede realizar un rastreo de ruta yendo a diagnósticos → Trazado, o usando traceroute en el de línea de comandos. De los clientes que ejecutan Windows, el programa está disponible bajo los tracert nombre.

Cada paquete IP contiene un tiempo de vida (TTL). Cuando un router pasa un paquete, disminuye el TTL en uno. Cuando un router recibe un paquete con un TTL de 1 y el destino no es un red conectada localmente, el enrutador devuelve un mensaje de error ICMP - Tiempo para vivir superado - Y descarta el paquete. Esto es para limitar el impacto de los bucles de enrutamiento, que de otro modo hacen que cada paquete de un bucle indefinidamente.

Trazado utiliza esta TTL a su favor para asignar la ruta a un destino de red específica. Es se inicia mediante el envío del primer paquete con un TTL de 1. El primer router (normalmente por defecto del sistema gateway) devolverá el error ICMP superado el tiempo de vivir. El tiempo entre el envío del paquete y recibir el error ICMP es la hora que se muestra, aparece junto con la IP que envió el error y su DNS inversa, si los hubiere. Después de enviar tres paquetes con un TTL de 1 y mostrar sus tiempos de respuesta, se incrementa el TTL en 2 y envía tres paquetes más, teniendo en cuenta la misma información para el segundo salto. Mantiene incrementando el TTL hasta que llega a la especificada destino, o excede el número máximo de saltos.

Trazado de funciones de forma ligeramente diferente en Windows y sistemas operativos tipo Unix (BSD, Linux, Mac OS X, Unix, etc.) Windows utiliza paquetes de solicitud de eco ICMP (ping), mientras que en Unix sistemas como el uso de paquetes UDP. ICMP y UDP son los protocolos de la capa 4, y la Ruta de seguimiento se realiza en la capa 3, por lo que el protocolo utilizado es irrelevante, excepto cuando se considera su política de enrutamiento de configuración. Trazado de los clientes de Windows se encamina la política sobre la base de que la regla permisos de peticiones de eco ICMP, mientras que los clientes Unix serán enviados por la regla de correspondencia de la UDP en uso.

En este ejemplo, vamos a tratar de encontrar la ruta a www.google.com:

```
#traceroute www.google.com
traceroute: Warning: www.google.com tiene varias direcciones, utilizando
74.125.95.99
traceroute para www.l.google.com (74.125.95.99), 64 saltos máximo, 40
paquetes de bytes
```

```
 1 conductor (172.17.23.1) 1.450 ms 1.901 ms 2.213 ms
 2 172.17.25.21 (172.17.25.21) 4,852 ms 3.698 ms 3.120 ms
 3 BB1-g4-0-2.ipltin.ameritech.net (151.164.42.156) 3.275 ms 3.210 ms 3.215
ms
 4 151.164.93.49 (151.164.93.49) 8,791 ms 8.593 ms 8.891 ms
 5 74.125.48.117 (74.125.48.117) 8,460 ms 39.941 ms 8.551 ms
 6 209.85.254.120 (209.85.254.120) 10,376 ms 8.904 ms 8.765 ms
 7 209.85.241.22 (209.85.241.22) 19,479 ms 20.058 ms 19.550 ms
 8 209.85.241.29 (209.85.241.29) 20,547 ms 19.761 ms
    209.85.241.27 (209.85.241.27) 20,131 ms
 9 209.85.240.49 (209.85.240.49) 30,184 ms
    72.14.239.189 (72.14.239.189) 21,337 ms 21.756 ms
10 iw en f99.google.com (74.125.95.99) 19.793 ms 19.665 ms 20.603 ms
```

Como puede ver, tomó 10 saltos para llegar allí, y la latencia en general aumenta con cada salto.

8.4.3. Rutas y VPN

Dependiendo de la VPN se utiliza, puede o no puede ver una ruta que muestra en la tabla para el lejos a tu lado. IPsec no utiliza la tabla de enrutamiento, en su lugar se manejan internamente en el núcleo usando
el SPD IPsec. Las rutas estáticas no hará que el tráfico que se dirige a través de una conexión IPsec. OpenVPN utiliza el sistema de la tabla de enrutamiento y, como tal, podrás ver las entradas de las redes accesibles
a través de un túnel OpenVPN, como en el ejemplo siguiente:

#**netstat-rn**

```
Las tablas de enrutamiento

Internet:
Destino Banderas Gateway Refs Use Netif Vencimiento
predeterminado 10.34.29.1 UGS 0 19693837 ng0
10.34.29.1 72.69.77.6 UH 1 205 590 ng0
72.69.77.6 lo0 UHS 0 0 lo0
172.17.212.0/22 192.168.100.1 UGS 0 617 tun0
127.0.0.1 127.0.0.1 UH 0 0 lo0
enlace 192.168.10.0/24 # 2 de la UC 0 0 Em0
192.168.100.1 192.168.100.2 UH 3 0 tun0
192.168.130.0/24 192.168.100.1 UGS 0 144 143 tun0
192.168.140.0/24 192.168.100.1 UGS 0 0 tun0
```

La interfaz de OpenVPN es 192.168.100.2, con una puerta de entrada de 192.168.100.1 y la interfaz tun0. Hay tres redes con OpenVPN empujó rutas en ese ejemplo: 192.168.130.0/24, 192.168.140.0/24 y 172.17.212.0/22.

Con IPsec, traceroute no es tan útil como con las configuraciones de enrutado como OpenVPN, ya que el IPsec túnel en sí no tiene direcciones IP. Cuando se ejecuta traceroute a un destino a través de IPsec, se le ver un tiempo de espera para el salto que es el túnel IPsec por esta razón.

Capítulo 9. Puente

Normalmente, cada interfaz en pfSense representa su propio dominio de difusión con una única subred IP, actuando de la misma como interruptores separados. En algunas circunstancias es deseable o necesario combinar interfaces múltiples en un único dominio de difusión, donde dos puertos en el firewall actúan como si estuvieran en el mismo switch, excepto el tráfico entre las interfaces pueden ser controlados con las reglas del cortafuegos. Esto se conoce comúnmente como cortafuegos transparente.

9.1. Puente y la capa 2 Loops

Cuando puente, es necesario tener cuidado para evitar la capa 2 bucles, o tiene una configuración de interruptor en lugar que las trata como usted desea. Una capa de 2 bucle es cuando se crea el mismo efecto que si conectado los dos extremos de un cable de conexión en el mismo interruptor. Si usted tiene una instalación con dos pfSense interfaces, las interfaces de puente juntos, a continuación, conecte las dos interfaces en el mismo interruptor que han creado una capa de 2 bucle. La conexión de dos cables de conexión entre dos switches también lo hace. switches gestionables emplean Spanning Tree Protocol (STP) para manejar situaciones como ésta, porque a menudo es deseable tener múltiples enlaces entre los switches, y usted no desee que su red estar expuesto al colapso total por alguien conectar un puerto de red a otra red puerto. STP no está habilitado por defecto en todos los switches gestionados sin embargo, y casi nunca disponibles con switches no gestionables. Sin STP, el resultado de una capa de 2 bucle marcos en la red círculo sin fin y la red será completamente dejará de funcionar hasta que el lazo se quita.
En pocas palabras - puente tiene el potencial de derretirse por completo por la red a la que conectar en caso de no ver lo que estás conectando dónde.

9.2. Puente y cortafuegos

Con funciones de filtrado de interfaces de puente de manera diferente que con interfaces de enrutado. Servidor de seguridad normas se aplican a cada miembro de interfaz del puente sobre una base de entrada. Los que han pfSense estado utilizando durante bastante tiempo recordarán un cuadro Habilitar el filtrado de verificación en el puente Sistema de → Página de avanzada. No está actualizado la información en referencia a numerosos lugares de este casilla de verificación. Fue heredado de m0n0wall, que hizo cerrar de una manera diferente. Desde pfSense utiliza una metodología diferente superar este cuadro no es necesario, y con la forma en la reducción de la metodología en las últimas versiones de FreeBSD funciona es imposible tener un puente no filtrado a menos que pf desactivar por completo.

9.3. Puente entre dos redes internas

Puede puente de dos interfaces internas para combinar en el mismo dominio de broadcast y permitir filtrado de tráfico entre las dos interfaces. Esto se hace comúnmente con interfaces inalámbricas configurado como un punto de acceso, para conectar los segmentos de cable e inalámbricas en la misma emisión dominio. De vez en cuando un servidor de seguridad con una interfaz LAN y OPT se utilizará en lugar de un interruptor en redes en las que sólo dos sistemas internos son necesarios. Usted puede encontrar escenarios en los que dos interfaces del servidor de seguridad deben estar en el mismo dominio de broadcast por otra razón.

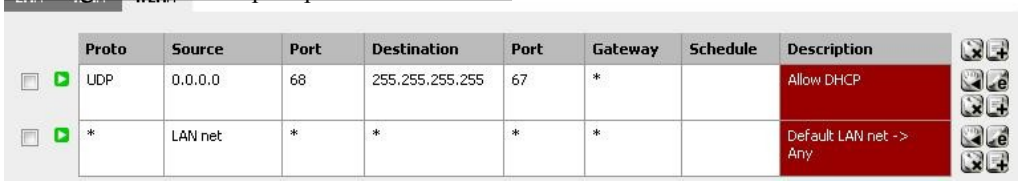
Nota

Existen requisitos adicionales y restricciones al puente inalámbrico interfaces por la forma en 802,11 funciones. Ver Sección 18.3, "Reducción y sin hilos " para más información.

9.3.1. DHCP y puentes internos

Si un puente de red interna a otra, dos cosas se deben hacer. En primer lugar, asegúrese de que DHCP sólo se ejecuta en la interfaz principal (el que tiene la dirección IP) y no el que se está puente. En segundo lugar, usted necesitará una regla de servidor de seguridad adicionales en la parte superior de las reglas en este territorio palestino ocupado interfaz para permitir el tráfico DHCP.

Normalmente, al crear una regla para permitir el tráfico en una interfaz, la fuente se especifica similares a "OPT1 subred", por lo que sólo el tráfico de la subred se les permite salir de ese segmento. Con DHCP, que no es suficiente. Debido a que un cliente no cuenta aún con una dirección IP, una solicitud DHCP realiza como una emisión. Para adaptarse a estas solicitudes, debe crear una regla en el puente interfaz con el protocolo establecido en **UDP**, El origen es **0.0.0.0**, Puerto de origen **68**, Destino **255.255.255.255**, Puerto de destino **67**. Añadir una descripción que indica que esto **Permitir DHCP**, a continuación, haga clic en Guardar cambios y aplicar. Usted va a terminar con una regla que parece Figura 9.1, "Las reglas de firewall para permitir el DHCP".



	Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
	UDP	0.0.0.0	68	255.255.255.255	67	*		Allow DHCP
	*	LAN net	*	*	*	*		Default LAN net -> Any

Figura 9.1. Las reglas de firewall para permitir el DHCP

Después de añadir esta regla, los clientes en el segmento de puente debe ser capaz de realizar con éxito pide al demonio DHCP escuchando en la interfaz a la que se tiende un puente.

9.4. Superar OPT a la WAN

Superar una interfaz opcional con WAN que permite utilizar IPs públicas en su red interna que tener una puerta de enlace IP que residen en la red WAN. Una situación en la que esto es común es para DHCP asigna direcciones IP públicas. Usted puede utilizar pfSense para proteger los sistemas que obtienen pública IP directamente desde su servidor ISP DHCP mediante una interfaz de puente. Esto también es útil en escenarios con un solo bloque IP pública donde se necesita IPs públicas directamente asignados a los hosts, como se describe en Sección 6.7.1.2.1, "Single subred IP".

9.5. Reducción de la interoperabilidad

Desde interfaces puente comportan de manera diferente que las interfaces normales en algunos aspectos, hay algunas cosas que son incompatibles con el puente, y otras en las consideraciones adicionales se debe hacer para dar cabida a salvar. En esta sección se describen las funciones que trabajan de manera diferente con puente que con interfaces no puenteado.

9.5.1. Portal cautivo

Portal cautivo (Capítulo 19, Portal Cautivo) No es compatible con el puente, ya que requiere una dirección IP en la interfaz que es un puente, que se utiliza para servir a los contenidos del portal. interfaces de puente no tiene una IP asignada.

9.5.2. CARP

CARP (Capítulo 20, Firewall de redundancia / alta disponibilidad) no es compatible con el puente en esta vez - pero, hay algunos hacks manual. Uso de CARP con las redes que involucran puente Generalmente no se recomienda, pero este tipo de instalación ha trabajado para un número de individuos. Gran cuidado se debe tomar para manejar la capa 2 bucles, que son inevitables en una carpa + Puente escenario. Cuando dos segmentos de red son un puente, que están en vigor se fusionaron en uno más grande de red, como se explicó anteriormente en este capítulo. Cuando CARP se añade a la mezcla, eso significa que hay será de dos vías entre los interruptores para cada interfaz respectiva, la creación de un bucle. switches gestionables puede manejar esto con Spanning Tree Protocol (STP), pero switches no gestionables no tienen defensas contra el bucle. Si no se controla, puede poner un lazo de una red de rodillas y hacen que sea imposible de pasar todo el tráfico. Si STP no está disponible, hay otros dos enfoques para el manejo de un puente en este escenario, similar pero no tan elegante como STP. Ambos métodos

necesario cambiar los archivos en el sistema de pfSense, y no podría sobrevivir una copia de seguridad / restauración, sin
una consideración especial. Estas técnicas son una secuencia de comandos cron para gestionar el puente, o un gancho DEVD
para gestionar el puente. Ambos métodos se describen en un puesto pegajosa en el CARP / VIP
[Foro http://forum.pfsense.org/index.php/topic, 4984.0.html].[1]

9.5.2.1. Configurar los servidores de seguridad primaria y de copia de seguridad

Configurar los servidores de seguridad primaria y de copia de seguridad como lo haría con cualquier implementación de

CARP, como
cubiertos en Capítulo 20, Firewall de redundancia / alta disponibilidad. Configure el puente de interfaz
tanto en la primaria y secundaria, con la descripción misma interfaz. Si el puente se OPT1
en el primario, lo convierten en OPT1 en el secundario. No conecte ambos puentes al mismo tiempo
hasta el final. Tendrá que ser capaz de acceder a la pfSense WebGUI desde una interfaz de servidor de seguridad
que no sea la interfaz de puente. Usted tendrá que realizar todos estos pasos, tanto para la primaria
y cortafuegos secundaria.

9.5.2.2. Configuración STP

Incluso con STP activa, la configuración será necesario en el interruptor con el fin de empujar STP
en tomar la decisión correcta sobre qué puerto debe mantenerse abierta y que debe ser bloqueado.
De lo contrario, podría terminar con una situación donde el tráfico es en realidad que fluye a través de su
enrutador de copia de seguridad del puente en lugar del router principal, que conduce a un comportamiento impredecible.
Puerto
bloqueo en esta situación se controla mediante el establecimiento de las prioridades del puerto y los costos de ruta.

En un conmutador Cisco, la configuración sería algo como esto:

```
interfaz FastEthernet0 / 1
  descripción Firewall - Primaria - Puerto DMZ
  switchport access vlan 20
  spanning-tree vlan 20 puertos con prioridad 64
  no cdp enable

interfaz FastEthernet0 / 2
  Descripción del servidor de seguridad - Copia de seguridad - Puerto DMZ
  switchport access vlan 20
  spanning-tree vlan 20 costará 500
  no cdp enable
```

Al dar el puerto principal de una prioridad más baja de lo normal (64 vs el valor predeterminado 128), será más
susceptibles de ser utilizados, especialmente dado el coste de la ruta más alta (500 vs el valor predeterminado 19) del puerto.
Estos valores se pueden comprobar de la siguiente manera (en el interruptor):

[1] http://forum.pfsense.org/index.php/topic, 4984.0.html

#mostrar FastEthernet0 spanning-tree interfaz / 1
```
Interfaz FastEthernet0 / 1 (puerto 13) en el Arbol 20 se TRANSMISIÓN
```
ruta Puerto costó 19, Puerto de la prioridad 64
```
Designado raíz tiene prioridad 32768, 0002.4b6e.xxxx dirección
puente designado tiene prioridad 32768, 0002.b324.xxxx dirección
puerto designado es el 3, el recorrido de costo 131
Temporizadores: edad mensaje 6, adelante retraso 0, mantenga oprimida 0
BPDU: 18411032 enviado, recibido 16199798
```

#mostrar FastEthernet0 spanning-tree interfaz / 2
```
Interfaz FastEthernet0 / 2 (puerto 14) en el árbol de expansión 20 se
```
BLOQUEO
ruta Puerto costará 500, Puerto de la prioridad 128
```
Designado raíz tiene prioridad 32768, 0002.4b6e.xxxx dirección
puente designado tiene prioridad 32768, 0002.b324.xxxx dirección
puerto designado es el 4, el recorrido de costo 131
Temporizadores: edad mensaje 6, adelante retraso 0, mantenga oprimida 0
BPDU: 434174 enviado, recibido 15750118
```

Como puede ver, el puerto de la red primaria de interruptor de reenvío se debe ser, y la copia de seguridad está bloqueando el puerto. Si el tráfico deja de fluir a través del puerto principal, la copia de seguridad debería cambiar a
un estado de reenvío.

Cambia de otros proveedores de apoyo una funcionalidad similar. Consulte la documentación del conmutador para obtener información sobre la configuración de STP.

En pfSense 2.0, STP se pueden configurar y manejar directamente en una interfaz de puente.

9.5.2.3. CARP secuencia de comandos de verificación de cron

En este método, un script se ejecuta desde cron cada minuto y comprueba si el sistema es MASTER o copia de seguridad del clúster CARP. Si el sistema MASTER, el puente es educado, si el sistema es el respaldo, el puente es derribado. Impide que el bucle sólo por tener un puente activa en un momento dado, pero como usted puede decir probablemente por la frecuencia con la secuencia de comandos cron se ejecuta, no
puede ser tanto como un minuto de tiempo de inactividad de los sistemas de puente antes de que el script detecta el interruptor
y activa el puente de copia de seguridad.

9.5.2.3.1. Añadir la secuencia de comandos

En primer lugar es necesario añadir un script para comprobar el estado de CARP y modificar su estado de puente en consecuencia. A continuación se presenta un ejemplo que puede ser utilizado. También está disponible para
descarga [] Http://files.pfsense.org/misc/bridgecheck.sh.

```
#! / Bin / sh
#
# CARP script de verificación para salvar
#
# De eblevins en el foro
#
si ifconfig carp0 | / grep COPIA DE SEGURIDAD> / dev null 2> & 1, a
continuación,
        / Sbin / ifconfig bridge0 abajo
más
        / Sbin / ifconfig bridge0 hasta
fi
```

Copiar el script en alguna parte, por ejemplo, `/ Usr / bin / bridgecheck.sh`. Los siguientes comando descargar este archivo desde files.pfsense.org y guárdelo como `/ Usr / bin / bridgecheck.sh`.

**#buscar-o / usr / bin / bridgecheck.sh **
http://files.pfsense.org/misc/bridgecheck.sh

Luego hay que hacer el script ejecutable ejecutando el siguiente comando.

#chmod + x / usr / bin / bridgecheck.sh

9.5.2.3.2. Programar la secuencia de comandos

Ahora tiene que programar la secuencia de comandos para ejecutar. Descargar una copia de seguridad de su configuración en el

Diagnóstico → Copia de seguridad / restauración de la pantalla. Abra la configuración en un editor de texto, y la búsqueda de

<cron>. Usted encontrará la sección de la configuración que contiene todas las tareas programadas que cron se ejecuta.

```
 <cron>
  <item>
   <minute> 0 </ min>
   <hora> * </ hora>
   <mday> * </ mday>
   <mes> * </ mes>
   <wday> * </ wday>
   <quién> raíz </ OMS>
   <command> / usr / bin / bonita-n20 newsyslog </ command>
  </ Item>
  <item>
   <minute> 1,31 </ minuto>
```

```
 <hora> 0-5 </ hora>
 <mday> * </ mday>
<mes> * </ mes>
 <wday> * </ wday>
 <quién> raíz </ OMS>
 <command> / usr / bin / bonita-n20 adjkerntz-a </ command>
</ Item>
```

Añadir bridgecheck.sh como una entrada de cron. Agregar el siguiente ejecutar el script cada minuto.

```
<item>
 * <minute> / 1 </ minuto>
 <hora> * </ hora>
 <mday> * </ mday>
 <mes> * </ mes>
 <wday> * </ wday>
 <quién> raíz </ OMS>
 <command> / usr / bin / bridgecheck.sh </ command>
</ Item>
```

Asegúrese de cambiar tanto la primaria y la secundaria.

9.5.2.3.3. Deshabilitar puente en el arranque

Usted desea agregar un comando para la configuración de abajo del puente en el arranque. Esto ayudar a prevenir la capa 2 bucles, como bridgecheck.sh va a instalar el maestro CARP de puente en 1 minuto. Por encima de la línea que dice `</ Sistema>`, Agregue la línea siguiente.

<shellcmd> / sbin / ifconfig bridge0 abajo </ shellcmd>

Guarde los cambios en los archivos de configuración. Ahora restaurar las configuraciones modificadas para tanto la primaria y la secundaria. Los cortafuegos se reiniciará después de restaurar la configuración, y cuando arranque una copia de seguridad que debería ser plenamente funcional.

9.5.2.4. DEVD Ganchos

Esta solución sólo es posible en pfSense 1.2.3 o posterior, y consiste en utilizar DEVD para coger el transición real del estado CARP como es el caso. Editar `/ Etc / devd.conf` en la copia de seguridad y maestro, y agregue estas líneas:

```
notificar a 100 {
            coinciden con "sistema" "IFNET";
```

```
            coinciden con "tipo" "LINK_UP";
            coinciden con "subsistema", "la carpa";
            acción "/ usr / local / bin / carpup";
};
notificar a 100 {
            coinciden con "sistema" "IFNET";
            coinciden con "tipo" "LINK_DOWN";
            coinciden con "subsistema", "la carpa";
            acción "/ usr / local / bin / carpdown";
};
```

A continuación, cree dos archivos nuevos: `/ Usr / local / bin / carpup`

```
#! / Bin / sh
/ Sbin / ifconfig bridge0 hasta
```

Y: `/ Usr / local / bin / carpdown`

```
#! / Bin / sh
/ Sbin / ifconfig bridge0 abajo
```

A continuación, realice los scripts ejecutables:

#chmod a + x / usr / local / bin / carpup
#chmod a + x / usr / local / bin / carpdown

Que automáticamente traerá el puente de arriba a abajo cada vez que se detecta un cambio de estado CARP.

9.5.2.5. Solución de problemas de conmutación por error puente

Si algo no está funcionando como se esperaba, compruebe el estado de → Interfaces de la página en ambos sistemas para revisar el `bridge0` interfaz, y la página de estado CARP para verificar maestro CARP o estado de copia de seguridad. Puede ejecutar bridgecheck.sh de la línea de comandos, así como la verificación de la interfaz estado usando ifconfig. La comprensión del sistema operativo subyacente FreeBSD puede ser necesario éxito solucionar cualquier problema con este tipo de implementación.

Muchos de los problemas con la carpa y el puente se levantará a partir de bucles interruptor y cuestiones STP. Ir más Sección 9.5.2, "CARP" otra vez, y también comprobar la configuración del interruptor para ver el estado del puerto para sus interfaces de puente. Si los puertos están bloqueando cuando deberían estar expedición, se le probablemente necesite ajustar la configuración de STP o emplear una de las técnicas alternativas para apagar un puente de copia de seguridad.

9.5.3. Multi-WAN

Puente, por su naturaleza es incompatible con multi-WAN en muchos de sus usos. Cuando se utiliza de transición,
común algo más que pfSense será la puerta de enlace predeterminada para los anfitriones en el puente
interfaz, y el router que es lo único que puede dirigir el tráfico de los anfitriones. Esto no
evitar que el uso de múltiples interfaces WAN con otros en el mismo servidor de seguridad que no son
puente, que sólo afecta a los anfitriones en las interfaces de un puente en el que usar algo que no sea
pfSense como su puerta de enlace predeterminada. Si puente de múltiples interfaces internas juntos y pfSense
es la puerta de enlace predeterminada para sus anfitriones en una interfaz de puente, entonces usted puede utilizar de múltiples WAN
mismo que con las interfaces no puenteado.

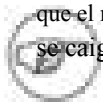
Capítulo 10. LAN virtuales (VLAN)

Las VLAN ofrecen un medio para segmentar un solo interruptor en dominios de difusión múltiple, permitiendo que un solo interruptor para funcionar lo mismo que varios switches. Esto se utiliza comúnmente para segmentación de la red de la misma manera que los interruptores múltiples podría ser utilizado, para colocar las máquinas de
un segmento específico tal como está configurada en el interruptor. Cuando se emplea trunking entre switches, dispositivos en el mismo segmento no es necesario residir en el mismo interruptor. Los conceptos, terminología y configuración de VLAN son tratados en este capítulo.

10.1. Requisitos

Hay dos requisitos, los cuales se deben cumplir para implementar las VLAN.

1. 802.1Q VLAN pueden cambiar - cada interruptor decente logrado fabricados desde alrededor de el año 2000 es compatible con 802.1Q VLAN trunking. No se puede utilizar con una VLAN no administrado interruptor.
2. Adaptador de red capaz de etiquetado VLAN - usted necesitará una tarjeta de red que soporta el hardware El etiquetado VLAN o cuenta con el apoyo del marco de largo. Debido a que cada marco tiene una etiqueta de 4 bytes agregó 802.1Q
   en la cabecera, el tamaño del marco puede ser de hasta 1522 bytes. Una tarjeta de red al hardware de soporte VLAN marcos de marcado o largo plazo es necesario porque otros adaptadores no funcionarán con los marcos más grandes que el máximo de bytes normal de 1518 con 1500 Ethernet MTU. Esto hará que grandes marcos se caigan, lo que provoca problemas de rendimiento y conexión de estancamiento.



Nota

El hecho de que un adaptador se muestra como contar con el apoyo del marco de largo no garantiza aplicación específica de su tarjeta de red de ese chipset soporta correctamente los marcos de largo. Realtek `rl (4)` NIC son los mayores infractores. Muchos no tendrán ningún problema, pero algunos no adecuadamente soporta frames de largo, y algunos no aceptará etiquetado 802.1Q
en todos los marcos. Si encuentra problemas al utilizar una de las NIC que figuran en soporte de la estructura de largo, tratando de una interfaz de hardware con soporte VLAN etiquetado es recomienda. No tenemos conocimiento de ningún problema similar con las NIC que figuran en VLAN soporte de hardware.

Interfaces Ethernet con soporte VLAN de hardware:

`AEC (4)`,`bge (4)`,`cxgb (4)`,`em (4)`,`ixgb (4)`,`msk (4)`,`ESN (4)`,`Re (4)`,`stge (4)`, `ti (4)`,`txp (4)`,`GVE (4)`.

interfaces Ethernet con soporte de la estructura de largo:

`bfe (4),CC (4),fxp (4),gema (4),hme (4),-le (4),educación no formal (4),NVE (4),rl (4),`
`sis (4),sk (4),ste (4),tl (4),tx (4),vr (4),xl (4)`

10.2. Terminología

Esta sección cubre la terminología que necesitará entender para implementar con éxito las VLAN.

10.2.1. Trunking

Trunking se refiere a un medio de cumplir con varias VLAN en el puerto mismo interruptor. Los marcos dejando a un puerto troncal están marcados con una etiqueta 802.1Q en la cabecera, permitiendo que la relacionada dispositivo para diferenciar entre varias VLAN. puertos troncales se utilizan para conectar múltiples interruptores, y para conectar todos los dispositivos que son capaces de etiquetado 802.1Q y requieren el acceso a múltiples VLANs. Esto comúnmente se limita sólo a la conectividad entre el router proporciona las VLAN, en este caso, pfSense, así como las conexiones con otros switches que contiene Varias VLAN.

10.2.2. VLAN ID

Cada VLAN tiene un identificador asociado a él que se utiliza para la identificación del tráfico agregó. Se trata de un número entre 1 y 4094. La VLAN por defecto en los switches es la VLAN 1, y debe esta VLAN No se utilizará al implementar VLAN trunking. Esto se discute más en Sección 10.3, "VLAN y la seguridad ". Además de evitar el uso de la VLAN 1, puede elegir qué números de las VLAN que desea utilizar. Algunos se iniciará con la VLAN 2 y el incremento por uno hasta el número requerido de VLAN que se llegó. Otra práctica común es usar el tercer octeto de la subred IP de la VLAN como el ID de VLAN. Por ejemplo, si utiliza 10.0.10.0/24, 10.0.20.0/24 y 10.0.30.0/24, es lógico utilizar VLAN 10, 20 y 30 respectivamente. Elegir un esquema de asignación de VLAN ID que tenga sentido para usted.

10.2.3. Padres interfaz

La interfaz principal se refiere a la interfaz física en la VLAN de residencia, tales como `Em0` o `bge0`. Al configurar redes VLAN en pfSense o FreeBSD, cada uno se le asigna una interfaz virtual, comenzando con `vlan0` e incrementar en uno por cada VLAN adicional configurado. En pfSense 1.2.x, el número de la interfaz VLAN no tiene correlación con el ID de VLAN. Usted no debe asignar la interfaz de los padres a cualquier interfaz de pfSense - su única función debe ser como el los padres de las VLAN definida. En algunas situaciones esto funcionará, pero puede causar dificultades

con la configuración de interruptor, puede causar problemas con el uso de Portal Cautivo, y te obliga a usar VLAN del puerto por defecto del tronco, que deben evitarse como se analiza en Sección 10.3, "VLAN y la seguridad".

10.2.4. Acceso al puerto

Un puerto de acceso se refiere a un puerto del conmutador de acceso a una sola VLAN, donde los marcos son no etiquetados con una cabecera 802.1Q. Se conecta todos los dispositivos que residen en una sola VLAN a un acceso al puerto. La mayoría de los puertos switch se configura como puertos de acceso. Los dispositivos de acceso los puertos no son conscientes de que ninguna de las VLAN en la red. Ellos ven cada VLAN los mismos que se un interruptor sin VLAN.

10.2.5. Doble etiquetado (QinQ)

También es posible duplicar el tráfico de etiquetas, usando una etiqueta 802.1Q exterior e interior. Esto se conoce como QinQ. Esto puede ser útil en grandes entornos ISP y algunas otras redes muy grandes. Triple etiquetado también es posible. pfSense no admite QinQ en este momento, pero en 2.0. Estos tipos de ambientes generalmente necesitan el tipo de enrutamiento de poder que sólo un router de gama alta basados en ASIC puede soportar, y QinQ agrega un nivel de complejidad que no es necesaria en la mayoría de entornos.

10.2.6. VLAN privada (PVLAN)

PVLAN se refiere a las capacidades de algunos interruptores de los ejércitos segmento dentro de una sola VLAN. Normalmente los hosts dentro de una VLAN solo funcionan igual que las máquinas de un solo interruptor sin VLAN configurado. PVLAN proporciona un medio para la prevención de los ejércitos en una VLAN de hablar con cualquier otro equipo en esa VLAN, sólo permite la comunicación entre el anfitrión y su valor predeterminado puerta de enlace. Esto no guarda relación directa con pfSense, pero es una pregunta común usuarios. Switch funcionalidad de este tipo es la única manera de impedir la comunicación entre hosts en el mismo subred. Sin una función como PVLAN, sin firewall de la red puede controlar el tráfico dentro de una subred porque nunca toca la puerta de enlace predeterminada.

10.3. VLANs y seguridad

Las VLAN ofrecen un gran medio para segmentar la red y aislar subredes, pero hay algunas problemas de seguridad que deben tenerse en cuenta al diseñar e implementar una solución participación de las VLAN. VLAN no son inherentemente inseguro, pero puede salir de una mala configuración de su red vulnerables. También ha habido problemas de seguridad en las implementaciones de proveedores de conmutadores ' de VLAN en el pasado.

10.3.1. Segregar las zonas Fiduciario

Debido a la posibilidad de una mala configuración, usted debe separar las redes de forma considerable diferentes niveles confianza en sus propios conmutadores físicos. Por ejemplo, mientras que técnicamente podría utilizar el mismo interruptor con VLAN para todas sus redes internas, así como la red exterior los servidores de seguridad, que debe ser evitado como una mala configuración del interruptor podría dar lugar a el tráfico de Internet sin filtro entren en su red interna. Como mínimo, usted debe utilizar dos interruptores en tales escenarios, uno para fuera del firewall y dentro de uno. En muchos entornos, segmentos de DMZ también son tratados por separado, en un tercer interruptor, además de la WAN y LAN interruptores. En otros, la WAN está en su propio interruptor, mientras que todas las redes de detrás del firewall están en los mismos modificadores utilizando VLAN. ¿Qué escenario es el más apropiado para su red depende de sus circunstancias específicas, y el nivel de riesgo y la paranoia.

10.3.2. Usando el valor por defecto VLAN1

Debido a la VLAN1 es el valor predeterminado, o "nativos", VLAN, puede ser utilizado de manera inesperada por la interruptor. Es similar al uso de un defecto permitir que la política sobre las reglas del cortafuegos por defecto en lugar de negar
y seleccionar lo que usted necesita. Siempre es mejor usar una VLAN diferente, y asegurarse de que sólo selecciona los puertos que desea en su grupo de pasar a estar en esa VLAN, para limitar el acceso mejor. Interruptores enviará protocolos internos como STP (Spanning Tree Protocol), VTP (VLAN Trunking Protocol), y CDP (Cisco Descubre Protocolo) sin etiquetar en la VLAN nativa, donde los interruptores utilizar estos protocolos. Por lo general, la mejor manera de mantener ese tráfico interno aislado de sus datos de tráfico.

Si tiene que usar VLAN1, debe tener mucho cuidado al asignar a cada puerto único en cada interruptor una VLAN diferente, excepto aquellos que desee en VLAN1, y no crear una interfaz de gestión para el cambio en VLAN1. También debe cambiar la VLAN nativa del grupo de cambiar a un diferentes, VLAN no utilizada. Algunos interruptores no puede apoyar ninguna de estas soluciones, por lo que es normalmente más fáciles de mover los datos a una VLAN diferente, en lugar de quejarse con la fabricación de VLAN1 disponible. Con la identificación de VLAN del 2 al 4094 para elegir, sin duda es mejor ignorar VLAN1 la hora de diseñar su esquema de VLAN.

10.3.3. Uso de un puerto troncal VLAN por defecto

Cuando el tráfico de VLAN etiquetado se envían a través de un tronco en la VLAN nativa, las etiquetas en los paquetes que
coincide con la VLAN nativa puede ser despojado por el interruptor para mantener la compatibilidad con mayores redes. Peor aún, los paquetes que son el doble etiquetado con la VLAN nativa y una VLAN diferente sólo tienen la etiqueta de VLAN nativa quita cuando canalización de esta manera y cuando se procesan después, que el tráfico puede terminar en una VLAN diferente. Esto también se llama "salto de VLAN".

Como se menciona en la sección anterior, el tráfico sin etiqueta en un puerto troncal se supone que la VLAN nativa, lo que también podría coincidir con una interfaz VLAN asignado. Dependiendo de cómo el interruptor controla el tráfico tal y como es visto por pfSense, mediante la interfaz directa podría dar lugar a dos interfaces de estar en la misma VLAN.

10.3.4. La limitación del acceso a los puertos del tronco

Debido a un puerto troncal puede hablar con cualquier VLAN en un grupo de conmutadores troncales, posiblemente,

incluso los

no está presente en el interruptor de corriente en función de las configuraciones de su conmutador, es importante fisicamente puertos troncales seguro. También asegúrese de que no hay puertos configurados para trunking que se deja desconectado donde gancho alguien puede en una sola, accidentalmente o de otra manera. Dependiendo en el conmutador, se puede apoyar la negociación dinámica de concentración de enlaces. Usted debe garantizar este funcionalidad está deshabilitada o restringida correctamente.

10.3.5. Otros problemas con los interruptores

Ha habido informes de que algunos interruptores basados en VLAN se escapará tráfico a través de las redes VLAN cuando sean objeto de cargas pesadas, o si una dirección MAC de un PC en una VLAN se ve en otro VLAN. Estos problemas tienden a ser mayores en los interruptores con firmware anticuado o muy bajos calidad de switches gestionados. Este tipo de cuestiones se han resuelto en gran medida hace muchos años, cuando este tipo de problemas de seguridad eran comunes. No importa lo que cambiar de marca lo que tiene, no algunas investigaciones en línea para ver si ha sido sometido a ningún tipo de pruebas de seguridad, y asegurarse de que se con el firmware más reciente. Si bien estas cuestiones son un problema con el interruptor, y no pfSense, que son parte de su seguridad general.
Muchas de las cosas aquí son específicos de marcas y modelos de interruptores. No puede ser diferentes consideraciones de seguridad específicas para el interruptor que está utilizando. Consulte su documentación para las recomendaciones de la VLAN de seguridad.

10.4. pfSense configuración

Esta sección cubre la configuración de VLAN en el lado pfSense.

10.4.1. Consola de configuración de VLAN

Puede configurar redes VLAN en la consola usando la función de Asignación de interfaces. Los siguientes ejemplo muestra cómo configurar dos VLAN, ID 10 y 20, con `le2` como la interfaz principal. Las interfaces VLAN se asignan como OPT1 y OPT2.

```
 pfSense configuración de la consola
**********************
```

```
 0) Cerrar sesión SSH (solamente)
 1) Asignar interfaces
 2) Establecer la dirección IP LAN
 3) Reiniciar contraseña webConfigurator
 4) Restablecer los valores predeterminados de fábrica
 5) Reiniciar el sistema
 6) Sistema de Parada
 7) Ping acogida
 8) Shell
 9) PFtop
10) Filtro de Registros
11) Reiniciar webConfigurator
12) pfSense desarrolladores Shell
13) Actualización de la consola
14) Desactivar Secure Shell (sshd)
98) Mover el archivo de configuración de dispositivo extraíble

Ingrese una opción: 1

interfaces válidos son:

le0 00:0 c: 29: d6: e7: CC (hasta)
le1 00:0 c: 29: d6: e7: e6 (hasta)
Le2 00:0 c: 29: d6: e7: f0 (hasta)
plip0 0

¿Quieres crear VLANs por primera vez?
Si no se va a utilizar VLAN, o sólo para interfaces opcionales, debe
dicen que no aquí y utilizar el webConfigurator para configurar redes VLAN después,
si es necesario.

¿Quieres crear VLANs ahora [y | n]? y

Capaz interfaces VLAN:

le0 00:0 c: 29: d6: e7: CC (hasta)
le1 00:0 c: 29: d6: e7: e6 (hasta)
Le2 00:0 c: 29: d6: e7: f0 (hasta)

Escriba el nombre de la interfaz principal para la nueva VLAN (o nada si ha
terminado):
Introduzca la etiqueta de VLAN (1 a 4094): 10
```

```
Capaz interfaces VLAN:

le0 00:0 c: 29: d6: e7: CC (hasta)
le1 00:0 c: 29: d6: e7: e6 (hasta)
Le2 00:0 c: 29: d6: e7: f0 (hasta)

Escriba el nombre de la interfaz principal para la nueva VLAN (o nada si ha
terminado):
Introduzca la etiqueta de VLAN (1 a 4094): 20

Capaz interfaces VLAN:

le0 00:0 c: 29: d6: e7: CC (hasta)
le1 00:0 c: 29: d6: e7: e6 (hasta)
Le2 00:0 c: 29: d6: e7: f0 (hasta)

Escriba el nombre de la interfaz principal para la nueva VLAN (o nada si ha
terminado):


VLAN interfaces:

vlan0 etiquetas VLAN 10, la interfaz le2
vlan1 etiquetas VLAN 20, la interfaz le2

Si usted no sabe los nombres de las interfaces, puede optar por utilizar
auto-detección. En ese caso, desconecte todos los interfaces de ahora,
antes de
golpear "a" para iniciar la detección automática.

Escriba el nombre de la interfaz LAN o 'a' para la detección automática: le1

Escriba el nombre de la interfaz WAN o 'a' para la detección automática: le0

Escriba el nombre de la interfaz opcional 1 o 'a' para la detección
automática
(O nada si acabados): vlan0

Escriba el nombre de la interfaz opcional de 2 o 'a' para la detección
automática
(O nada si acabados): vlan1

Escriba el nombre de la interfaz opcional de 3 o 'a' para la detección
automática
(O nada si acabados): <enter>

Las interfaces serán asignados de la siguiente manera:
```

```
LAN -> le1
WAN -> le0
OPT1 -> vlan0
OPT2 -> vlan1

¿Desea continuar [y | n]? y

Un momento mientras recarga la configuración de ...
```

Después de unos segundos, la configuración volverá a cargar y se le devuelve al menú de la consola. Al configurar las interfaces VLAN en la consola, no le advierten sobre el reinicio de que puede ser necesaria antes de VLAN funcionará. Algunos adaptadores de red o los controladores no funcionan correctamente con VLAN hasta que se reinicie el sistema. Esto no siempre es necesario, pero no hemos sido capaz de encontrar la forma de detectar cuando se necesiten. Para estar en el lado seguro, reiniciar después de que su configuración VLAN inicial se recomienda. Para adiciones VLAN VLAN futuro una vez que se ya está configurado, un reinicio no es necesario.

10.4.2. interfaz web de configuración de VLAN

Examinar a las interfaces → Asignar. Figura 10.1, "Interfaces: Asignar" muestra el sistema utilizado para este ejemplo. WAN y LAN se asignan como `le0` y `le1` , respectivamente. También hay un `le2` interfaz que se utiliza como la interfaz principal de VLAN.

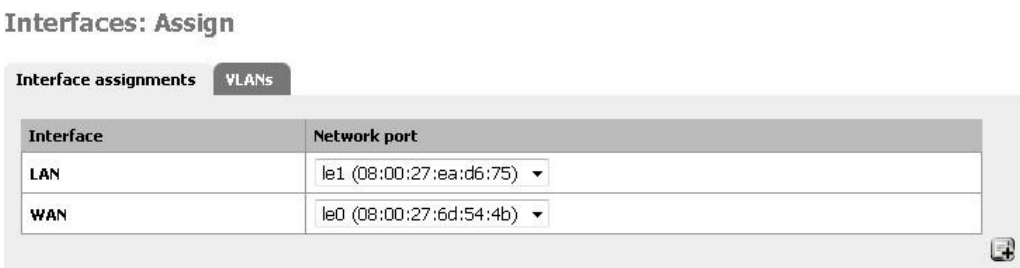


Figura 10.1. Interfaces: Asignar

Haga clic en la ficha VLAN. A continuación, haga clic aquí para agregar una nueva VLAN, como se muestra en Figura 10.2, "Lista de VLAN".

Figura 10.2. Lista de

VLAN

La pantalla de edición de VLAN ahora se muestra, como Figura 10.3, "Edición de VLAN". A partir de aquí, elegir una interfaz de Padres, **le2**. A continuación, introduzca una etiqueta de VLAN, **10**, Y escriba una descripción, como lo

Firewall: VLAN: Edit

red está en esa VLAN (DMZ, bases de datos, pruebas, etc.)

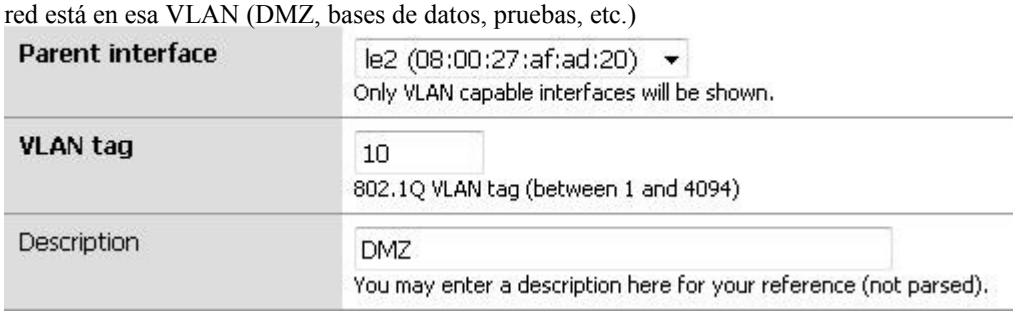


Figura 10.3. Editar VLAN

Una vez que se hace clic en Guardar, volverá a la lista de las VLAN disponibles, que ahora debe incluir el recién agregado VLAN 10. Repita este proceso para agregar VLAN adicionales, tales como VLAN 20. Estos pueden verse en Figura 10.4, "Lista de VLAN"

Interfaces: VLAN

Figura 10.4. Lista de VLAN

Ahora, para asignar la VLAN a las interfaces, haga clic en la ficha Interfaz de misiones, a continuación, haga clic en, y
en la lista desplegable de las asignaciones de interfaz disponibles, debería ver la nueva VLAN. Por
OPT1, escoja la interfaz con el ID de VLAN 10. Haga clic de nuevo, y para OPT2, escoja la interfaz
con el ID de VLAN 20. Cuando haya terminado, que se verá algo así como Figura 10.5, "Interfaz lista con VLAN".

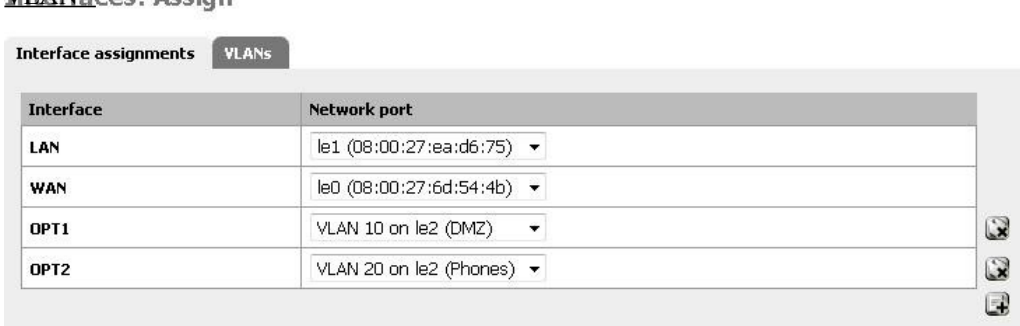


Figura 10.5. Interfaz lista con VLAN

Las interfaces VLAN basada en OPT-se comportan como las interfaces OPT hacen otros, lo que significa
Se deben activar, configurar reglas de firewall añadido, y servicios como el servidor de DHCP necesitará
para configurar si es necesario. Ver Sección 4.3.4, "Interfaces opcionales" Para obtener más información sobre
configurar las interfaces opcionales.

10.5. Interruptor de configuración

En esta sección se proporciona orientación sobre la configuración de su conmutador. Esto ofrece una guía genérica que se aplican a la mayoría si no todos los interruptores capaces 802.1Q, luego pasa a la cubierta de configuración en interruptores específicos de Cisco, HP, Netgear, y Dell. Nota: esta es la configuración de mínimo
Ud. va a necesitar para VLANs para funcionar, y no necesariamente el interruptor de seguridad ideal
configuración para su entorno. Una discusión a fondo de la seguridad interruptor está fuera de la
alcance de este libro.

10.5.1. Interruptor general sobre la configuración

En general, usted tendrá que configurar tres o cuatro cosas en VLAN interruptores capaces.

1. Agregar o definir la VLAN - la mayoría de interruptores de tener un medio de VLANs añadir, y que se debe
   agregó antes de que se pueden configurar en cualquier puerto.

2. Configure el puerto troncal - configurar el puerto de pfSense se conectará a un puerto troncal, etiquetado de todas sus redes VLAN en la interfaz.

3. Configurar los puertos de acceso - configurar los puertos de su servidor interno va a utilizar como el acceso puertos de la VLAN que desee, con VLAN sin etiqueta.

4. Configurar el puerto de VLAN ID (PVID) - algunas de las opciones necesitan configurar el PVID para un puerto. Esto especifica que la VLAN a utilizar para el tráfico que entra en ese puerto del switch. Para algunos interruptores se trata de un proceso de paso, configurando el puerto como un puerto de acceso en un determinado VLAN, automáticamente el tráfico que viene en las etiquetas en ese puerto. Otros interruptores que necesita para configurar esto en dos lugares. Consulte la documentación del conmutador para obtener más información si no es un se detallan en este capítulo.

10.5.2. Cisco IOS interruptores basados en

Configuración y uso de las VLAN en los switches de Cisco con IOS es un proceso bastante sencillo, teniendo sólo unos pocos comandos para crear y utilizar VLANs, puertos troncales y la asignación de puertos a las VLAN. Muchos interruptores de otros fabricantes se comportan de manera similar a IOS, y utilizará si no casi la misma sintaxis idéntica para la configuración.

10.5.2.1. Crear VLAN

Las VLAN se pueden crear de manera independiente, o el uso de VLAN Trunk Protocol (VTP). Uso de VTP puede ser más conveniente, ya que se propagan automáticamente la configuración de VLAN a todos los interruptores en un dominio VTP, aunque también puede crear sus propios problemas de seguridad y abrir posibilidades de inadvertidamente acabando con la configuración de VLAN. Con VTP, si usted decide necesidad de otra VLAN sólo necesita añadirse a un solo interruptor, y luego todos los interruptores de concentración de enlaces otros
en el grupo puede asignar los puertos a la VLAN. Si VLAN se configuran de forma independiente, debe añadir a cada interruptor con la mano. Consulte la documentación de Cisco en VTP para asegurarse de tener una configuración segura que no son propensas a la destrucción accidental. En una red con sólo unos interruptores donde las VLAN no cambian con frecuencia, suelen ser mejor no usar VTP para evitar su caídas potenciales.

10.5.2.1.1. Independiente de las VLAN

Para crear VLANs independiente:

```
sw # vlan base de datos
sw (vlan) # vlan 10 nombre "Servidores DMZ"
sw (vlan) # vlan 20 nombre "Móviles"
```

```
sw (vlan) # salida
```

10.5.2.1.2. VTP VLAN

Para configurar el switch para VTP y las VLAN, crear una base de datos VTP en el interruptor principal y, a continuación crear dos VLAN:

```
sw # vlan base de datos
sw (vlan) # VTP servidor
sw (vlan) # vtp de dominio example.com
sw (vlan) # vtp contraseña SuperSecret
sw (vlan) # vlan 10 nombre "Servidores DMZ"
sw (vlan) # vlan 20 nombre "Móviles"
sw (vlan) # salida
```

10.5.2.2. Configurar puerto troncal

Para pfSense, un puerto del conmutador no sólo tiene que estar en modo de tronco, pero también debe utilizar 802.1q etiquetado. Esto se puede hacer así:

```
sw # configure terminal
sw (config) # La interfaz FastEthernet0 / 24
sw (config-if) # switchport tronco de modo de
sw (config-if) # switchport dot1q tronco encapsulación
```

Nota

En algunos nuevos conmutadores de Cisco IOS, el Cisco-propietario de ISL VLAN método de encapsulación es obsoleto y ya no es soportada. Si el interruptor se No permita que el **dot1q encapsulación** opción de configuración, sólo es compatible con 802.1Q y usted no necesita preocuparse acerca de cómo especificar la encapsulación.

10.5.2.3. Agregar puertos a la VLAN

Para añadir puertos a estas redes VLAN, es necesario para asignar de la siguiente manera:

```
sw # configure terminal
sw (config) # La interfaz FastEthernet0 / 12
sw (config-if) # switchport acceder al modo
sw (config-if) # switchport access vlan 10
```

10.5.3. Cisco basado en interruptores CatOS

La creación de VLAN en CatOS es un poco diferente, aunque la terminología es la misma que utiliza VLAN en IOS. Aún dispone de la opción de utilizar independiente o VTP VLAN o para mantener la base de datos de VLAN:

#conjunto de dominio VTP ejemplo el modo de servidor
#conjunto vtp passwd *SuperSecret*
#conjunto vlan *10* nombre *DMZ*
#conjunto vlan *20* nombre *teléfonos*

Y configurar un puerto troncal para manejar de forma automática cada VLAN:

#conjunto del tronco *5 / 24* en dot1q 1-4094

A continuación, agregue los puertos a la VLAN:

#conjunto vlan *10 5/1-8*
#conjunto vlan *20 5/9-15*

10.5.4. HP ProCurve interruptores

HP ProCurve cambia sólo el apoyo de trunking 802.1q, por lo que no cuenta es necesario allí. En primer lugar, telnet en el interruptor y hacer aparecer el menú de gestión.

10.5.4.1. Habilitar el soporte VLAN

En primer lugar, soporte VLAN debe estar habilitado en el interruptor, si no lo está ya.

1. Elija la configuración del interruptor
2. Elija las funciones avanzadas
3. Elija Menú VLAN ...
4. Elija Apoyo VLAN
5. Establecer redes VLAN Habilitar a Sí, si no está ya, y elegir un número de VLAN. Cada vez que este valor se cambia el interruptor debe ser reiniciado, así que asegúrese de que es lo suficientemente grande como para apoyar VLAN como usted imaginar que necesitan.
6. Reinicie el interruptor para aplicar los cambios.

10.5.4.2. Crear VLAN

Antes de la VLAN se puede asignar a los puertos, es necesario crear las VLAN. En el interruptor configuración del menú:

1. Elija la configuración del interruptor
2. Elija las funciones avanzadas
3. Elija Menú VLAN ...
4. Elegir los nombres de VLAN
5. Elija Agregar
6. Introduzca el ID de VLAN, ***10***
7. Escriba el nombre, ***LAN***
8. Seleccione Guardar
9. Repita los pasos de Añadir a Guardar para cualquier VLAN restantes

10.5.4.3. Asignación de puertos a las VLAN Trunk

A continuación, configure el puerto troncal para el servidor de seguridad, así como los puertos tronco va a otros conmutadores
contiene varias VLAN.

1. Elija la configuración del interruptor
2. Elija Menú VLAN ...
3. Elija asignación de VLAN de puerto
4. Elija Edición
5. Encuentra el puerto que desea asignar
6. Espacio prensa en la VLAN por defecto hasta que dice no
7. Hazte a un lado de la columna para cada una de las VLAN en este puerto del tronco, y el espacio de prensa hasta que dice la etiqueta. Cada VLAN en uso deben ser marcados en el puerto troncal.

10.5.4.4. Asignación de puertos de acceso a las VLAN

1. Elija la configuración del interruptor

2. Elija Menú VLAN ...

3. Elija asignación de VLAN de puerto

4. Elija Edición

5. Encuentra el puerto que desea asignar

6. Espacio prensa en la VLAN por defecto hasta que dice no

7. Hazte a un lado de la columna de la VLAN a la que este puerto se le asignará

8. Espacio prensa hasta que se dice sin etiquetar.

10.5.5. Netgear switches gestionados

Este ejemplo está en el buen GS108T, pero otros modelos de Netgear hemos visto son muy similares, si no idénticos. Hay también varios otros proveedores incluyendo Zyxel que venden conmutadores realizados por el mismo fabricante, utilizando la misma interfaz web con un logotipo diferente. Acceda a su conmutador interfaz web para empezar.

10.5.5.1. Planificación de la configuración de VLAN

Antes de configurar el interruptor, lo que necesita saber cómo las VLAN que usted va a configurar, lo que ID que va a utilizar, y cómo cada puerto del switch debe ser configurado. Para este ejemplo, estamos utilizando un GS108T puerto 8, y será la configuración como se muestra en Tabla 10.1, "GS108T Netgear Configuración de VLAN ".

Puerto del switch	El modo de VLAN	VLAN asignado
1	tronco	*10* y *20*, Agregó
2	el acceso	*10* sin etiquetar
3	el acceso	*10* sin etiquetar
4	el acceso	*10* sin etiquetar
5	el acceso	*20* sin etiquetar
6	el acceso	*20* sin etiquetar
7	el acceso	*20* sin etiquetar
8	el acceso	*20* sin etiquetar

Tabla 10.1. GS108T Netgear configuración VLAN

10.5.5.2. Habilitar 802.1Q VLAN

En el menú del sistema en el lado izquierdo de la página, haga clic en Configuración del grupo de VLAN, como se indica en Figura 10.6, "Grupo de VLAN Marco".

Figura 10.6. VLAN Grupo Marco

Seleccione IEEE 802.1Q VLAN (Figura 10.7, "Habilitar 802.1Q VLAN").

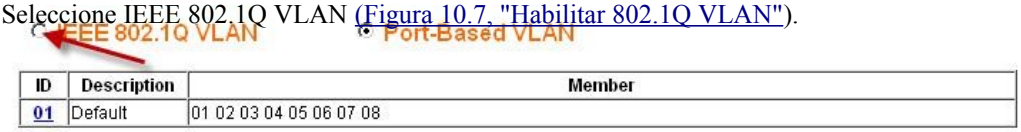


Figura 10.7. Habilitar 802.1Q VLAN

Le avisará con un pop-up preguntando si realmente quieres cambiar, y la lista de algunos de las consecuencias, como se muestra en Figura 10.8, "El cambio de confirmación para 802.1Q VLAN". Si desea VLAN, ahora debe usar 802.1Q. Haga clic en Aceptar.

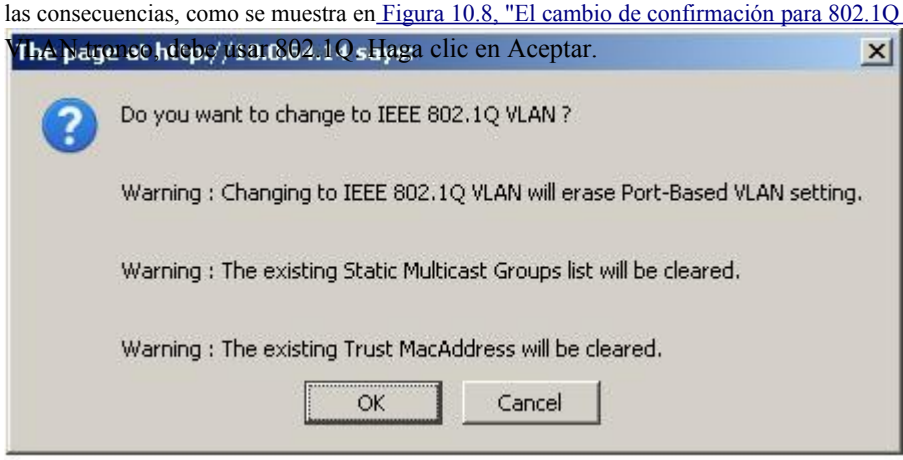


Figura 10.8. Confirmar el cambio de 802.1Q VLAN

Después de hacer clic en Aceptar, la página se actualizará con la configuración de VLAN 802.1Q, como se muestra en
Figura 10.9, "Configuración por defecto 802.1Q".

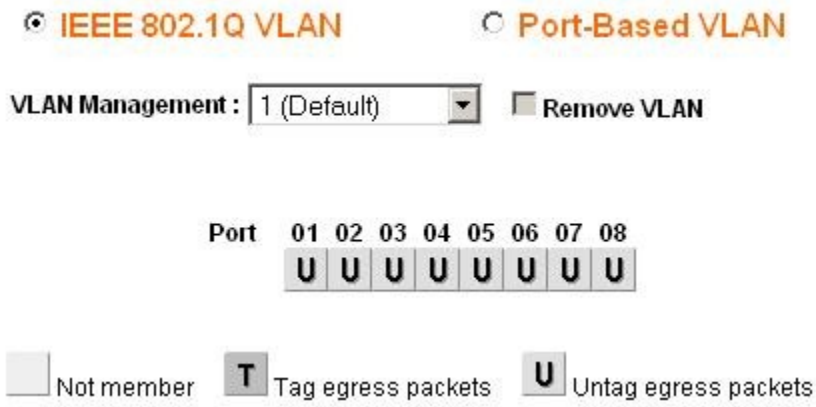


Figura 10.9. Configuración por defecto 802.1Q

10.5.5.3. Añadir VLAN

Para este ejemplo, voy a añadir dos VLAN con ID *10* y *20*. Para agregar una VLAN, haga clic en la VLAN Gestión desplegable y haga clic en Agregar nueva VLAN como se muestra en Figura 10.10, "Añadir nueva VLAN".

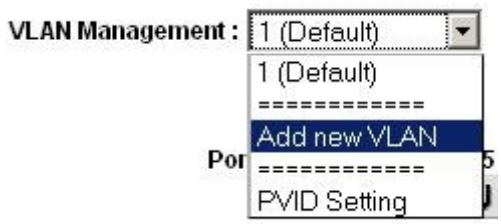


Figura 10.10. Añadir nueva VLAN

Introduzca el ID de VLAN para esta nueva VLAN, a continuación, haga clic en Aplicar. La pantalla de VLAN ahora te dejaré
configurar VLAN *10* (Figura 10.11, "Añadir VLAN 10"). Antes de configurar, yo de nuevo, haga clic en Añadir nueva VLAN como se muestra en Figura 10.10, "Añadir nueva VLAN" para agregar VLAN *20* (Figura 10.12, "Añadir VLAN 20").

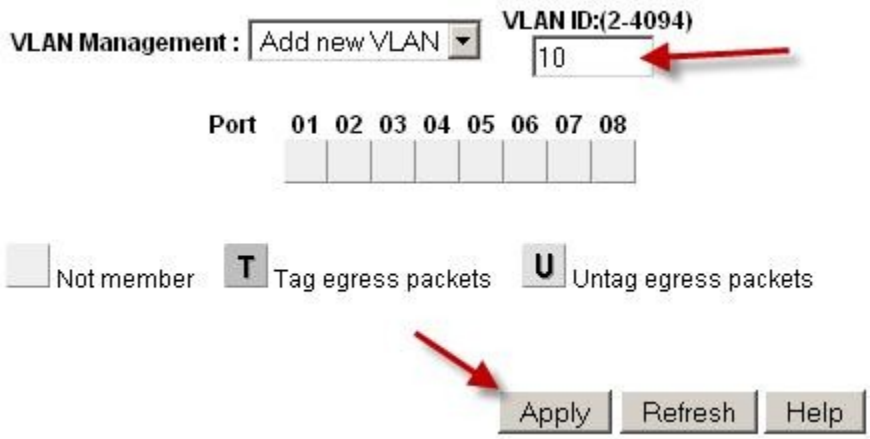


Figura 10.11. Agregar la VLAN 10

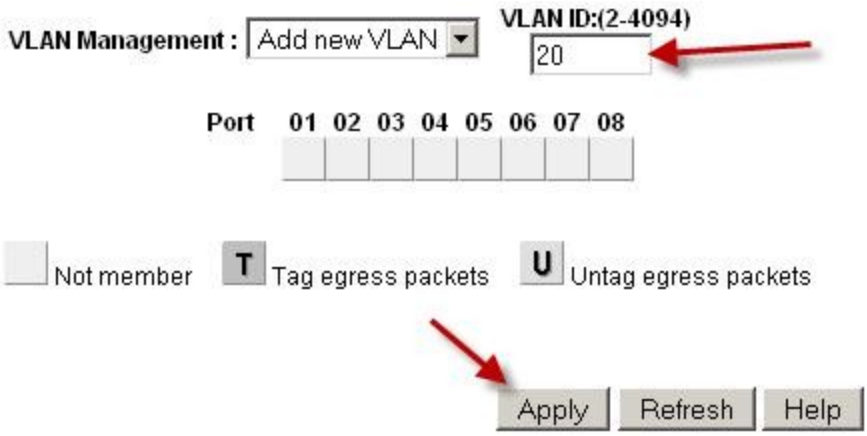


Figura 10.12. Añadir VLAN 20

Añadir como VLAN que sea necesario, y luego continuar a la siguiente sección.

10.5.5.4. Configurar el etiquetado VLAN

Cuando se selecciona una VLAN del menú desplegable de la VLAN de administración hacia abajo, que le muestra la forma en que

VLAN se configura en cada puerto. Un cuadro en blanco indica que el puerto no es miembro del seleccionado

VLAN. Una caja que contiene **T** mediante la VLAN se envía en ese puerto con la etiqueta 802.1Q. **U** indica el puerto es un miembro de esa VLAN y deja el puerto sin etiquetar. El puerto troncal tendrá que han añadido dos VLAN y etiquetados.

Nota

No cambie la configuración del puerto que está utilizando para acceder al interruptor de interfaz web. Usted mismo bloqueo, con el único medio de recuperación en la GS108T está golpeando el restablecimiento de fábrica de botones por defecto - no tiene consola serie. Para los interruptores que tiene de serie consolas, tiene un cable de módem nulo útil en caso de que desconectarse de la conectividad de red con el interruptor. Configuración de la VLAN de administración se describe más adelante en esta sección.

Haga clic en las casillas bajo el número de puerto como se muestra en Figura 10.13, "Activar VLAN miembros " para alternar entre las tres opciones de VLAN.

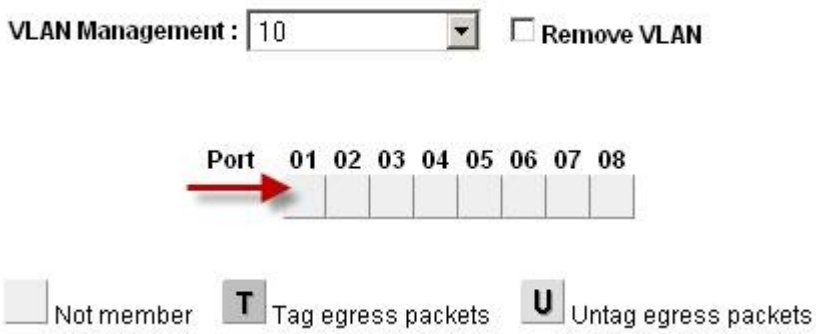


Figura 10.13. Activar pertenencia a la VLAN

10.5.5.4.1. Configurar la VLAN 10 miembros

Figura 10.14, "Configuración de la VLAN 10 miembros" muestra VLAN *10* configurado como se indica en Tabla 10.1, "Configuración de VLAN Netgear GS108T". Los puertos de acceso en esta VLAN se establecen en sin etiqueta, mientras que el puerto troncal se establece agregó.

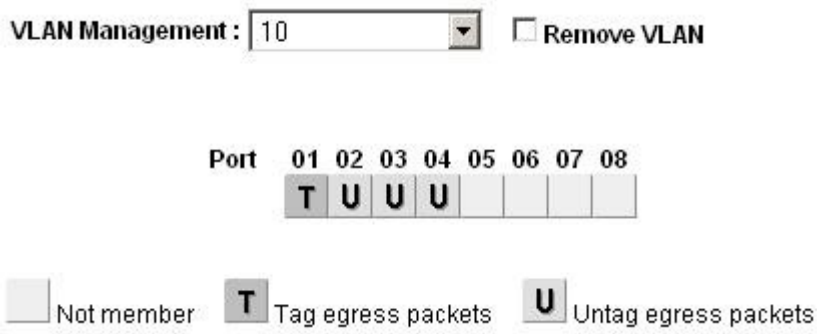


Figura 10.14. Configurar la VLAN 10 miembros

10.5.5.4.2. Configuración de VLAN 20 miembros

Seleccione *20* de la VLAN de administración desplegable para configurar los miembros en el puerto de VLAN *20*.

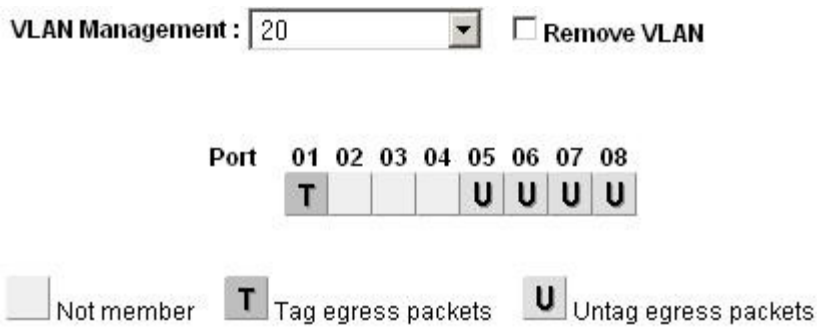


Figura 10.15. Configuración de VLAN 20 miembros

10.5.5.4.3. Cambio PVID

En los switches de Netgear, además de la configuración configurado previamente marcado, también debe configurar el PVID para especificar la VLAN utiliza para los marcos de entrar en ese puerto. En la VLAN Gestión desplegable, haga clic en PVID Marco como se muestra en Figura 10.16, "PVID Marco".

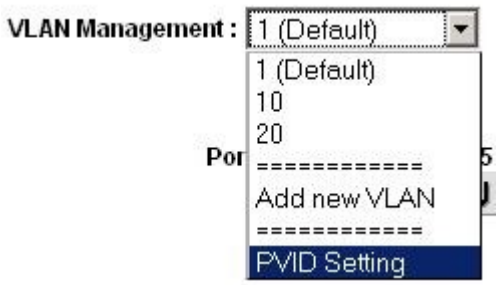


Figura 10.16. PVID Marco

El valor predeterminado PVID configuración es la VLAN 1 para todos los puertos como se muestra en Figura 10.17, "PVID por defecto Configuración."

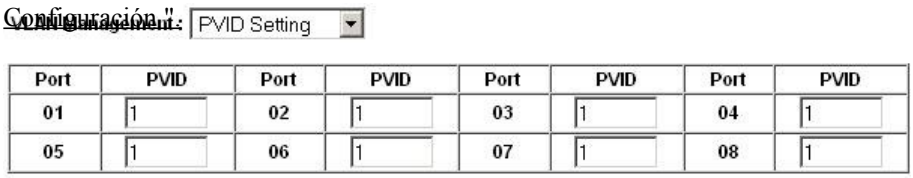


Figura 10.17. Configuración por defecto PVID

Cambiar el PVID para cada puerto de acceso, pero abandonar el puerto del tronco y el puerto que está utilizando acceder a la interfaz de administración del conmutador establece **1**.Figura 10.18, "VLAN 10 y 20 PVID de configuración " muestra la configuración PVID juego las asignaciones de puerto se muestra en la Tabla 10.1, "GS108T Netgear configuración VLAN", Con 8 puertos se utilizan para acceder a la cambiar la interfaz de gestión. Aplica los cambios cuando haya terminado.

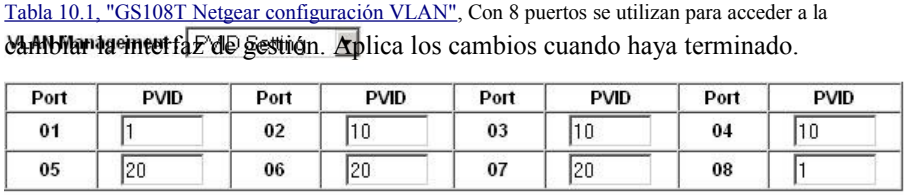


Figura 10.18. VLAN 10 y 20 de configuración PVID

10.5.5.4.4. Quite la configuración de VLAN 1

Por defecto, todos los puertos son miembros de una VLAN con marcos de salida sin etiquetar. Seleccione **1 (Por defecto)** desde la caída de la VLAN de administración hacia abajo. Eliminar una VLAN de todos los puertos excepto el que usted está utilizando para gestionar el switch y el puerto de tronco, por lo que no se desconecta. I estoy usando el puerto de 8 a gestionar el switch. Cuando haya terminado, la pantalla debe ser similar a Figura 10.19, "Eliminar la pertenencia a VLAN 1".

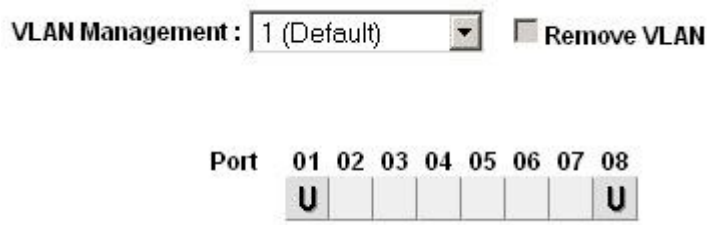


Figura 10.19. Retire pertenencia a la VLAN 1

Aplica los cambios cuando haya terminado.

10.5.5.4.5. Verificar la funcionalidad VLAN

Configure su VLAN en pfSense, incluyendo el servidor DHCP en la VLAN de interfaces si se utiliza DHCP. Conecte los sistemas en los puertos de acceso configurado y la conectividad de la prueba. Si todo funciona como se desea, continúe con el siguiente paso. Si las cosas no funcionan como se esperaba, la revisión el etiquetado y la configuración PVID en el interruptor, y la configuración de VLAN y la interfaz asignaciones en pfSense.

10.5.6. Dell PowerConnect switches gestionados

La interfaz de gestión de conmutadores de Dell varía ligeramente entre los modelos, pero los siguientes procedimiento tendrá en cuenta la mayoría de modelos. La configuración es muy similar en estilo a Cisco IOS.

En primer lugar, crear las VLAN:

```
consola # config
consola (config) # vlan base de datos
consola (config-vlan) # vlan 10 nombre DMZ los medios de comunicación Ethernet
consola (config-vlan) # vlan 20 nombre teléfonos los medios de comunicación Ethernet
consola (config-vlan) # salida
```

A continuación, configurar

un puerto troncal:

```
consola (config) # Interfaz Ethernet 1 / 1
consola (config-if) # switchport tronco de modo de
consola (config-if) # switchport VLAN permite añadir 1-4094 etiquetado
consola (config-if) # salida
```

Por último, agregar los puertos a las VLAN:

```
consola (config) # Interfaz Ethernet 1 / 15
consola (config-if) # switchport permite añadir vlan 10 sin etiquetar
consola (config-if) # salida
```

Capítulo 11. Múltiples conexiones WAN

La WAN múltiples (multi-WAN) de las capacidades de pfSense le permiten utilizar Internet de múltiples conexiones para lograr un mayor tiempo de actividad y una mayor capacidad de rendimiento. Antes de proceder a una configuración multi-WAN, se necesita un trabajo de dos de interfaz (LAN y WAN) de configuración. pfSense es capaz de manejar muchas interfaces WAN, con las múltiples partidas con 10-12 WAN en la producción. Debe escala aún mayor que, a pesar de que no son conscientes de que ninguna de instalaciones que utilizan más de 12 redes WAN.

Cualquier adicionales interfaces WAN se conocen como OPT interfaces WAN. Las referencias a la WAN referirse a la principal interfaz WAN y WAN OPT a cualquier adicional interfaces WAN. No diferencias importantes entre los dos tipos de pfSense 1.2 que se cubren a través de este capítulo.

Este capítulo comienza cubriendo cosas que usted debe tener en cuenta al implementar cualquier multi-WAN solución, entonces cubre configuración multi-WAN con pfSense.

11.1. La elección de su conectividad a Internet

La elección ideal de conectividad a Internet dependerá en gran medida las opciones disponibles en su ubicación, pero hay algunos factores adicionales a tener en cuenta.

11.1.1. Cable Caminos

Hablando desde la experiencia de aquellos que han visto de primera mano los efectos de cable de múltiples la búsqueda de retroexcavadoras, así como infames ladrones de cobre, es muy importante asegurarse de que su opciones de conectividad para una implementación multi-WAN utilizan diferentes rutas de cableado. En muchos lugares, todas las conexiones T1 y DSL, así como cualesquiera otras que utilizan pares de cobre se llevan a cabo un solo cable sujeto al corte del cable mismo.

Si usted tiene una conexión que vienen de par de cobre (T1, DSL, etc), elegir una secundaria con la utilización de un tipo diferente y la ruta del cableado. conexiones de los cables suelen ser las más ampliamente las opciones disponibles que no están sujetos a la misma corte de los servicios de cobre. Otras opciones incluyen inalámbrica fija, y servicios de fibra que llegaba por un camino de cable distintos de los servicios de su cobre.

No se puede depender de dos conexiones del mismo tipo para proporcionar redundancia en la mayoría de los casos. Una interrupción del ISP o de corte de cable normalmente se establecen todas las conexiones del mismo tipo. Algunos pfSense usuarios hacer uso de múltiples líneas ADSL o cable módems múltiples, aunque la redundancia sólo que típicamente ofrece es que el aislamiento de módem u otro CPE (Customer Premise Equipment)

fracaso. Debe tener en cuenta múltiples conexiones desde el mismo proveedor, ya que sólo una solución para ancho de banda adicional, como la redundancia que ofrece este despliegue es mínimo.

11.1.2. Rutas de acceso a Internet

Otra consideración al seleccionar la conexión a Internet es el camino de su conexión a Internet. Para fines de redundancia, varias conexiones de Internet de la proveedor de la misma, especialmente del mismo tipo no se debe confiar en ellas.

Con los proveedores más grandes, dos diferentes tipos de conexiones, como un módem DSL y línea T1 generalmente atraviesan las redes de muy diferentes hasta llegar a las partes principales de la red. Estos componentes de red de la base suelen ser diseñados con alta redundancia y los posibles problemas se tratan rápidamente, ya que tienen efectos generalizados. Por lo tanto la conectividad como es aislado de la mayoría de las cuestiones ISP, pero ya que habitualmente utilizan el camino mismo cable, todavía le deja vulnerables a los apagones prolongados cortes de cable.

11.1.3. Redundancia mejor, más ancho de banda, menos dinero

Durante muchos años, el servicio T1 ha sido la opción para cualquier entorno de alta disponibilidad los requisitos. En general, el Service Level Agreements (SLA) que ofrece en las conexiones T1 mejor que otros tipos de conectividad, y la T1 son generalmente vistos como más confiables. Sin embargo, con capacidades multi-WAN pfSense, usted puede tener más ancho de banda y redundancia mejor por menos dinero en muchos casos.

La mayoría de las organizaciones que necesitan una alta disponibilidad de conexiones a Internet no quieren confiar en DSL, cable o de otro tipo "clase inferior" conexiones de banda ancha a Internet. Aunque por lo general son significativamente más rápido y más barato, el menor de SLA es suficiente para que muchas empresas seguir con T1 conectividad. En las zonas donde las opciones de costo más bajo múltiples de banda ancha están disponibles, tales como DSL y el cable, la combinación de pfSense y dos conexiones de Internet a bajo costo ofrece más ancho de banda y mejor redundancia a un menor costo. La posibilidad de dos diferentes banda ancha conexiones bajando al mismo tiempo es significativamente menor que la probabilidad de un fracaso o T1 interrupción de un servicio único.

11.2. Multi-WAN Terminología y conceptos

Esta sección cubre la terminología y conceptos que se necesitan para entender el despliegue de múltiples WAN con pfSense.

11.2.1. Política de encaminamiento

Política de encaminamiento se refiere a un medio de encaminamiento del tráfico en más de la dirección IP de destino
el tráfico, como se hace con la tabla de enrutamiento en la mayoría de sistemas operativos y routers. Esto es
logra mediante el uso de una política de algún tipo, por lo general las reglas del firewall o una lista de control de acceso. En pfSense, el campo de puerta de enlace disponible al modificar o agregar reglas de firewall permite el uso de política de enrutamiento. El campo Gateway contiene todas las interfaces WAN de su, más que ninguna conmutación por error o de la carga
equilibrio de las piscinas que haya definido.

Política de enrutamiento proporciona un poderoso medio de dirigir el tráfico a la interfaz WAN adecuada, ya que permite que se pongan en venta cualquier cosa que una regla de firewall puede igualar. hosts específicos, subredes, protocolos
y más se puede utilizar para dirigir el tráfico.

> **Nota**
>
> Recuerde que todas las reglas de cortafuegos incluida la política de las reglas de enrutamiento se procesan en
> orden de arriba hacia abajo, y gana el primer partido.

11.2.2. Puerta de enlace de Piscinas

piscinas de puerta de enlace son los que proporcionan la funcionalidad de conmutación por error y equilibrio de carga en pfSense. Ellos
se configuran en Servicios → Equilibrador de carga, en la ficha Pool.

11.2.3. Conmutación por error

Conmutación por error se refiere a la capacidad de utilizar una única interfaz WAN, pero no a otro si WAN
el preferido WAN falla.

11.2.4. Equilibrio de carga

El equilibrio de carga se refiere a la capacidad de distribuir la carga entre varias interfaces WAN. Nota
que el equilibrio de carga y conmutación por error no se excluyen mutuamente. Equilibrio de carga de forma automática también
proporciona capacidades de conmutación por error, como cualquier interfaz que está abajo se quita del equilibrio de carga piscina.

11.2.5. Monitor de PI

Al configurar el equilibrio de conmutación por error o de la carga, cada interfaz WAN se asocia con un monitor IP. pfSense se ping esta IP, y si deja de responder, la interfaz se marca como hacia abajo. Si este

monitor de IP se encuentra en una interfaz WAN OPT, pfSense añadirá automáticamente una ruta estática para este
de destino para dirigir el tráfico a cabo la correcta interfaz WAN. Esto significa que cada WAN debe tener un único monitor de IP. Usted puede utilizar el mismo monitor IP en varios grupos, siempre y cuando se utiliza en asociación con un solo WAN.

11.2.5.1. Así que lo que constituye un fracaso?

Como habrás adivinado, es un poco más compleja que "si hace ping a la IP del monitor no,
la interfaz se marca como hacia abajo. "Específicamente, el siguiente comando ping se utiliza para este seguimiento.

#ping-t 5-5-i OQC 0.7 <*dirección IP*>

A menos que usted está excepcionalmente bien versado en ping, que no te dice mucho. Las opciones son se detalla en Tabla 11.1, "Disección de la vigilancia de ping".

Opción de línea de comandos	Función
`-T 5`	Espere 5 segundos
`-O`	Salir con éxito después de recibir una respuesta paquete
`-Q`	Silencioso de salida. Sólo el resumen de salida al comienzo y al
`-C 5`	de meta.
`-I 0.7`	Enviar 5 paquetes Espere a 0,7 segundos entre el envío de cada paquete

Tabla 11.1. Disección de la vigilancia de ping

Así que esto significa que envía 5 pings a su monitor IP, a la espera 0.7 segundos entre cada una de ping. Es espera de hasta 5 segundos para una respuesta, y sale con éxito si se recibe una respuesta. Esto ha ha ajustado y afinado varias veces en los últimos años para llegar a este punto. Detecta casi todos los fracasos, y no es demasiado sensible. Ya que tiene éxito con la pérdida de paquetes del 80%, es teóricamente posible que la conexión podría estar experimentando la pérdida de paquetes tanto que no se puede utilizar, pero no está marcada como hacia abajo. Esto solía ser más estrictos, pero hemos encontrado que los falsos positivos y batir eran comunes en lugares menos estrictos, y esta es la mejor combinación para detectar los cortes y evitando el tratamiento innecesario aleteo. Algunas de estas opciones serán configurables por el usuario en pfSense 2.0.

11.3. Multi-WAN Advertencias y consideraciones

Esta sección contiene las advertencias y consideraciones específicas a la multi-WAN de pfSense.

11.3.1. Múltiples WAN compartiendo una única puerta de enlace IP

Debido a la pf manera controla el tráfico multi-WAN, sólo puede dirigirla por la puerta de enlace IP de la conexión. Esto está bien en la mayoría de escenarios. Si usted tiene múltiples conexiones en la misma red utilizando la misma puerta de enlace IP, como es común si tiene varios módems por cable, debe utilizar un dispositivo intermedio NAT para pfSense ve cada puerta de enlace WAN como IP única.

11.3.2. PPPoE o PPTP múltiples WAN

pfSense 1.2 sólo admite una única interfaz PPPoE o PPTP WAN, en la WAN primario. OPT WAN DHCP o debe ser asignado estáticamente. Usted puede acomodar múltiples WAN PPPoE configurar el PPPoE en el módem y que pasa a través de la IP pública de pfSense. pfSense 2.0 es compatible con PPPoE y PPTP en un número ilimitado de redes WAN.

11.3.3. Los servicios locales y Multi-WAN

Hay algunas consideraciones con los servicios locales y de múltiples WAN, ya que cualquier tráfico iniciado desde el servidor de seguridad en sí misma no se verán afectadas por las políticas de enrutamiento que han configurado, sino más bien
siguiente tabla de enrutamiento del sistema. Por lo tanto las rutas estáticas se requiere en algunas circunstancias utilizando las interfaces WAN OPT, de lo contrario sólo la interfaz WAN se utiliza. Esperamos
para ofrecer la capacidad de tráfico de la política de la ruta iniciada por el servidor de seguridad en pfSense 2.0 para permitir que más
flexibilidad. Esto sólo se aplica al tráfico que se inicia por el firewall. En el caso de tráfico iniciado en Internet destinado a una interfaz WAN OPT, pfSense utiliza automáticamente PF `de respuesta a` Directiva en todas las WAN y las normas OPT WAN, lo que garantiza el tráfico de respuesta es enviada de vuelta la correcta interfaz WAN.

Nota

A continuación se supone que está ejecutando pfSense 1.2.1 o más reciente. Si está ejecutando una versión anterior, en algunas circunstancias, puede encontrar problemas causados por un error determinado a partir de 1.2 fue liberado.

11.3.3.1. DNS Forwarder

Los servidores DNS utilizado por el promotor de DNS debe tener rutas estáticas definidas si utilizan un OPT Interfaz WAN, como se describe más adelante en este capítulo. No hay otras precauciones a reenviador DNS en entornos multi-WAN.

11.3.3.2. IPsec

IPsec es totalmente compatible con multi-WAN. Para conexiones de sitio a sitio con OPT WAN interfaces, una ruta estática se agrega automáticamente para el punto final del túnel remoto que apunta a la OPT WAN gateway para garantizar el cortafuegos envía el tráfico a la interfaz correcta cuando se iniciar la conexión. Para las conexiones móviles, el cliente siempre inicia la conexión, y el tráfico de respuesta es correcta derrotado por la tabla de estado.

11.3.3.3. OpenVPN

OpenVPN capacidades multi-WAN se describen en Sección 15.7, "OpenVPN y Multi-WAN".

11.3.3.4. Servidor PPTP

El servidor PPTP no es multi-WAN compatibles. Sólo se puede utilizar en la primaria WAN interfaz.

11.3.3.5. CARP y multi-WAN

CARP es multi-WAN capaz, siempre y cuando todas las interfaces WAN utilizan direcciones IP estáticas y tiene por lo menos tres IPs públicas por la WAN. Esto se trata en Sección 20.5, "Multi-WAN con la carpa".

11.4. Interfaz de configuración y DNS

En primer lugar usted necesita para configurar las interfaces WAN y los servidores DNS.

11.4.1. Interfaz de configuración

Las interfaces WAN primero tiene que ser configurado. Configuración de la WAN primaria según lo descrito previamente en Sección 4.2, "Asistente de configuración". Luego de las interfaces WAN OPT, seleccione DHCP o estático, en función de su tipo de conexión a Internet. Para conexiones estáticas de IP, escriba la dirección IP y puerta de enlace.

11.4.2. Configuración del servidor DNS

Usted tendrá que configurar pfSense con los servidores DNS de cada conexión WAN para asegurar su siempre es capaz de resolver nombres de dominio. Esto es especialmente importante si utiliza su red interna de pfSense Reenviador DNS para la resolución de DNS. Si se usa solamente un proveedor de Internet los servidores DNS, un corte de luz de ese Conexión WAN se traducirá en un corte de internet completa, independientemente de su política de enrutamiento puesto que la función de configuración de DNS ya no.

11.4.2.1. Servidores DNS y rutas estáticas

pfSense utiliza su tabla de enrutamiento para llegar a los servidores DNS configurados. Esto significa, sin

estática

rutas configurado, sólo utilizará la conexión WAN primaria para llegar a los servidores DNS. Estática
las rutas deben estar configurados para cualquier servidor DNS en una interfaz WAN OPT, por lo que utiliza el pfSense
correcta de interfaz WAN para llegar a ese servidor DNS.

Esto es necesario por dos razones. Uno, la mayoría de todos los ISP prohibir consultas recursivas de hosts fuera
su red, por lo tanto, debe utilizar la interfaz WAN correctos para acceder a ese servidor DNS del ISP.
En segundo lugar, si usted pierde su WAN primaria y no tienen una ruta estática definida por uno de sus
otros servidores DNS, perderá toda capacidad de resolución de DNS de pfSense sí mismo como todos los servidores DNS
será inalcanzable cuando el sistema de puerta de enlace predeterminada es inalcanzable. Si está utilizando pfSense
como su servidor DNS, esto se traducirá en un fracaso completo de DNS de la red.
Los medios para conseguir esto varía dependiendo del tipo de WAN en uso.

11.4.2.2. Todas las redes WAN IP estática

Este es el escenario más fácil de manejar, ya que cada WAN tiene una puerta de enlace IP que no va a cambiar. N
consideraciones adicionales son necesarios aquí.

11.4.2.3. Todas las redes WAN IP dinámica

IP dinámica interfaces WAN plantear dificultades debido a que su puerta de entrada está sujeta a cambios y
rutas estáticas en pfSense 1.2 debe apuntar a una dirección IP estática. Esta frecuencia no es un problema importante
porque sólo la dirección IP cambia mientras la puerta de entrada sigue siendo el mismo. Si su OPT WAN
públicos los cambios subredes IP y por lo tanto pasarelas con frecuencia, el uso del agente de DNS en pfSense
no es una solución adecuada para los servicios DNS redundantes, ya que no tendrás ningún medio fiable de
llegar a un servidor DNS en otra cosa que la interfaz WAN.
En escenarios donde no se puede configurar una ruta estática para llegar a uno de los servidores DNS a través de
una WAN territorio palestino ocupado, tiene dos alternativas. Dado que el tráfico de las redes dentro de la política
derrotados por las reglas de su firewall, no está sujeto a esta limitación. Usted puede utilizar los servidores DNS
en Internet en todos sus sistemas internos, tales como OpenDNS [Http://www.opendns.com]O
utilizar un servidor DNS o promotor de la red interna. Mientras que las peticiones DNS se inician
desde el interior de la red, y no en el servidor de seguridad en sí como en el caso de la agente de DNS,
rutas estáticas no son necesarios (y no tienen ningún efecto sobre el tráfico iniciado dentro de su red cuando
utilización de la política de enrutamiento).
Otra opción a considerar es el uso de una de sus direcciones IP del servidor DNS de cada conexión a Internet
como el período de investigación del monitor para esa conexión. Esto agregará automáticamente las rutas estáticas
adecuadas
para cada servidor DNS.

11.4.2.4. Mezcla de WAN IP estática y dinámica

Si usted tiene una mezcla de estática y dinámica dirigida interfaces WAN, la primaria WAN debe ser una de sus dinámicas WAN IP desde las rutas estáticas no son necesarios para los servidores DNS en la principal interfaz WAN.

11.4.2.5. Ejemplo de configuración de ruta estática

Este ejemplo ilustra el uso de OpenDNS [http://www.opendns.com/] Servidores DNS 208.67.220.220 y 208.67.222.222, uno en la WAN y uno en WAN2. En este ejemplo, el puerta de enlace de la WAN es 10.0.0.1 y la puerta de entrada de WAN2 es 192.168.0.1. La ruta estática para WAN no se requiere, como la ruta predeterminada del sistema siempre reside en la interfaz WAN, pero añadiendo no va a doler nada y deja claro que utiliza el servidor DNS que la WAN. Las rutas de este ejemplo debe aparecer como Figura 11.1, "Ejemplo de configuración de rutas estáticas para multi-WAN absoluto de los servicios "

Interface	Network	Gateway	Description
WAN2	208.67.220.220/32	192.168.0.1	OpenDNS #2 out WAN2
WAN	208.67.222.222/32	10.0.0.1	OpenDNS #1 out WAN

Figura 11.1. Ejemplo de configuración ruta estática para Multi-WAN servicios DNS

11.4.3. Escala a un gran número de interfaces WAN

Hay muchos usuarios pfSense desplegar 12.6 conexiones a Internet en una única instalación.

Un usuario pfSense tiene 10 líneas de ADSL porque en su país, es significativamente más barato que conseguir diez 256 Kb conexiones de lo que es una conexión de 2.5 MB. Él usa pfSense para equilibrar la carga un gran número de máquinas internas de cada 10 conexiones diferentes. Para obtener más información sobre esta escala de implementación, vea Sección 11.11, "Multi-WAN en un palo" acerca de "Multi-WAN en un palo", más adelante en este capítulo.

11.5. Casos especiales de Multi-WAN

Algunas implementaciones multi-WAN requieren soluciones debido a las limitaciones en pfSense 1.2. Este sección trata de los casos y la forma de acomodarlos.

11.5.1. Múltiples conexiones con la misma puerta de enlace IP

Debido a la forma pfSense distribuye el tráfico a través de conexiones de Internet múltiples, si usted tiene múltiples conexiones a Internet utilizando la misma puerta de enlace IP, tendrá que insertar un dispositivo NAT entre todos, pero una de esas conexiones. Esto no es una gran solución, pero es factible. Nosotros quisiera dar cabida a esta en una versión futura, pero es muy difícil debido a la forma en que el software subyacente dirige el tráfico cuando se hace política de enrutamiento.

11.5.2. Múltiples conexiones PPPoE o PPTP Tipo

pfSense sólo puede acomodar a una conexión PPPoE o PPTP WAN. OPT interfaces WAN

No se puede utilizar PPPoE o PPTP tipos WAN. La mejor solución es usar PPPoE o PPTP en su módem, u otro servidor de seguridad fuera de pfSense.

Para PPPoE, la mayoría de los módems DSL pueden manejar la PPPoE y ya sea directamente asignar su dirección IP pública

a pfSense, o darle una dirección IP privada y proporcionar NAT. Pública pasarela IP es posible en muchos módems y es el medio preferido para lograr esto.

11.6. Multi-WAN y NAT

El valor predeterminado NAT reglas generadas por pfSense se traducirá cualquier tráfico que sale de la WAN o un OPT interfaz WAN a la dirección IP de dicha interfaz. En una LAN predeterminado de la interfaz de dos y WAN configuración, pfSense se NAT todo el tráfico de salir de la interfaz WAN a la IP WAN dirección. La incorporación del territorio palestino ocupado interfaces WAN se extiende esto a NAT el tráfico dejando un OPT

Interfaz WAN a la dirección IP de dicha interfaz. Todo esto es manejado automáticamente a menos avanzada Salida NAT está habilitada.

La política de reglas de enrutamiento de dirigir el tráfico a la interfaz WAN utiliza, y la salida y 1:1 reglas NAT especificar cómo el tráfico será traducido.

11.6.1. NAT de salida multi-WAN y Avanzado

Si necesita avanzada de salida NAT con multi-WAN, lo necesario para garantizar configurar reglas NAT para todas las interfaces WAN.

11.6.2. Multi-WAN y redireccionamiento de puertos

Cada puerto hacia adelante se aplica a una sola interfaz WAN. Un puerto determinado se puede abrir en múltiples Interfaces WAN mediante el uso de múltiples entradas puerto hacia adelante, uno por cada interfaz WAN. La manera más fácil

para lograr esto es agregar el puerto para la conexión en la primera conexión WAN, a continuación, haga clic en el a
el derecho de que la entrada para añadir otro puerto hacia adelante sobre la base de que uno. Cambiar la interfaz a la deseada WAN, y haga clic en Guardar.

11.6.3. Multi-WAN y NAT 01:01

01:01 Las entradas NAT son propias de un solo interfaz WAN. sistemas internos pueden configurarse con tus 01:01 NAT en cada interfaz WAN, o una entrada de 1:1 en una o más interfaces WAN y el uso el NAT de salida por defecto a los demás. Cuando se configuran las entradas 01:01, siempre prevalecer sobre cualquier otra de salida NAT de configuración de la interfaz específica donde se configura la entrada de 1:1.

11.7. Equilibrio de carga

La funcionalidad de balanceo de carga en pfSense le permite distribuir el tráfico a través de múltiples WAN conexiones en una forma de round robin. Esto se hace sobre una base por conexión.

Una vigilancia IP se configura para cada conexión, que se pfSense ping. Si los pings no, la interfaz se puede marcar como y retirado de todos los grupos hasta que el ping éxito de nuevo.

11.7.1. Configuración de un grupo de balanceo de carga

En el pfSense WebGUI, vaya a Servicios → Equilibrador de carga. En la ficha Grupos, haga clic en. Este le llevará a la piscina del equilibrador de carga pantalla de edición. En las secciones siguientes se describe cada campo en esta página.

11.7.1.1. Nombre

En el campo Nombre, escribir un nombre para el grupo de conmutación por error de hasta 16 caracteres de longitud. Esto se
el nombre utilizado para referirse a este grupo en el campo de puerta de enlace en las reglas del cortafuegos. Este campo es obligatorio.

11.7.1.2. Descripción

Usted puede entrar en una descripción aquí para su consulta. Este campo se muestra en el equilibrador de carga pantalla de Piscinas, y no afecta a la funcionalidad de la piscina. Es opcional.

11.7.1.3. Tipo

Seleccione Puerta de enlace en este cuadro desplegable.

11.7.1.4. Comportamiento

Seleccione el Equilibrio de carga de aquí.

11.7.1.5. Puerto

Este campo aparece en gris cuando se utiliza el equilibrio de carga de puerta de enlace.

11.7.1.6. Monitor

Este campo aparece en gris cuando se utiliza el equilibrio de carga de puerta de enlace, ya que sólo ICMP se puede utilizar
para supervisar puertas de enlace.

11.7.1.7. Monitor IP

Esta es la dirección IP que va a determinar si la interfaz seleccionado (seleccionado a continuación) está disponible.
Si hace ping a esta dirección no, esta interfaz se marca como hacia abajo y ya no se utiliza hasta que se acceso de nuevo, como se explica en Sección 11.2.5, "Monitor de IP".

11.7.1.8. Nombre de interfaz

Aquí se define la interfaz que se usa junto con el monitor anterior período de investigación. Como se trata de una carga equilibrio de la piscina, cada interfaz añadida se utiliza por igual, siempre y cuando su monitor IP responde.
Si cualquier interfaz en la lista de falla, se quita de la piscina y la carga se distribuye entre
la interfaz restante (s).

11.7.1.9. Añadir a la piscina

Después de seleccionar una interfaz y elegir un monitor de IP, haga clic en el botón Añadir a la piscina para agregar la interfaz.

Después de añadir la primera interfaz de la piscina, seleccione la segunda interfaz, seleccione su IP supervisar y haga clic en Añadir a la piscina de nuevo. Cuando termine de agregar interfaces a la piscina, haga clic en Guardar, luego aplique
Cambios.

11.7.2. Problemas con el equilibrio de carga

Algunos sitios web almacenan sesión de información incluyendo su dirección IP, y si un posterior con el sitio se dirige a otro interfaz WAN usando una diferente dirección IP pública, la sitio web no funcionará correctamente. Esto es muy rara y sólo incluye algunos bancos en mi

la experiencia. Los medios sugeridos de trabajar alrededor de esto es crear un grupo de conmutación por error y directo
el tráfico destinado a estos sitios a la piscina de conmutación por error en lugar de la piscina de equilibrio de carga.

La función de las conexiones pegajosa de pf se supone que para resolver este problema, pero ha tenido problemas en el pasado. Esto debe ser resuelto en el número 1.2.3 y más allá.

11.8. Conmutación por error

Conmutación por error se refiere a la capacidad de utilizar sólo una conexión WAN, pero cambiar a otro si la WAN conexión preferida falla. Esto es útil para situaciones en las que quieres cierto tráfico, o la totalidad de su
el tráfico de utilizar una conexión WAN específica, a menos que no está disponible.

11.8.1. Configuración de un grupo de conmutación por error

En el pfSense WebGUI, vaya a Servicios → Equilibrador de carga. En la ficha Grupos, haga clic en. Este
le llevará a la piscina del equilibrador de carga pantalla de edición. En las secciones siguientes se describe cada campo en esta página. Estos campos son en gran parte los mismos que para la configuración de la carga de billar de equilibrio.

11.8.1.1. Nombre

En el campo Nombre, escribir un nombre para el grupo de conmutación por error de hasta 16 caracteres de longitud. Esto se
el nombre utilizado para referirse a este grupo en el campo de puerta de enlace en las reglas del cortafuegos. Este campo es obligatorio.

11.8.1.2. Descripción

Usted puede entrar en una descripción aquí para su consulta. Este campo se muestra en el equilibrador de carga pantalla de Piscinas, y no afecta a la funcionalidad. Es opcional, pero recomendado para entrar
algo descriptivo aquí.

11.8.1.3. Tipo

Seleccione Puerta de enlace en este cuadro desplegable. Todo el equilibrio de carga para multi-WAN utiliza el tipo de puerta de enlace.

11.8.1.4. Comportamiento

Seleccione de conmutación por error aquí.

11.8.1.5. Puerto

Este campo aparece en gris cuando se utiliza el equilibrio de carga de puerta de enlace.

11.8.1.6. Monitor

Este campo aparece en gris cuando se utiliza el equilibrio de carga de puerta de enlace, ya que sólo ICMP se puede utilizar
para supervisar puertas de enlace.

11.8.1.7. Monitor IP

Esta es la dirección IP que va a determinar si la interfaz seleccionado (seleccionado a continuación) está disponible. Si hace ping a esta dirección no, esta interfaz se marca como hacia abajo y ya no se utiliza hasta que se acceso de nuevo.

11.8.1.8. Nombre de interfaz

Aquí se define la interfaz que se usa junto con el monitor anterior período de investigación. Dado que se trata de un Piscina de conmutación por error, la primera interfaz agregó serán utilizados siempre y cuando su monitor IP es la respuesta a
pings. Si la primera interfaz añadida a la piscina falla, la segunda interfaz en la piscina se utilizará.

Asegúrese de agregar las interfaces a la piscina por orden de preferencia. El primero en la lista
Siempre se utilizará a menos que falle, momento en el que las interfaces restantes en la lista son retrocedido en el fin de arriba hacia abajo.

11.8.1.9. Añadir a la piscina

Después de seleccionar una interfaz y elegir un monitor de IP, haga clic en el botón Añadir a la piscina para agregar la interfaz.

Después de añadir la primera interfaz de la piscina, seleccione la segunda interfaz, seleccione su IP supervisar y haga clic en Añadir a la piscina de nuevo. Cuando termine de agregar interfaces a la piscina, haga clic en Guardar, luego aplique
Cambios.

11.9. Comprobación de la funcionalidad

Una vez que la configuración de la configuración multi-WAN que se desea verificar su funcionalidad. Los siguientes secciones se describe cómo probar cada parte de su configuración multi-WAN.

11.9.1. Prueba de conmutación por error

Si ha configurado la conmutación por error, tendrá que probarlo después de completar la configuración de asegurarse de que funciona como usted desea. No cometa el error de esperar hasta que uno de su Internet conexiones no tratar por primera vez la configuración de conmutación por error.

Vaya a Estado → Equilibrador de carga y asegurar todas las conexiones WAN muestran como "en línea" en Estado. Si no es así, verificar la configuración IP de vigilancia como se explicó anteriormente en este capítulo.

11.9.1.1. Creación de un error de la WAN

Hay un número de maneras en que puede simular un fallo de la WAN, que difieren según el tipo de conexión a Internet que se utiliza. Para cualquier tipo, en primer lugar tratar de desconectar el objetivo de interfaz WAN Cable Ethernet desde el servidor de seguridad.

Para las conexiones de cable y DSL, también querrá tratar de apagar el módem, y justo desenchufar el cable coaxial o línea telefónica del módem. Para los tipos T1 y otras conexiones con un router fuera de pfSense, intente desconectar la conexión a Internet desde el router, y también apagar el router.

Todos los escenarios de prueba descrito probablemente terminará con el mismo resultado. Sin embargo, hay algunas circunstancias en las que tratar todas estas cosas de forma individual se encuentra una culpa que no se de otro modo notado hasta que un fallo real. Uno de los más común es usar un monitor de IP asignado a su módem DSL o por cable (en algunos casos puede no ser consciente de que su puerta de enlace IP reside). Por eso, cuando la línea telefónica coaxial o se desconecta, la simulación de un proveedor falta más que un error de Ethernet o módem, el monitor de ping todavía tiene éxito, ya que es ping el módem. De lo que te dije pfSense para supervisar, la conexión sigue siendo hasta, por lo que no dejará de más aún si la conexión es realmente abajo. Existen otros tipos de fracaso que de igual forma puede sólo pueden detectarse mediante pruebas de todas las posibilidades individuales para el fracaso.

11.9.1.2. Verificación del estado de la interfaz

Después de crear un fallo de la WAN, volver a cargar el Estatuto → Equilibrador de carga de la pantalla para comprobar el actual de estado.

11.9.2. Verificación de la funcionalidad de equilibrio de carga

En esta sección se describe cómo comprobar la funcionalidad de la configuración de equilibrio de carga.

11.9.2.1. Verificación de equilibrio de carga HTTP

La forma más fácil de verificar una configuración de equilibrio de carga HTTP es visitar uno de los sitios web que muestra la dirección IP pública a qué atenerse. Una página en el sitio pfSense está disponible para este propósito [] Http://pfsense.org/ip.php, Y también hay un sinnúmero de otros sitios que sirven a la

mismo propósito. Búsqueda de "¿cuál es mi dirección IP" y encontrará numerosos sitios web que mostrar lo que la dirección IP pública de la solicitud HTTP está viniendo. La mayoría de estos sitios tienden a estar lleno de anuncios de spam, por lo que ofrecen varios sitios que simplemente le dice a su dirección IP.

HTTP sitios para encontrar su dirección IP pública

•http://www.pfsense.org/ip.php

•http://files.pfsense.org/ip.php

•http://cvs.pfsense.org/ip.php

•http://www.bsdperimeter.com/ip.php

HTTPS sitio para encontrar su dirección IP pública

•https: / / portal.pfsense.org / ip.php

Si se carga uno de estos sitios, y actualizar su navegador en varias ocasiones, debe consultar a su cambiar la dirección IP si el equilibrio de carga de configuración es correcta. Nota: si usted tiene cualquier otra tráfico de la red, es probable que no vea a su cambio de dirección IP en cada actualización de la página. Actualiza la página 20 o 30 veces y usted debe ver el cambio de IP por lo menos un par de veces. Si el IP no cambia, trate de varios sitios diferentes, y asegúrese de que su navegador es en realidad su interés la página de nuevo, y no regresar algo de su caché o el uso de una conexión permanente a el servidor. Eliminar manualmente el caché y tratando de múltiples navegadores web son cosas buenas para antes de intentar solucionar los problemas de configuración del equilibrador de carga adicional. Uso de rizo, como se describe en Sección 17.2.6, "Verificación de balanceo de carga" es una mejor alternativa, ya que garantiza la caché y conexiones persistentes no tendrá ningún impacto en los resultados.

11.9.2.2. Prueba de equilibrio de carga con traceroute

La utilidad traceroute (o tracert en Windows) le permite ver la trayectoria de la red llevado a un determinado destino. Ver Sección 8.4.2, "Utilización de traceroute" para obtener más información sobre el uso de traceroute.

11.9.2.3. Uso de los gráficos de tráfico

El tráfico en tiempo real los gráficos, en Estado → Gráfico del tráfico, son útiles para mostrar el tiempo real rendimiento de las interfaces WAN. Sólo puede mostrar un gráfico a la vez por la ventana del navegador, pero puede abrir ventanas o pestañas adicionales en el navegador y demostrar a todos sus interfaces WAN al mismo tiempo. La característica Dashboard en pfSense 2.0 (también disponible como un paquete beta 1.2) permite la visualización simultánea de múltiples gráficos de tráfico en una sola página.

Los gráficos de tráfico RRD en Estado → Los gráficos son útiles para la RRD largo plazo e histórico evaluación de su utilización WAN individuales.

Nota

Su uso de ancho de banda no puede ser exactamente igual distribuidos, ya que las conexiones simplemente se dirigió en forma de round robin sin tener en cuenta para el uso del ancho de banda.

11.10. Política de enrutamiento, el equilibrio de carga y Estrategias de conmutación por error

Usted tendrá que determinar la configuración multi-WAN que mejor se adapte a las necesidades de su el medio ambiente. Esta sección proporciona una orientación sobre los objetivos comunes, y cómo se logra con pfSense.

11.10.1. La agregación de ancho de banda

Uno de los deseos primarios con multi-WAN es la agregación de ancho de banda. Con el equilibrio de carga, pfSense puede ayudar a lograr esto. Hay, sin embargo, una advertencia. Si tiene dos 5 Mbps circuitos WAN, no se puede obtener 10 Mbps de rendimiento con una conexión de cliente único. Cada conexión individual debe estar atado a un solo WAN específica. Esto es cierto para cualquier multi-WAN solución, no se puede agregar el ancho de banda de dos conexiones a Internet en una sola gran "Tubo" sin la participación de la ISP. Con el equilibrio de carga, ya que las conexiones individuales equilibrado en una forma de round robin, puede alcanzar los 10 Mbps de transferencia de 5 Mbps utilizando dos circuitos, pero no con una sola conexión. Las aplicaciones que utilizan múltiples conexiones, tales como aceleradores de descargar muchos, será capaz de lograr la capacidad de rendimiento combinado de los dos o más conexiones.
En las redes con numerosos equipos internos el acceso a Internet, balanceo de carga permitirá a alcanzar cerca del rendimiento total por el equilibrio de las conexiones internas de muchos todas las interfaces WAN.

11.10.2. La segregación de los servicios prioritarios

En algunas situaciones, puede que tenga una conexión fiable a Internet de alta calidad que ofrece baja ancho de banda, o los altos costos de las transferencias excesivas, y otra conexión que es rápido pero de menor calidad (mayor latencia, jitter más o menos fiable). En estas situaciones, se puede segregar los servicios entre las dos conexiones a Internet de su prioridad. Servicios de alta prioridad puede incluir VoIP,

el tráfico destinado a una red específica, como un proveedor de aplicaciones externalizadas, algunos específicos
protocolos utilizados por las aplicaciones críticas, entre otras opciones. Baja el tráfico de prioridad común incluye todo el tráfico permitido que no coincide con la lista de tráfico de alta prioridad. Usted puede configurar su política de reglas de enrutamiento de tal manera que dirigir el tráfico de alta prioridad a la alta calidad conexión a Internet y el tráfico de menor prioridad a la conexión de menor calidad.

Otro ejemplo de un escenario similar es conseguir una conexión a Internet dedicada a la calidad servicios críticos, como VoIP, y sólo mediante esa conexión para los servicios.

11.10.3. Sólo de conmutación por error

Hay algunas situaciones en las que es posible que desee utilizar sólo conmutación por error. Algunos usuarios han pfSense una conexión secundaria de copia de seguridad de Internet con un límite de ancho de banda bajo, y sólo quiere usar esa conexión si su conexión primaria falla, y sólo mientras se está abajo. piscinas de conmutación por error le permiten para lograr esto.

Otro uso para las piscinas de conmutación por error es cuando se quiere garantizar un cierto protocolo o de destino siempre utiliza una sola WAN.

11.10.4. Costo de equilibrio de carga desigual

En pfSense 1.2, no puede configurar un valor de peso o de preferencia a las WAN. Sin embargo, esto no no significa equilibrar la carga desigual de los costos no pueden ser alcanzados. Esto es un poco de un truco, pero funciona así. Si usted tiene WAN y WAN2, WAN y añadir a la piscina dos veces, y una vez WAN2, WAN obtener dos terceras partes del tráfico total y WAN2 recibirá un tercio. La siguiente tabla muestra algunos las combinaciones posibles y la distribución porcentual en cada WAN.

WAN casos	casos WAN2	WAN de carga	carga WAN2
3	2	60%	40%
2	1	67%	33%
3	1	75%	25%
4	1	80%	20%

Tabla 11.2. Desigual carga de los costos de equilibrio

Figura 11.2, "carga desigual equilibrio de costes de configuración" muestra un saldo de 67% en la WAN y 33% en una WAN OPT llamado DSL.

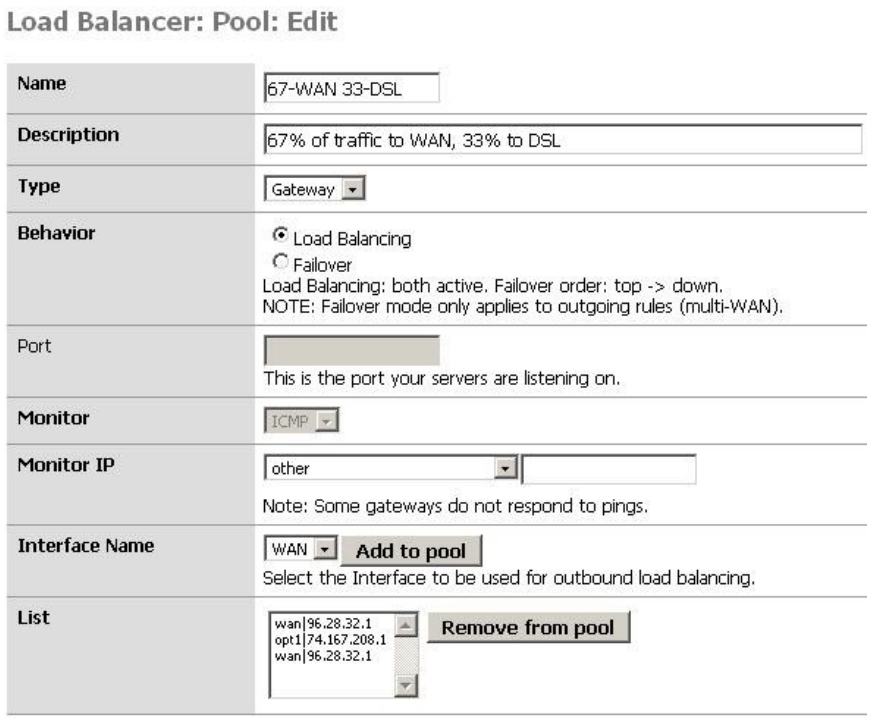


Figura 11.2. Desigual carga de los costos de equilibrio de configuración

Tenga en cuenta que esta distribución está estrictamente equilibrar el número de conexiones, que no tiene rendimiento de la interfaz en cuenta. Esto significa que su uso de ancho de banda no es necesario ser distribuidos por igual, aunque en la mayoría de los entornos que resulta ser más o menos distribuidos de la configurado con el tiempo. Esto también significa que si una interfaz se ha cargado a su capacidad con un solo alto con el rendimiento, conexiones adicionales seguirá siendo dirigido a esa interfaz. Lo ideal sería que quisiera que la distribución de las conexiones basadas en los pesos de interfaz y el rendimiento actual de la interfaz. Estamos estudiando las opciones para este escenario ideal para las versiones pfSense futuro, aunque los medios actuales de equilibrio de carga funciona muy bien para la mayoría de todos los ambientes.

11.11. Multi-WAN en un palo

En el mundo del router, Cisco y otros se refieren a un router VLAN como un "router en un palo", ya que puede ser un router funcionamiento con una sola conexión de red física. Ampliando esto, podemos han multi-WAN en un palo con VLAN y un conmutador administrado capaz de 802.1q trunking. La mayoría de las implementaciones de correr más de 5 WAN utilizan esta metodología para limitar el número

de interfaces físicas que se exigen en el firewall. En ese despliegue, la WAN todos residen en un interfaz física en el servidor de seguridad, con la red interna (s) sobre otras interfaces físicas. Figura 11.3, "Multi-WAN en un palo" ilustra este tipo de implementación.

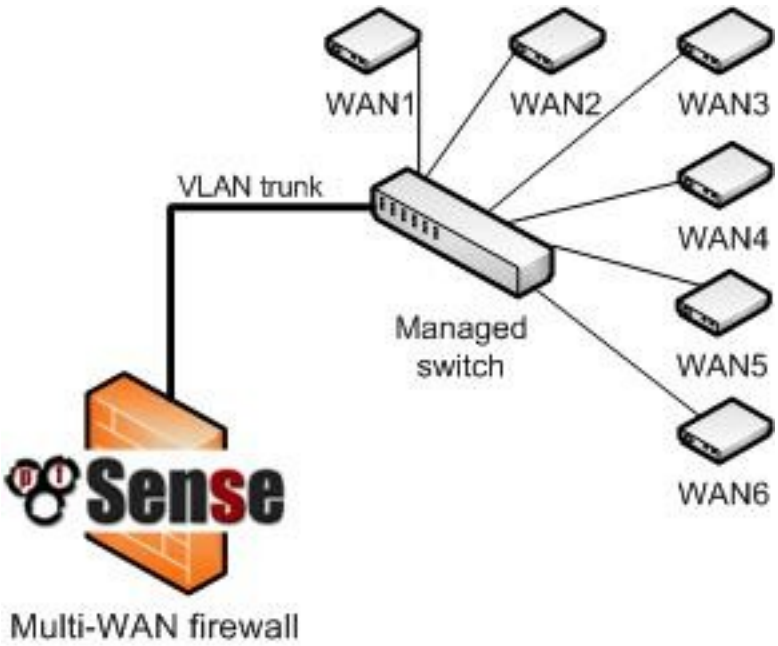


Figura 11.3. Multi-WAN en un palo

11.12. Solución de problemas

En esta sección se describen algunos de los problemas más comunes con multi-WAN y cómo solucionarlos.

11.12.1. Verifique su estado de configuración

El error más común en la configuración multi-WAN es una configuración incorrecta regla de firewall.

Recuerde que la primera regla que coincida gana - cualesquiera otras normas se ignoran. Si se agrega una política regla de enrutamiento por debajo de la norma por defecto de LAN, no hay tráfico siempre coincidirá con esta regla, ya que coincidirá con
la regla de LAN primer impago.

Si la regla de pedidos y la configuración parece correcta, puede ayudar a habilitar el registro en la reglas. Vea la sección de solución de problemas en el capítulo de firewall para obtener más información. Asegúrese de que el
política apropiada regla de enrutamiento pasa el tráfico.

11.12.2. Balanceo de carga no funciona

En primer lugar, garantizar la regla de firewall está emparejado dirige el tráfico a la piscina de equilibrio de carga. Si las reglas
son correctas, y el tráfico es que coincidan con una regla con la piscina equilibrador de carga especificado, compruebe que todas las conexiones de mostrar como en línea en Estado → Equilibrador de carga. Conexiones marcado como Fuera de línea no se utilizará. Por último, este puede ser un problema no con la configuración, pero con la metodología de ensayo. En lugar de probar con un navegador web, pruebe con rizos como se describe en Sección 17.2.6, "Verificación de balanceo de carga".

11.12.3. Conmutación por error no funciona

Si los problemas se producen cuando una conexión a Internet falla, normalmente es porque el monitor IP es todavía responder por lo que el piensa que el servidor de seguridad de conexión está disponible. Comprobar estado → Equilibrador de carga
para verificar. Puede que esté utilizando la dirección IP de su módem como un monitor de IP, que normalmente sigue ser accesibles incluso si la conexión a Internet no funciona.

Capítulo 12. Redes privadas virtuales

Las VPNs proporcionan un medio de túneles de tráfico a través de una conexión encriptada, evitando que se ser vistos o modificados en tránsito. pfSense ofrece tres opciones de VPN con IPSec, OpenVPN y PPTP. En este capítulo se ofrece una visión general del uso de VPN, los pros y los contras de cada tipo de VPN en pfSense, y cómo decidir cuál es la mejor opción para su entorno. Los capítulos siguientes van a discutir cada opción VPN en detalle.

12.1. despliegues comunes

Hay cuatro usos comunes de las capacidades de VPN de pfSense, cada uno cubierto en esta sección.

12.1.1. Sitio para conectividad de sitio

Sitio para conectividad de sitio se utiliza principalmente para conectar redes en múltiples ubicaciones físicas, donde una dedicada, conexión permanente entre los lugares se requiere. Esto es con frecuencia utiliza para conectar sucursales con una oficina principal, conectar las redes de socios de negocios, o conectar su red a otra ubicación, como un entorno de co-localización. Antes de la proliferación de la tecnología VPN, los circuitos privados WAN eran la única solución para conectar varias ubicaciones. Estas tecnologías incluyen un punto a otro de circuitos dedicados, conmutación de paquetes tecnologías como Frame Relay y ATM, y, más recientemente, MPLS (Multiprotocol Label Switching) y fibra y cobre servicios basados en Ethernet metropolitanas. Si bien este tipo de conectividad WAN privadas ofrecen conexiones fiables, baja latencia, que también son muy costosas con recurrencia de cuotas mensuales. La tecnología VPN ha crecido en popularidad, ya que proporciona la mismo lugar seguro para la conectividad de sitio usando conexiones de Internet que son generalmente mucho menos costoso.

12.1.1.1. Limitaciones de la conectividad VPN

En algunas redes, sólo un circuito privado WAN puede cumplir los requisitos de ancho de banda o latencia. La latencia es generalmente el factor más importante. Un punto a punto del circuito T1 tiene una latencia de extremo a extremo de alrededor de 3.5 ms, mientras que la latencia hasta el primer salto en el ISP de la red general, será a por lo tanto si no más. Servicios Metro Ethernet tienen un extremo a otro de latencia de alrededor de 1.3 ms, por lo general menos de la latencia hasta el primer salto de su proveedor de Internet de la red. Que variará algunos basados de la distancia geográfica entre los sitios. Los números indicados son típicos de los sitios dentro de un par de cientos de kilómetros uno del otro. VPN suelen ver la latencia de alrededor de 30 a 60 ms dependiendo en las conexiones a Internet en el uso y la distancia geográfica entre los lugares. Usted puede minimizar la latencia y maximizar el rendimiento de VPN utilizando el mismo proveedor para todas sus VPN lugares, pero esto no siempre es factible.

Algunos protocolos funcionan muy mal con la latencia inherente a las conexiones a través de Internet. compartir archivos de Microsoft (SMB) es un ejemplo común. En sub-10 ms de latencia, se desempeña bien. A los 30 ms o más, es lento, y en más de 50 ms es dolorosamente lenta, causando frecuentes se bloquea al navegar por carpetas, guardar archivos, etc Obtener un listado de directorio simple requiere numerosas conexiones de ida y vuelta entre el cliente y el servidor, lo que agrava considerablemente el retraso cada vez mayor de la conexión. En Windows Vista y Server 2008, Microsoft introdujo SMB 2.0, que incluye nuevas capacidades para abordar el problema descrito aquí. SMB 2.0 permite el envío de múltiples acciones en una sola solicitud, así como la capacidad de las solicitudes de tuberías, es decir, el cliente puede enviar solicitudes adicionales sin esperar la respuesta de antes peticiones. Si su red utiliza exclusivamente Vista y Server 2008 o sistemas operativos más recientes de este no será una preocupación, pero dada la rareza de estos entornos, lo cual suele ser una consideración.
Dos ejemplos más de los protocolos sensibles a la latencia son Microsoft Remote Desktop Protocol (RDP) y el ICA de Citrix. No es una actuación clara y la diferencia de respuesta con estos protocolos de entre los sub-20 ms tiempo de respuesta se encuentran típicamente en una red WAN privada, y el 50-60 + veces ms respuesta común a las conexiones VPN. Si los usuarios remotos el trabajo publicado en equipos de escritorio que utilizan dispositivos de cliente ligero, habrá una diferencia de rendimiento notable entre un privadas WAN y VPN. Ya sea que la diferencia de rendimiento es lo suficientemente importantes como para justificar la expensas de una WAN privada variará de un entorno a otro. He trabajado en fina entornos de cliente que aceptó el impacto en el rendimiento, y en otros en los que se considera inaceptable.
Puede haber otras aplicaciones de red en su entorno que son sensibles a la latencia, donde la reducción del rendimiento de una VPN es inaceptable. O usted puede tener todas las ubicaciones dentro de un relativamente pequeña área geográfica con el mismo proveedor de Internet, donde el rendimiento de sus rivales VPN de conexiones WAN privada. El rendimiento es una consideración importante al planear una solución VPN.

12.1.2. Acceso remoto

VPN de acceso remoto permiten a los usuarios conectarse de forma segura a su red desde cualquier lugar donde una conexión a Internet está disponible. Esto es de uso más frecuente para los trabajadores móviles (a menudo conocido como "Road Warriors"), cuyo trabajo requiere de viajes frecuentes y poco tiempo en la oficina, y dar a los empleados la posibilidad de trabajar desde casa. También puede permitir a los contratistas o proveedores acceso temporal a la red.

12.1.3. Protección para redes inalámbricas

Una VPN puede proporcionar una capa adicional de protección para sus redes inalámbricas. Esta protección es doble, ya que proporciona una capa adicional de cifrado para el tráfico que atraviesa su red inalámbrica

red, y puede ser desplegado de forma que requiere autenticación adicional antes de el acceso a los recursos de la red está permitido. Esto se implementa en su mayoría los mismos que el acceso remoto VPN. Esto se trata en Sección 18.6, "la protección adicional para su red inalámbrica".

12.1.4. Asegure relé

VPN de acceso remoto se puede configurar de una manera que pasa todo el tráfico desde el sistema cliente través de la VPN. Esto es bueno tener al utilizar redes no confiables, tales como puntos de acceso inalámbrico como le permite impulsar todo el tráfico Internet a través de la VPN, y salen a Internet desde su VPN servidor. Esto lo protege de una serie de ataques que la gente podría estar intentando de confianza redes, a pesar de que tiene un impacto en el rendimiento, ya que añade el lúpulo y la latencia adicional a todas sus conexiones. Ese impacto es mínimo por lo general con conectividad de alta velocidad cuando se están relativamente cerca geográficamente.

12.2. Elegir una solución VPN para su el medio ambiente

Cada solución VPN tiene sus pros y sus contras. En esta sección se cubren las principales consideraciones en elegir una solución de VPN, proporcionando la información necesaria para tomar una decisión para su el medio ambiente.

12.2.1. Interoperabilidad

Si necesita una solución para interoperar con un firewall o un router producto de otro proveedor, IPsec suele ser la mejor opción ya que se incluye con cada dispositivo VPN con capacidad. También mantiene que de ser encerrados en cualquier servidor de seguridad particular, o una solución VPN. Para el sitio de la interoperabilidad, para
conectividad de sitio, IPsec suele ser la única opción. OpenVPN es interoperable con otros pocos cortafuegos envasados / soluciones VPN, pero no muchos. La interoperabilidad en este sentido no es aplicable con PPTP, ya que no se puede utilizar para conexiones de sitio a sitio.

12.2.2. Autenticación de las consideraciones

De las opciones disponibles para la VPN en pfSense 1.2.x, sólo admite PPTP nombre de usuario y contraseña autenticación. IPsec y OpenVPN dependa únicamente de claves compartidas o certificados. OpenVPN certificados pueden ser protegidos con contraseña, en cuyo caso un certificado en peligro por sí sola no es adecuada para la conexión a la VPN. La falta de autenticación adicional puede ser una garantía riesgo de que un sistema de pérdida, robo, o comprometida que contiene un medio clave o certificado de quien tiene acceso al dispositivo puede conectarse a la VPN. Sin embargo, aunque no es ideal, no es tan grande

riesgo que pueda parecer. Un sistema comprometido puede fácilmente tener instalado un capturador de teclado para capturar
la información de nombre de usuario y contraseña y fácil derrotar a esa protección. En el caso de pérdida o
sistemas de robo de claves que contiene, si el disco duro no está cifrado, las claves se puede utilizar para conectarse.
Sin embargo la adición de autenticación de contraseña no es de gran ayuda no sea, como suele ser el mismo
nombre de usuario y contraseña se utiliza para iniciar sesión en el ordenador, y la mayoría de las contraseñas se manipulable
en cuestión de minutos utilizando hardware moderno cuando se tiene acceso a un disco sin cifrar. Contraseña
la seguridad es también con frecuencia por los usuarios comprometidos con notas sobre su ordenador portátil o en su ordenador portátil
caso con la contraseña escrita.
En pfSense 2.0, todas las opciones disponibles de soporte VPN nombre de usuario y contraseña de autenticación en
Además de compartir las claves y certificados.

12.2.3. Facilidad de configuración

Ninguna de las opciones disponibles de VPN son muy difíciles de configurar, pero hay diferencias
entre las opciones. PPTP es muy sencillo de configurar y es el más rápido y más fácil de conseguir
de trabajo, pero tiene desventajas considerables en otras áreas. IPsec tiene una configuración de numerosos
opciones y puede ser difícil para los no iniciados. OpenVPN requiere el uso de certificados de
de acceso remoto en la mayoría de entornos, que viene con su propia curva de aprendizaje y puede ser una
ardua poco de manejar. IPsec y OpenVPN son opciones preferibles en muchos escenarios para otros
razones expuestas en este capítulo, pero la facilidad de configuración no es uno de sus puntos fuertes.

12.2.4. Multi-WAN capaz

Si desea que los usuarios tienen la posibilidad de conectarse a múltiples conexiones WAN, PPTP no es
una opción por la forma en que funciona GRE en combinación con la forma en pfSense multi-WAN
funciones. Ambos IPsec y OpenVPN puede ser utilizado con multi-WAN.

12.2.5. Cliente disponibilidad

Para VPNs de acceso remoto, la disponibilidad de software de cliente es una consideración primordial. PPTP
la única opción con el apoyo de cliente integrado en la mayoría de sistemas operativos, pero las tres opciones son
multiplataforma compatible.

12.2.5.1. IPsec

clientes IPsec están disponibles para Windows, Mac OS X, BSD y Linux a pesar de que no están incluidos
en el sistema operativo a excepción de algunas distribuciones de Linux. Una buena opción gratuita para Windows es la
Domada suave
cliente [http://www.shrew.net/]. Mac OS X incluye soporte IPsec, pero no la interfaz de usuario amigable
para su utilización. Hay opciones gratuitas y comerciales disponibles con una interfaz gráfica de usuario fácil de usar.

El cliente de Cisco IPsec incluye con el iPhone y el iPod Touch no es compatible con pfSense IPsec.

12.2.5.2. OpenVPN

OpenVPN tiene clientes para Windows, Mac OS X, todos los BSD, Linux, Solaris y Windows Mobile, pero el cliente no viene pre-instalado en cualquiera de estos sistemas operativos.

12.2.5.3. PPTP

clientes PPTP se incluyen en todas las versiones de Windows desde Windows 95 OSR 2, todos los Mac OS versión X, iPhone y iPod Touch, y los clientes están disponibles para todos y cada uno de los BSD principales distribuciones de Linux.

12.2.6. Firewall de amistad

protocolos de VPN puede causar dificultades a muchos cortafuegos y dispositivos NAT. Esto se debe principalmente relevantes para la conectividad de acceso remoto, donde los usuarios estarán detrás de un gran número de servidores de seguridad sobre todo fuera de su control con diferentes configuraciones y capacidades.

12.2.6.1. IPsec

IPsec utiliza tanto el puerto UDP 500 y el protocolo ESP para funcionar. Algunos servidores de seguridad no manejan ESP tráfico, así que se trata de NAT, ya que el protocolo no tiene números de puerto TCP como y UDP que lo hacen fácilmente rastreables por los dispositivos NAT. clientes IPsec detrás de NAT puede requerir NAT-T para la función, que encapsula el tráfico de pesetas a través del puerto UDP 4500. En la actualidad, pfSense no es compatible con NAT-T, para que los clientes detrás de NAT no puede funcionar en algunos casos. Hay una advertencia a la falta de soporte de NAT-T, discutido en Sección 13.7, "IPsec y NAT-T".

12.2.6.2. OpenVPN

OpenVPN es la mayoría de firewalls de las opciones de VPN. Puesto que utiliza TCP o UDP y se no se ve afectado por cualquiera de las funciones de NAT comunes, como la reescritura de los puertos de origen, es raro encontrar un cortafuegos que no funcionará con OpenVPN. La única dificultad es posible si el protocolo y puerto en uso está bloqueado. Es posible que desee utilizar un puerto común como UDP 53 (por lo general DNS), o TCP 80 (normalmente HTTP) o 443 (por lo general HTTPS) o para evadir la mayoría de filtrado de salida.

12.2.6.3. PPTP

PPTP se basa en un canal de control que se ejecutan en el puerto TCP 1723 y utiliza el protocolo GRE para transmisión de datos. GRE es con frecuencia bloqueado o roto por los cortafuegos y dispositivos NAT. También es

sujeto a las limitaciones NAT en muchos firewalls incluyendo pfSense (descrito en Sección 14.4, "Limitaciones PPTP). PPTP funciona en muchos ambientes, pero los usuarios se encontrarán con probabilidad lugares en los que no funciona. En algunos casos esto puede ser un problema importante la prevención de la uso de PPTP. A modo de ejemplo, algunos proveedores de datos inalámbricos 3G asignar direcciones IP privadas a los clientes,
y no bien NAT tráfico GRE, por lo que el uso de PPTP a través de 3G imposible en algunos redes.

12.2.7. Criptográficamente segura

Una de las funciones críticas de una VPN para garantizar la confidencialidad de los datos transmitidos.
PPTP ha sufrido varios problemas de seguridad en el pasado, y tiene algunos defectos de diseño que lo convierten en un débil solución VPN. La situación no es tan grave como algunos lo hacen ser, aunque el seguridad de PPTP depende de los usuarios la elección de contraseñas seguras. Como la mayoría de usuarios no utilizar contraseñas seguras, o seguir las malas prácticas, tales como escribir las contraseñas, PPTP más sujetos a compromiso de las otras opciones. PPTP sigue siendo ampliamente utilizado, aunque si debe ser un tema de debate. Las contraseñas seguras siempre debe ser empleado, lo que limita el riesgo. Siempre que sea posible, no recomendamos el uso de PPTP. Algunos implementarlo sin tener en cuenta porque del factor de conveniencia.
IPsec con claves pre-compartidas se puede romper si una clave débil es utilizado. Utilice una clave fuerte, por lo menos 10 caracteres de longitud que contiene una mezcla de mayúsculas y minúsculas, números y símbolos.
cifrado OpenVPN se ve comprometida si el PKI o claves compartidas se dan a conocer.

12.2.8. Resumen

Tabla 12.1, "Funciones y características según el tipo de VPN" muestra una visión general de la consideraciones previstas en esta sección.

Tipo de VPN	Cliente incluidos en	Ampliamente interoperables	Crypto Multi-	WAN-gráficamente	Servidor de seguridad ambiente
IPsec	la mayoría de operativos	sistemas	sí	seguro sí	no (sin
	No	sí			NAT-T)
OpenVPN	No	No	sí	sí	sí
PPTP	sí	n / a	No	No	más

Tabla 12.1. Características y propiedades por Tipo de VPN

12.3. VPNs y reglas de firewall

VPNs y las reglas del firewall se manejan algo incompatible en pfSense 1.2.x. En esta sección describe cómo se manejan las reglas del cortafuegos para cada una de las opciones individuales de VPN. Para el añade automáticamente las reglas discutidas aquí, puede deshabilitar la incorporación de esas normas por los cheques Deshabilitar todas las reglas VPN agregó automática en Sistema → Avanzado.

12.3.1. IPsec

Reglas para el tráfico IPsec que llegan a la interfaz WAN se especifica de forma automática permite como se describe en Sección 6.5.1.5, "IPsec". Tráfico cerrada dentro de una conexión IPsec activa controla a través de normas definidas por el usuario en la pestaña Servidor de seguridad de IPsec en → Normas.

12.3.2. OpenVPN

OpenVPN no agrega automáticamente las normas de interfaces WAN, pero lo agrega automáticamente normas que permitan el tráfico de los clientes autenticados, frente al comportamiento de IPSec y PPTP.

12.3.3. PPTP

PPTP agrega automáticamente normas que permitan TCP 1723 y el tráfico GRE en el IP WAN. Tráfico de conectar clientes PPTP se controla a través de normas definidas por el usuario en la pestaña Servidor de seguridad de PPTP en → Normas, similares a IPsec.

Capítulo 13. IPsec

IPSec VPN proporciona una implementación basada en estándares que es compatible con una amplia gama de clientes para la conectividad móvil, y otros cortafuegos y routers para el sitio de la conectividad del sitio. Es compatible con numerosos dispositivos de terceros y se utiliza en la producción de dispositivos que van de los routers Linksys grado de consumo todo el camino hasta a IBM z / OS mainframes, y todo imaginable en el medio. En este capítulo se describen las opciones de configuración disponibles, y cómo configurar diferentes escenarios comunes.

Para una discusión general de los distintos tipos de redes privadas virtuales disponibles en pfSense y sus pros y sus contras, ver Capítulo 12, Redes privadas virtuales.

13.1. Terminología de IPsec

Antes de ahondar demasiado en la configuración, hay algunos términos que se utilizan en todo el capítulo que necesitan una explicación previa. Otros términos que se explican con más detalle sobre su su uso en las opciones de configuración.

13.1.1. Asociación de Seguridad

Una Asociación de Seguridad (SA) es un túnel de una vía a través del cual el tráfico cifrado viajará.

Cada túnel IPsec activa tendrá dos asociaciones de seguridad, uno para cada dirección. El Consejo de Seguridad Las asociaciones son de configuración entre las direcciones IP públicas para cada extremo. El conocimiento de estos asociaciones de seguridad activas se mantiene en la Base de Datos de Seguridad de la Asociación (SAD).

13.1.2. Política de Seguridad

Una Política de Seguridad Manges las especificaciones completas del túnel IPSec. Al igual que con seguridad Asociaciones, se trata de un solo sentido, así que para cada túnel habrá uno en cada dirección. Estos las entradas se mantienen en la Base de Datos de Seguridad Común (SPD). El SPD se rellena con dos entradas para cada conexión del túnel tan pronto como un túnel, se añade. Por el contrario, las entradas SAD sólo existen en éxito de la negociación de la conexión.

13.1.3. Fase 1

Hay dos fases de la negociación de un túnel IPsec. Durante la Fase 1, los dos extremos instalación de un túnel de un canal seguro entre los extremos utilizando Internet Security Association y Key Management Protocol (ISAKMP) para negociar las entradas SA y las claves de cambio. Este

También incluye la autenticación, control de los identificadores y la comprobación de las claves pre-compartida (PSK) o
certificados. Cuando se haya completado la Fase 1 los dos extremos pueden intercambiar información de forma segura, sino que han
No se ha decidido lo que el tráfico atravesará el túnel o la forma en que se cifrará.

13.1.4. Fase 2

En la Fase 2, los dos extremos de negociar la forma de codificar y enviar los datos para los anfitriones privado basado en políticas de seguridad. Esta es la parte que construye el túnel real que se utiliza para transferir datos entre los puntos finales y clientes cuyo tráfico es manejado por los routers. Si la Fase 2 se ha ha establecido con éxito, el túnel estará listo y preparado para su uso.

13.2. Elegir opciones de configuración

IPsec ofrece numerosas opciones de configuración, que afectan el rendimiento y la seguridad de su Conexiones IPsec. Siendo realistas, poco importa que las opciones que elija aquí el tiempo que no uso de DES, y el uso de una clave fuerte pre-compartida, a menos que esté protegiendo algo tan valioso que un adversario con muchos millones de dólares en poder de procesamiento está dispuesto a dedicar que para romper con su IPsec. Incluso en ese caso, no es probable una manera más fácil y mucho más barato que entrar en su red y lograr el mismo resultado final (ingeniería social, por ejemplo).

13.2.1. Interfaz de selección

En muchos casos, la opción de interfaz para un túnel IPSec se WAN, ya que los túneles son conectarse a sitios remotos. Sin embargo, hay un montón de excepciones, el más común de lo que A continuación se describen.

13.2.1.1. CARP entornos

En los entornos de CARP (Capítulo 20, Firewall de redundancia / alta disponibilidad), Cualquier CARP direcciones IP virtuales también están disponibles en el menú desplegable de la interfaz. Usted debe elegir el adecuada dirección de las carpas para la WAN oa cualquier otro lugar del túnel IPSec terminará en la sistema de pfSense. Al utilizar la dirección IP CARP, asegura que el túnel IPSec se manejará por el miembro principal del grupo CARP, así que incluso si el firewall principal es hacia abajo, el túnel se conectará a cualquier miembro de la CARP clúster se ha hecho cargo.

13.2.1.2. Multi-WAN entornos

Cuando se utiliza Multi-WAN (Capítulo 11, Múltiples conexiones WAN), Usted debe escoger el adecuada elección de la interfaz WAN del tipo al que se conectará el túnel. Si

esperar la conexión para entrar a través de WAN, elija WAN. Si el túnel debe utilizar otro WAN, elegir cualquier territorio palestino ocupado de interfaz WAN es necesario.

13.2.1.3. Inalámbrico de protección interna

Si va a configurar IPSec para añadir cifrado a una red inalámbrica, como se describe en Sección 18.6.2, "protección adicional con VPN", usted debe elegir la interfaz que OPT corresponde a la tarjeta inalámbrica. Si está usando un punto externo de acceso inalámbrico, escoger el pfSense interfaz se puede utilizar para conectarse al punto de acceso inalámbrico.

13.2.2. Los algoritmos de cifrado

Hay seis opciones para los algoritmos de cifrado en tanto la fase 1 y fase 2. DES (Data Encryption Standard) se considera inseguro debido a su pequeño tamaño 56 bits clave, y nunca debe utilizarse a menos que se ven obligados a conectar con un dispositivo remoto que sólo es compatible con DES. La opciones restantes son considerados criptográficamente seguros. ¿Cuál elegir depende de lo que dispositivo que se conecta a, y el hardware disponible en el sistema. Cuando se conecta a dispositivos de terceros, 3DES (también llamada "Triple DES") es comúnmente la mejor opción ya que puede ser la única opción compatible con el otro extremo. Para los sistemas sin un acelerador de hardware de criptografía, Blowfish y CAST son las opciones más rápido. Cuando se utilizan sistemas con `glxsb` aceleradores, como como ALIX, elija Rijndael (AES) para un mejor rendimiento. Para los sistemas con `hifn` aceleradores, eligió 3DES o AES para el mejor funcionamiento.

13.2.3. Cursos de la vida

La vida útil especificar la frecuencia con la conexión debe ser rekeyed, especificado en segundos. 28800 segundos en la fase 1 y 3600 segundos en la fase 2 es una configuración bastante estándar y se apropiado para la mayoría de escenarios.

13.2.4. Protocolo

Con IPsec tiene la opción de elegir AH (Encabezado autenticados) o ESP (Encapsulado Carga de seguridad). En casi todas las circunstancias, debe utilizar pesetas, ya que es la única opción que encripta el tráfico. AH sólo ofrece la garantía del tráfico de vino de la fuente de confianza y es rara vez se utiliza.

13.2.5. Algoritmos hash

Los algoritmos hash se utilizan con IPsec para verificar la autenticidad de los datos del paquete. MD5 y SHA1 son los algoritmos hash disponibles en la fase 1 y fase 2. Ambos son considerados criptográficamente

seguro, aunque SHA1 (Secure Hash Algorithm, Revisión 1) es considerado el más fuerte de la dos. SHA1 requiere más ciclos de CPU. Estos algoritmos hash también se puede referir con HMAC (Hash Message Authentication Code) en el nombre en algunos contextos, pero que varía según el uso dependiendo en el hardware o el software en uso.

13.2.6. DH clave de grupo

Todos los DH (Diffie-Hellman, el nombre de sus autores) las opciones de clave de grupo se consideran criptográficamente segura, aunque los números más altos son un poco más segura en el costo de mayor uso de la CPU.

13.2.7. PFS de clave de grupo

Confidencialidad directa perfecta (PFS) proporciona el material de claves con una mayor entropía, por lo tanto, la mejora de la seguridad de cifrado de la conexión, en el costo de uso de CPU más alta cuando cambio de claves se produce.

13.2.8. Muerto de detección de pares (DPD)

Dead Peer Detection (DPD) es una revisión periódica que el host en el otro extremo del túnel IPSec todavía está vivo. Si un cheque no DPD, el túnel es derribado por la eliminación de sus asociados de las entradas SAD y se intenta la renegociación.

13.3. IPsec y las reglas del firewall

Al configurar una conexión de túnel IPSec, firewall pfSense agrega automáticamente oculta normas para permitir que el puerto UDP 500 y el protocolo ESP en el portal de IP remota destinado a la interfaz IP especificada en la configuración. Cuando Permitir a los clientes móviles se activa, el mismo las reglas del firewall se añaden, con excepción de la fuente se define en cualquier. Para anular la adición automática de estas normas, visita deshabilitar todas las reglas VPN agregó automáticamente en Sistema → Avanzado. Si marca esa caja, debe agregar manualmente las reglas del cortafuegos para UDP 500 y ESP para el caso WAN interfaz.

Tráfico inicia desde el extremo remoto de una conexión IPsec se filtra con las reglas configuradas en virtud de firewall → Reglas, ficha IPsec. Aquí usted puede restringir lo que los recursos se puede acceder por los usuarios remotos IPsec. Para controlar el tráfico que se puede transmitir de redes locales para el control remoto IPsec VPN conectados dispositivos o redes, las normas relativas a la interfaz local donde el anfitrión reside controlar el tráfico (por ejemplo, la conectividad de los hosts de la LAN se controlan con las normas de LAN).

13.4. Un sitio a otro

Un sitio a otro túnel IPSec permite interconectar dos redes como si fueran directamente conectadas por un router. Sistemas en el sitio A puede llegar a los servidores u otros sistemas en el sitio B, y viceversa. Este tráfico también puede ser regulada a través de reglas de firewall, al igual que con cualquier otra red interfaz. Si más de un cliente se conecta a otro sitio de la misma controlada lugar, un sitio para hacer un túnel sitio probablemente será más eficiente, por no mencionar más conveniente y más fácil de soportar.

Con un sitio para hacer un túnel del sitio, los sistemas de cualquier red no necesita tener ningún conocimiento de que un VPN existe. No se necesita software de cliente, y todo el trabajo del túnel está a cargo de la routers en cada extremo de la conexión. Esta es también una buena solución para los dispositivos que han de red apoyo, pero no manejan las conexiones VPN, tales como impresoras, cámaras, sistemas de climatización, y otros integrado de hardware.

13.4.1. Sitio en la configuración de sitio de ejemplo

La clave para hacer un trabajo túnel IPsec es asegurarse de que ambas partes tienen sus correspondientes ajustes para la autenticación, encriptación, etc. Antes de comenzar, tome nota de lo local y remoto WAN direcciones IP, así como las subredes internas locales y remotos que se conectan.

Una dirección IP de la subred remota de ping es opcional, pero recomendado para mantener el túnel con vida. El sistema no busca respuestas, ya que cualquier tráfico iniciado a una IP en la red a distancia activar la negociación de IPsec, por lo que no importa si el host responde realmente o no, siempre y cuando se una dirección IP en el otro lado de la conexión. Aparte de la descripción del túnel de cosméticos y estos piezas de información, la configuración de otro tipo de conexión será el mismo.

En este ejemplo, y algunos de los ejemplos posteriores en este capítulo, la configuración de los siguientes se supone:

El sitio A		Sitio B	
Nombre	Louisville Oficina	Nombre	Oficina de Londres
WAN IP	172.23.1.3	WAN IP	172.16.1.3
Conexión de subred	192.168.1.0/24	Conexión de subred	10.0.10.0/24
IP de la LAN	192.168.1.1	IP de la LAN	10.0.10.1

Tabla 13.1. Configuración de IPsec de punto final

Vamos a empezar con el sitio A. En primer lugar, debe habilitar IPsec en el router. Vaya a VPN → IPsec, de verificación Habilitar IPsec, haga clic en Guardar (Figura 13.1, "Habilitar IPsec").

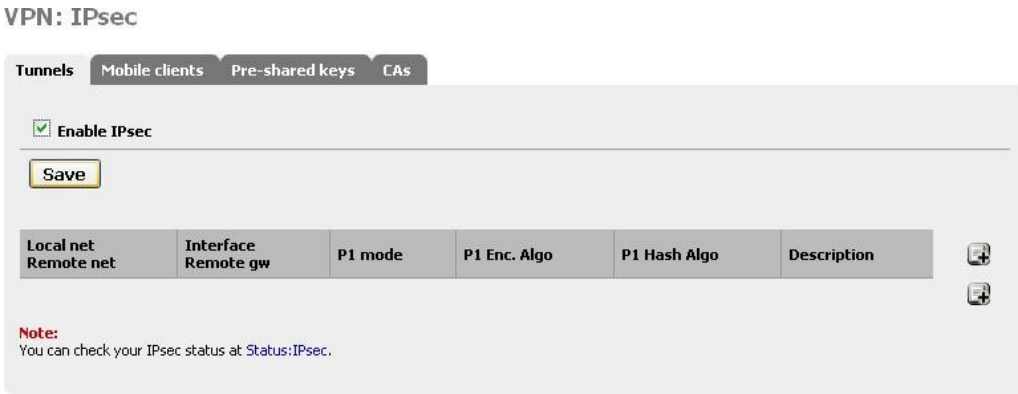


Figura 13.1. Habilitar IPsec

Ahora, crear el túnel presionando el botón. Ahora verá una página de gran tamaño que tiene todo ajuste necesario para el túnel de funcionar. No sea demasiado desalentados, ya que muchos de estos valores pueden ser dejados en sus valores por defecto.

Para empezar, llene la parte superior que contiene la información general del túnel y de la red configuración, que se muestra en la Figura 13.2, "el sitio A del túnel VPN Configuración". Los elementos en negrita son obligatorios. Hacer Asegúrese de que el cuadro Desactivar este túnel no está marcada. La configuración de la interfaz debe ser probable **WAN**, Pero véase la nota anterior en el capítulo sobre la selección de la interfaz adecuada si no está seguro. Rellene el Dead Peer Detection (DPD) con algo de valor razonable, tales como **60** segundos. Dependiendo de sus necesidades en un valor inferior puede ser mejor, más como **10** o **20** segundos, pero una problemática WAN de conexión en cualquier lado puede hacer que demasiado baja. Para la subred local, es probablemente mejor dejar esto como **Conexión de subred**. También puede cambiar esto a **Red** y rellenar el valores propios, en este caso **192.168.1.0/24**, Pero dejando como **Conexión de subred** se asegurará de que si la red cada vez pasa a ser, este extremo del túnel seguir. Tenga en cuenta los otros final se debe cambiar manualmente. La subred remota será la red en el sitio B, en este caso **10.0.10.0/24**. El portal de acceso remoto es la dirección de la WAN en el Sitio B, **172.16.1.3**. Por último, Escriba una descripción para el túnel. Es una buena idea poner el nombre del sitio B de este cuadro, y algunas detalles sobre el propósito del túnel también puede ayudar a la futura administración. Vamos a poner "**ExampleCo Oficina de Londres**"En la descripción de lo que tenemos alguna idea de dónde termina el túnel.

La siguiente sección controles Fase IPsec 1, o la autenticación. Se muestra en la Figura 13.3, "Sitio La Fase 1 Configuración ". Los valores predeterminados son deseables para la mayoría de estas configuraciones, y simplifica el proceso. El ajuste más importante para hacerlo bien es la clave pre-compartida. Como se mencionó en la VPN información general, IPsec utilizando claves pre-compartidas se puede romper si una clave débil es utilizado. Utilice una clave fuerte, por lo menos 10 caracteres de longitud que contiene una mezcla de mayúsculas y minúsculas, números y

símbolos. La clave exactamente el mismo tendrá que ser ingresado en la configuración del túnel para el sitio B más tarde, así que lo desea, puede escribir o copiar y pegar en otro lugar. Copia y pega puede muy útil, sobre todo con una clave compleja como **abc123 XyZ9% $ 7qwErty99**. Toda una vida ajuste también se puede especificar, de lo contrario el valor por defecto de **86400** se utilizará. A medida que se utilizando una clave pre-compartida y no certificados, deje todas las casillas de certificado de vacío.

En cuanto a la Fase 2 (Figura 13.4, "el sitio A la Fase 2 Configuración"), No puede haber una variabilidad poco más. La Protocolo de elección podría ser **AH** por sólo paquetes autenticados o **ESP** para el cifrado. ESP es el elección en casi todos los casos inusuales pocos. Los algoritmos de cifrado y algoritmos hash se pueden establecer para permitir múltiples opciones, y ambas partes negocian y acuerdan las ajustes. En algunos casos puede ser una buena cosa, pero por lo general es mejor limitar esto a la opciones que sabe que estar en uso. Para este ejemplo, el algoritmo de cifrado sólo algunos es 3DES, y el único algoritmo de hash SHA1 es seleccionado. PFS, o confidencialidad directa perfecta, puede ayudar a proteger contra ciertos ataques clave, pero es opcional. Un valor de por vida también se puede especificar, de lo contrario el valor por defecto de **3600** se utilizará.

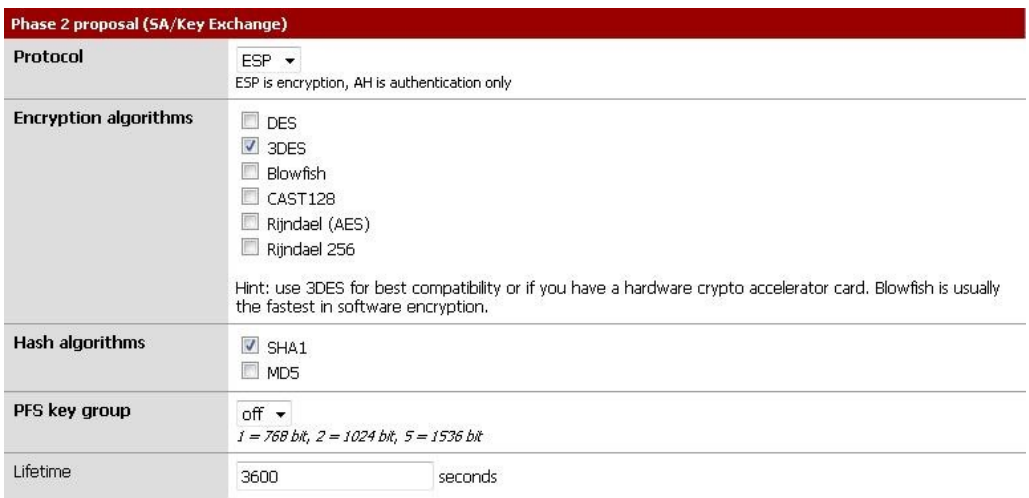


Figura 13.4. Un sitio de la Fase 2 Configuración

Por último, puede introducir una dirección IP para un sistema en la red LAN remota que periódicamente deben ser envía un ping ICMP, como en Figura 13.5, "el sitio A Keep Alive". El valor de retorno del ping no es marcada, esto sólo se asegurará de que algunos se envía el tráfico en el túnel de modo que se quedará establecido. En esta configuración, se puede utilizar la dirección IP de LAN del router pfSense en el Sitio B, **10.0.10.1**.

Figura 13.5. Un sitio Keep Alive

Haga clic en el botón Guardar y, a continuación, tendrá que haga clic en Aplicar los cambios en los túneles IPSec
VPN: IPsec
pantalla, como se ve en Figura 13.6. "Aplicar configuración de IPsec".

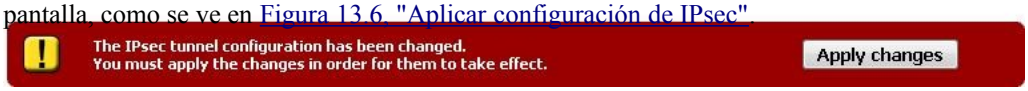


Figura 13.6. Aplicar Configuración de IPsec

El túnel para el sitio A está terminado, pero ahora las reglas del cortafuegos son necesarios para permitir el tráfico desde el sitio
la red B que está por venir en medio del túnel IPSec. Estas normas se debe agregar a la ficha de IPsec en Servidor de seguridad → Normas. Véase el capítulo de reglas de firewall para obtener información específica sobre la adición de las normas. Es posible que
ser tan permisiva como quieras, (permitir cualquier protocolo desde cualquier parte), o restrictivas (Permitir que TCP desde un host en el sitio B a un host determinado en el sitio A en un puerto determinado). En cada caso, asegúrese de que la dirección de origen (es) son las direcciones del sitio B, tales como **10.0.10.0/24**. La direcciones de destino debe ser el sitio de una red, **192.168.1.0/24**.

Ahora que el sitio A está configurado, es hora de hacer frente a sitio B. Repita el proceso en el router de la web de B para que IPsec y agregar un túnel.

Sólo dos partes de esta configuración puede ser diferente desde el sitio A. Estos son los parámetros generales y la Mantener el ajuste vivo, como se puede ver en Figura 13.7, "Sitio B Configuración VPN Tunnel". Asegúrese de que que el cuadro Desactivar este túnel no está marcada. La configuración de la interfaz debe ser **WAN**. Rellene el Dead Peer Detection (DPD) de valor con la misma configuración del sitio A.. Para la subred local, es probablemente sea mejor dejar esto como **Conexión de subred**. También puede cambiar esto a **Red** y llenar en los valores adecuados, en este caso **10.0.10.0/24**. La subred remota será la red
en el sitio A, en este caso **192.168.1.0/24**. El portal de acceso remoto es la dirección de la WAN en el Sitio A, **172.23.1.3**. Descripción del túnel es una buena idea. Vamos a poner "**ExampleCo Louisville Oficina**"En este lado.

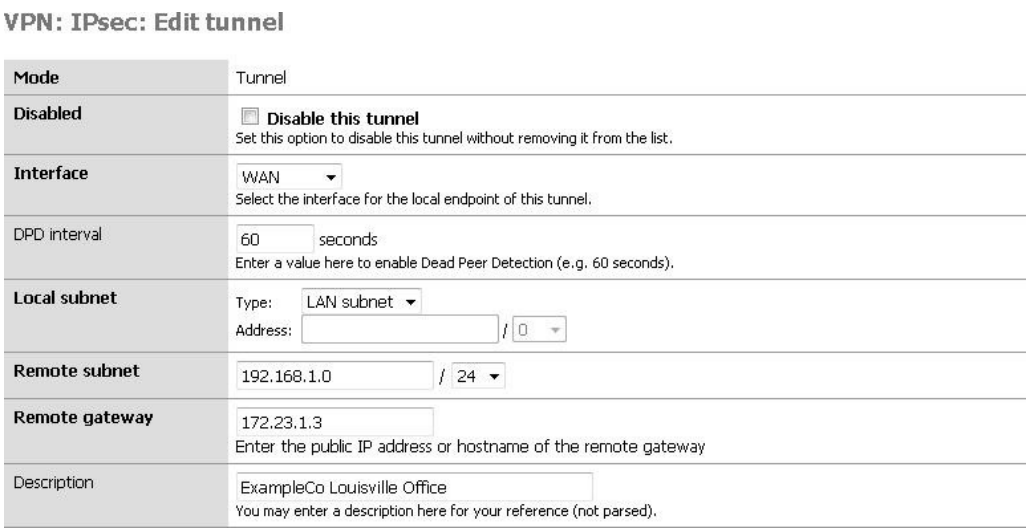


Figura 13.7. Sitio B Configuración del túnel VPN

La Fase 1 y Fase 2 configuración debe coincidir con el sitio A exactamente. Revisión de que el artículo de este ejemplo
para los detalles y las cifras.

El último cambio es el valor Keep Alive (Figura 13.8, "B Sitio Keep Alive"). En esta configuración, que puede utilizar la dirección IP de LAN del router pfSense en el sitio A, **192.168.1.1**.

Figura 13.8. Sitio B Keep Alive

Ahora haga clic en el botón Guardar y, a continuación, haga clic en Aplicar los cambios en la pantalla de túneles IPSec.

Al igual que con el sitio A, también debe agregar las reglas del firewall para permitir el tráfico en el túnel para cruzar de Sitio A al sitio B. Añadir estas normas a la pestaña Servidor de seguridad de IPsec en → Normas. Para más detalles,
ver Sección 13.3, "IPsec y las reglas del firewall". Esta vez, el origen del tráfico sería Sitio Una, el destino del sitio B.

Ambos túneles se configuran ahora y debe ser activo. Compruebe el estado de IPsec, visite Estado → IPsec. Usted debe ver una descripción del túnel, junto con un icono indicador de su estado.

Si no encuentra el icono, puede haber un problema de establecer el túnel. Esto pronto, el más razón probable es que el tráfico no ha tratado de cruzar el túnel. Intente hacer ping a un sistema en el subred remota en el Sitio B desde el sitio A (o viceversa) y ver si el túnel se establece. Mira Sección 13.6, "Prueba de conectividad IPsec" para otros medios de prueba de un túnel.

En su defecto, la IPsec registros ofrecerá una explicación. Ellos se encuentran en Estado → Sistema de Registros en la ficha VPN IPsec. Asegúrese de comprobar el estado y los registros en ambos sitios. Para obtener más solución de problemas, consulte la Sección 13.8, "Solución de problemas de IPsec" más adelante en este capítulo.

13.4.2. Enrutamiento y las consideraciones de puerta de enlace

Cuando el punto final de VPN, en este caso un router pfSense, es la puerta de enlace predeterminada para una red que debería haber problemas con el enrutamiento. Como un PC cliente envía el tráfico, irá a la caja de pfSense, sobre el túnel, y por el otro extremo. Sin embargo, si el router pfSense no es la puerta de enlace predeterminada para una red dada, las medidas de encaminamiento a continuación, otros tendrán que ser tomadas.

Como ejemplo, imagine que el router pfSense es la puerta de enlace en el sitio B, pero no el sitio A, como se ilustra en la Figura 13.9, "un sitio a otro IPsec Cuando pfSense no es la puerta de enlace". Un cliente, PC1 en el sitio B envía un ping a PC2 en el sitio A. El paquete de hojas de PC1, luego a través de la web del router B, a través del túnel, el router pfSense en el sitio A, y en la PC2. Pero lo que sucede en el camino de nuevo? puerta de entrada PC2 es otro router por completo. La respuesta al ping será enviado a la puerta de enlace sistema y es muy probable que arrojó a cabo, o peor aún, se puede enviar el enlace a Internet y perder de esa manera.

Hay varias maneras de evitar este problema, y cualquiera puede ser mejor en función de la circunstancias de cada caso. En primer lugar, una ruta estática se podía entrar en la puerta de enlace que redirigirá el tráfico destinado al otro lado del túnel para el router pfSense. Incluso con esta ruta, las complejidades adicionales se introducen porque este escenario resulta en el enrutamiento asimétrico como se explica en Sección 8.1.2, "Bypass reglas de firewall para el tráfico en la interfaz de la misma". En caso de que no funciona, una ruta estática puede ser añadido a los sistemas cliente de forma individual para que conozcan a enviar ese tráfico directamente a la caja de pfSense y no a través de su puerta de enlace predeterminada. A menos que haya sólo un número muy pequeño de los ejércitos que necesitan acceder a la VPN, se trata de un dolor de cabeza gestión y deben evitarse. Por último pero no menos importante, en algunas situaciones puede ser más fácil para que el pfSense cuadro de la puerta de entrada y se deja manejar su conexión a Internet.

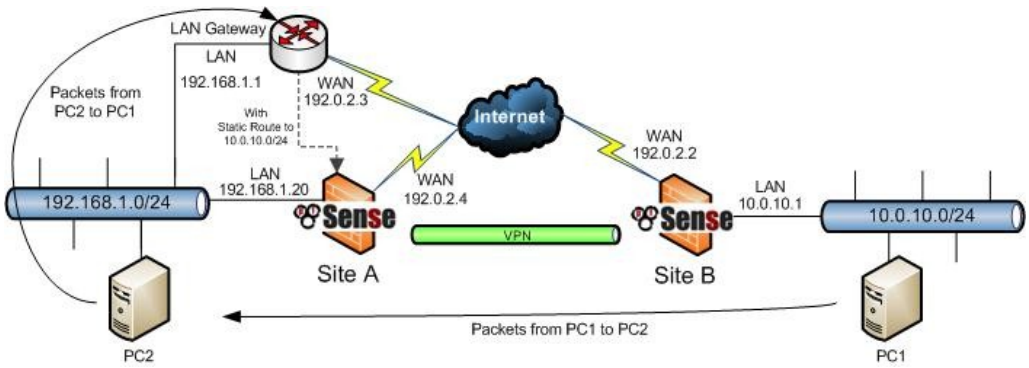


Figura 13.9. Un sitio a otro IPsec Cuando pfSense no es la puerta de enlace

13.4.3. Enrutamiento de múltiples subredes a través de IPsec

Si necesita subredes múltiples rutas IP a través de IPSec, usted tiene dos opciones - CIDR resumen y paralelo túneles IPsec. pfSense 2.0 permite la definición de varias subredes por conexión IPsec, pero el 1,2 que debe hacer uno de los siguientes.

Nota

Tráfico atravesará un túnel IPsec sólo si coincide con una entrada existente SAD. Estática rutas nunca no enrutar el tráfico a través de una conexión IPsec, configurar rutas estáticas para el tráfico IPsec excepto en el caso del tráfico iniciado desde pfSense en sí (que será discutido más adelante).

13.4.3.1. CIDR de resumen

Si las subredes son contiguos, puede subredes ruta múltiple en un túnel con un más grande de subred que incluye todas las subredes más pequeñas. Por ejemplo, si un sitio incluye el subredes 192.168.0.0/24 y 192.168.1.0/24, que pueden resumirse como 192.168.0.0/23. Ver Sección 1.7.5, "de resumen CIDR" para más información.

13.4.3.2. Paralelo túneles IPsec

La única opción si las subredes no se resumen es la creación de túneles IPsec paralelas, una para cada subred.

Haga clic en el a la derecha de la primera conexión a añadir otra en función de ésta. Cambiar sólo el subred remota (a la segunda subred que desea conectarse) y establecer el PSK a algo diferente de la primera conexión. Guarde los cambios.

13.4.4. pfSense iniciado por tráfico e IPsec

Para acceder a la final alejado de las conexiones IPsec desde pfSense sí mismo, tendrá que "falso" el sistema mediante la adición de una ruta estática que apunta la red remota a la LAN IP del sistema. Nota este ejemplo supone la VPN se conecta la interfaz LAN en ambos lados. Si su IPsec conexión es la conexión de un interfaz de OPT, cambie la dirección IP de interfaz y de la interfaz en consecuencia. Debido a la forma de IPsec está ligada en el kernel de FreeBSD, sin la ruta estática el tráfico seguirá tabla de enrutamiento del sistema, que probablemente enviará este tráfico de la WAN interfaz en lugar de sobre el túnel IPSec. Tome Figura 13.10, "un sitio a otro IPsec", por ejemplo.

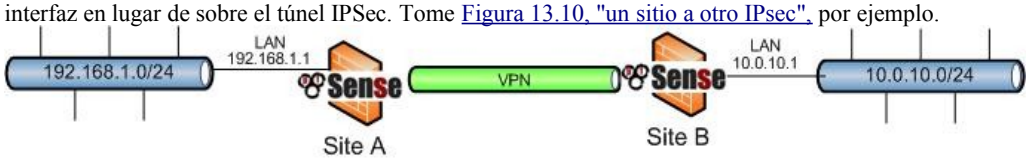


Figura 13.10. Un sitio a otro IPsec

Es necesario agregar una ruta estática en cada servidor de seguridad. Figura 13.11, "Sitio A - ruta estática a distancia subred " y Figura 13.12, "Sitio B - ruta estática a la subred remota" mostrar la ruta que se agregó en cada lado.

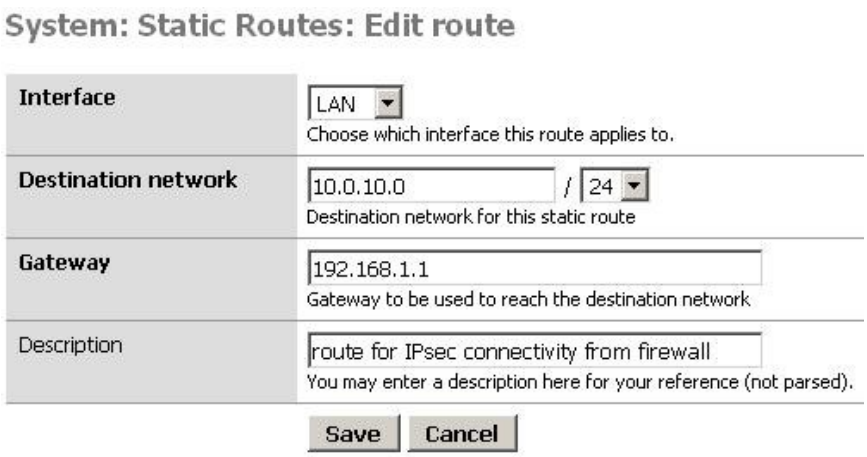


Figura 13.11. Sitio A - ruta estática a la subred remota

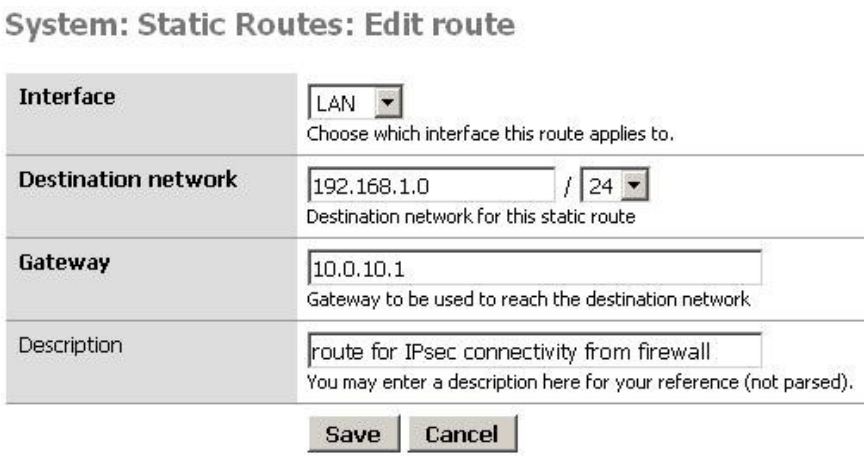


Figura 13.12. Sitio B - ruta estática a la subred remota

13.5. Móvil IPsec

Móvil IPsec le permitirá hacer una llamada "Road Warrior" con estilo, el nombre de
la naturaleza variable de cualquier persona que no está en la oficina que necesita para conectarse de nuevo a la principal
red. Puede ser una persona de las ventas mediante Wi-Fi en un viaje de negocios, el jefe de su limosina a través de
Módem 3G, o un programador de trabajo de su línea de banda ancha en casa. La mayoría de estos se
se ven obligados a lidiar con direcciones IP dinámicas, ya menudo ni siquiera se conoce la dirección IP que
tener. Sin un router o firewall apoyo IPsec, una tradicional túnel IPsec no funcionará. En
teletrabajo escenarios, por lo general es indeseable e innecesario para conectar al usuario de todo
red doméstica a la red, e introducirá enrutamiento complicaciones. Aquí es donde IPsec
Los clientes móviles vienen pulg
Sólo hay una definición para móviles IPsec en pfSense, por lo que se estará preguntando cómo
configuración de varios clientes. En lugar de confiar en una dirección fija para el extremo remoto del túnel, una
identificador único / precompartida par de claves se utiliza, como un nombre de usuario y contraseña. Esto permite que
que los clientes estén autenticados y distinguen entre sí.

Antes de empezar a configurar los clientes, es posible que desee elegir un rango de direcciones IP que se
a utilizar. Esto no se controla en el servidor, así que algún tipo de atención serán necesarios para asegurar que
Las direcciones IP no se superponen al configurar el software de cliente. Las direcciones IP deben ser diferentes de
los que se utilizan en el lugar de alojamiento del túnel móvil. En este ejemplo, *192.168.111.0/24* se
ser utilizado, pero puede ser cualquier subred no utilizados que usted desea. Por otra parte, no están obligados a
especificar una dirección IP. Los clientes pueden configurar para que pase a través de la dirección IP local

el cliente que se conecta. Esta será una IP privada donde el cliente está detrás de NAT, y una IP pública donde uno es asignado directamente al cliente. Si se basa en el filtrado de IP de origen en el interfaz IPsec, tendrá que especificar una dirección IP para cada cliente para que siempre sepa la IP de origen y no va a cambiar. Si no se especifica la IP de origen también puede crear dificultades de encaminamiento, donde el cliente está en una red local en conflicto con uno de sus redes internas.

13.5.1. Ejemplo de configuración del servidor

Hay dos componentes en la configuración del servidor para los clientes móviles: Creación del túnel, y crear las claves pre-compartidas.

13.5.1.1. Cliente móvil túnel Creación

En primer lugar, debe habilitar IPsec en el router si no lo ha hecho. Vaya a VPN → IPsec, IPsec de verificación Habilitar, haga clic en Guardar. Con IPsec activa, el soporte de cliente móvil también debe estar encendido. Desde VPN → IPsec, haga clic en la pestaña de clientes móviles (Figura 13.13, "Activa Móvil IPsec Clientes "). Compruebe la casilla Permitir clientes móviles, y luego continúe con el siguiente opciones.

Figura 13.13. Habilitar móvil clientes IPsec

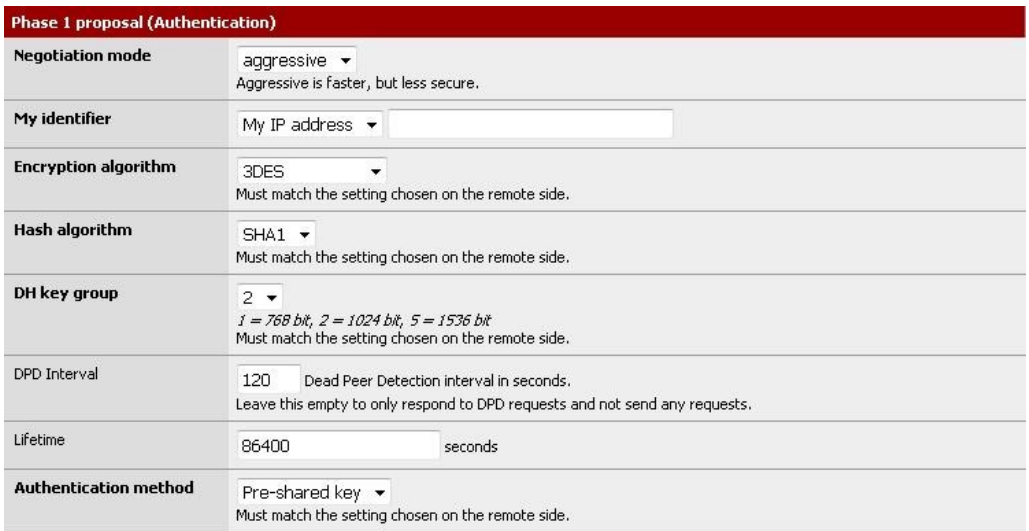


Figura 13.14. Los clientes móviles de la Fase 1

La Fase 1 propuesta ahora debe estar configurado para la autenticación, como se muestra en Figura 13.14, "Fase clientes móviles 1". Cuando se trate de clientes móviles, lo mejor es el uso seguro y ampliamente configuración compatible. Uso de **agresivos** para el modo de negociación que permiten utilizar un amplio gama de tipos de identificadores, tales como el estilo de dirección de correo electrónico que se utilizan en este ejemplo de configuración.

Desde este lado debe tener una dirección estática, utilizando **Mi dirección IP** Mi identificador para la opción deben ser seguros. El algoritmo de cifrado, **3DES** y el algoritmo de hash **SHA1** son seguros y bien apoyado. Un grupo clave de DH **2** es una tierra buena y segura, medio también. Debido a la gran variación en los tipos de conexión que se tratarán, un mayor valor de alrededor de DPD **120** segundo Es más probable que garantizar que las conexiones no se caen antes de tiempo. La vida se puede establecer mucho menor si lo desea, pero **86400** todavía debe ser aceptable. Nosotros vamos a usar **Precompartida Clave** para el método de autenticación, ya que en este ejemplo, queremos que todos tengan individuales Identificadores y claves pre-compartidas.

Figura 13.15, la "Fase 2 clientes móviles" muestra la fase 2 de las opciones para los túneles móviles. Desde el tráfico cifrado es importante en este caso, el Protocolo debe ser establecido para **ESP**. El cifrado algoritmos para la Fase 2 se pueden establecer para las que sea necesario. Es posible que determinado software los clientes se comportan mejor que los demás utilizando diferentes algoritmos. Una elección segura es por lo menos al momento del check

3DES, Pero otros pueden ser utilizados. Para los algoritmos hash, se puede elegir tanto **SHA1** y **MD5**O sólo uno de los dos. PFS es opcional, y dependiendo del software de cliente involucrado puede ser mejor dejar esta **fuera**. El valor por defecto de por vida **3600** es probablemente una buena idea aquí. Ahora haga clic en Guardar y seguir adelante.

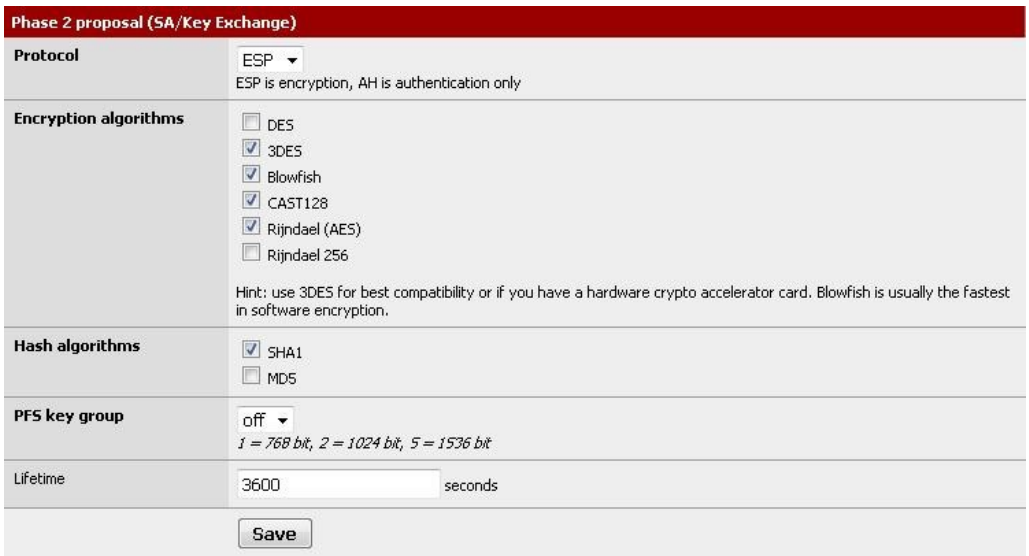


Figura 13.15. Los clientes móviles de la Fase 2

Después de hacer clic en Guardar la configuración se debe aplicar antes de que surtan efecto. Haga clic en Aplicar cambios (Figura 13.16, "Aplicar configuración móvil del túnel") Y luego el túnel de configuración para móviles clientes se ha completado.

Figura 13.16. Aplicar configuración del túnel móvil

13.5.1.2. Cliente móvil clave Creación precompartida

La siguiente parte de la instalación del cliente móvil es para entrar en los identificadores y pre-compartidas claves para la clientes individuales. Desde VPN → IPsec, haga clic en la ficha de claves pre-compartidas. Esto mostrará una lista de todos los
Actualmente creado Identificador pares PSK, como se ve en Figura 13.17, "IPsec Pre-Shared Key" Usuario " Lista ". Como nos acaba de empezar, es probable vacío. Para crear un nuevo par, haga clic en el botón.

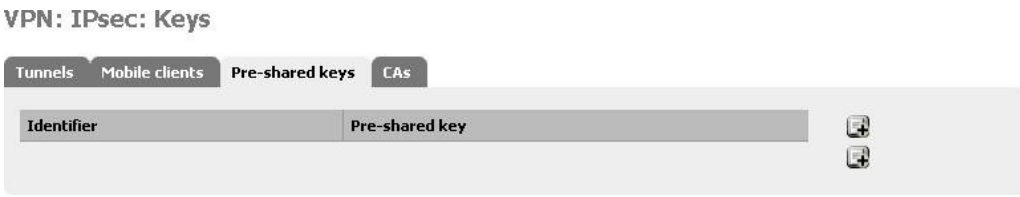


Figura 13.17. IPsec Pre-Shared Key "Usuario" Lista

Una pantalla con dos campos aparecerá. Uno para el identificador, y uno para la clave pre-compartida (Figura 13.18, "Adición de un Identificador / par de claves pre-compartidas"). En el primer cuadro, escriba un e-mail dirección para este cliente. No tiene que ser un verdadero, una dirección válida, basta con que se parecen a uno. Como se menciona en el resumen de VPN, IPSec mediante claves pre-compartidas se puede romper si una clave débil es utilizados. Utilice una clave fuerte, por lo menos 10 caracteres de longitud que contiene una mezcla de mayúsculas y minúsculas
letras, números y símbolos. Haga clic en Guardar cuando haya terminado.

Figura 13.18. Adición de un Identificador / par de claves pre-compartidas

Al igual que con la configuración del túnel, después de la modificación de las configuraciones principales, los cambios deben aplicarse. La

Identificador y una clave pre-compartida acaba de crear también deben figurar en esta pantalla. Si hay más Identificador pares PSK agregar, haga clic y repita el paso anterior. De lo contrario, haga clic en Aplicar cambios para completar la configuración de IPsec (Figura 13.19, "Aplicar los cambios; Lista PSK").

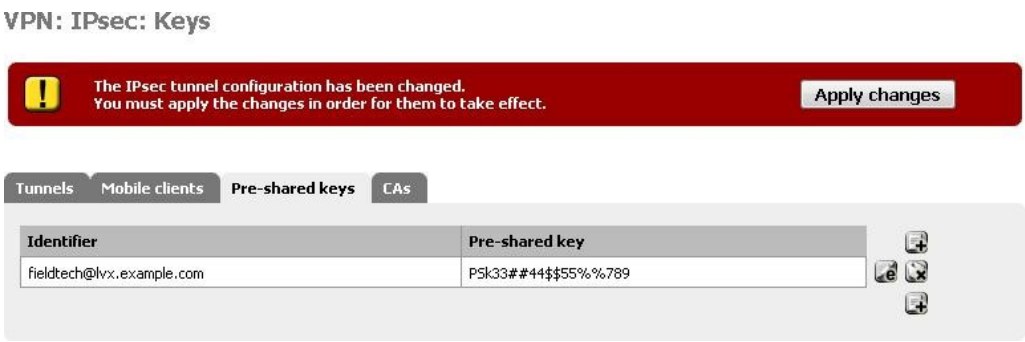


Figura 13.19. Aplicar los cambios; Lista PSK

13.5.1.3. Reglas de cortafuegos

Al igual que con los túneles estáticos de sitio a sitio, túneles móviles también necesitan reglas de firewall añadido a la

IPsec en Firewall de ficha → Normas. En este caso, el origen del tráfico sería la subred que ha elegido para los clientes móviles (o las direcciones de sus redes a distancia), y el destino será su red LAN. Para más detalles, Sección 13.3, "IPsec y las reglas del cortafuegos".

13.5.2. Ejemplo de configuración del cliente

Cada equipo de cliente móvil tendrá que ejecutar algún tipo de software de cliente IPSec. Hay muchos clientes diferentes IPsec disponibles para su uso, algunos gratuitos, y algunas aplicaciones comerciales. Normalmente, IPSec es un protocolo bastante interoperables en lo que respecta a los túneles de enrutador a enrutador, pero programas de cliente han demostrado ser más voluble, o, a veces incorporan extensiones propietarias que son no es compatible con las implementaciones de IPsec basada en estándares. Como se mencionó antes, el Cisco cliente IPSec incluye con el iPhone y el iPod Touch no es compatible con pfSense IPsec, y el cliente siempre para la conexión a Watchguard cajas de fuego ha visto resultados mixtos también.

13.5.2.1. Domada suave de cliente para Windows

La musaraña suave VPN Client es una sólida opción para el uso de IPSec en Windows. No sólo es fácil de usar y fiable, pero también está disponible totalmente gratis. Visita http://www.shrew.net y descargar la última versión del cliente domada suave para su plataforma. Ejecuta el instalador, y haga clic en Siguiente o Continuar a través de todas las indicaciones.

Inicio domada suave cliente haciendo clic en el icono de Access Manager. La pantalla principal debe aparecer, y se parecen Figura 13.20, "domada Administrador suave VPN de acceso - Sin embargo Conexiones". A continuación, haga clic en el botón Agregar para comenzar a configurar una nueva conexión.

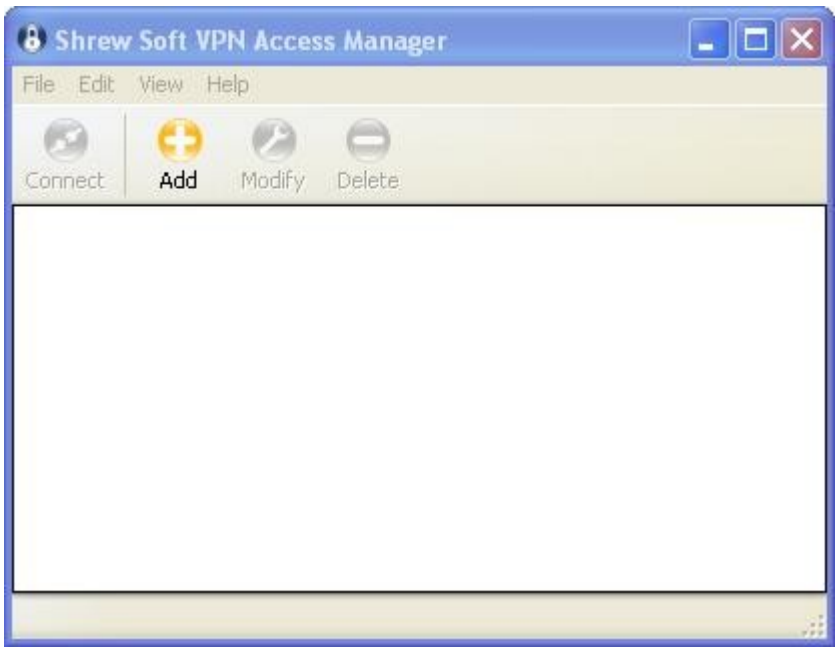


Figura 13.20. Domada VPN suave Access Manager - Sin conexiones Sin embargo,

La ventana de configuración de VPN de sitio debe abrir, con varias pestañas como en la figura 13.21, el

"Cliente

Configuración: Ficha General ". Se debe comenzar en la ficha General. A continuación, entrar en el host como el pfSense Caja IP WAN, o la dirección IP de la interfaz pfSense elegido previamente para utilizar IPsec. En nuestro ejemplo, **172.23.1.3**. El puerto debe ser **500**. Configuración automática debe ser **Personas de movilidad reducida**. Para el método de dirección, cambio que a **El uso del adaptador virtual y se les asignará dirección**. En el campo dirección, elija una de IP del rango que decidirse antes. Usaremos *192.168.111.5*, Con una máscara de red de *255.255.255.0*. Alternativamente, si lo que desea es pasar a través de la IP del cliente sin especificar uno específico de IPsec, en el método de direcciones cuadro, seleccione **Utilice un adaptador existente y la dirección actual**.

Los cambios no pueden ser necesarios en la ficha de cliente. Los valores por defecto debería estar bien, pero se puede comparar con la Figura 13.22, "Configuración del cliente: El cliente Tab" para asegurarse de que coinciden con los por defecto en el momento presente se está escribiendo.

En la ficha de resolución de nombres, desactive la opción Activar WINS (Windows Internet Name Service) y desactive la opción Activar DNS. Usted puede experimentar con estas opciones en lo que respecta a su configuración propia,
pero en este ejemplo vamos a dejarlos fuera. Vea la Figura 13.23, "Configuración del cliente: la resolución de nombres Tab "para ver ejemplos. En entornos en los que un servidor WINS puede estar presente, usted puede entrar en el

dirección IP aquí para un servidor accesible a través de este túnel, para ayudar en la resolución de nombres NetBIOS y navegar por la red remota. Adición de servidores DNS aquí no funcionen como se esperaba con Muchos ISP. Normalmente, los servidores DNS para clientes IPSec se utilizan como último recurso. Si un nombre no se resuelve a través de servidores normales del cliente DNS, los servidores adicionales pueden ser utilizados. Desafortunadamente, muchos ISP son "amablemente" que prestan servicios que resolver cualquier inexistente dominios de una página de destino lleno de publicidad. En este escenario, los nombres irresoluble nunca suceder y por lo tanto servidores adicionales no serán utilizados. Utilice esta opción con cautela, y la prueba por primera vez
antes de usarlo en los clientes en la naturaleza.

Figura 13.24. Configuración del cliente: Autenticación, Identidad Local

La ficha Autenticación tiene tres sub-pestañas de configuración que necesitan también. En primer lugar, establecer la autenticación
Método para **Mutua PSK** en la parte superior, a continuación, continúe con la ficha de identidad local por debajo, se muestra
en Figura 13.24, "Configuración del cliente: Autenticación, Identidad Local". Establecer el tipo de identificación a **Identificador de clave**, Y la clave ID de cadena a uno de los identificadores de estilo de correo electrónico que fue creado anteriormente para un cliente móvil.

Haga clic en la ficha Identidad remoto (Figura 13.25, "Configuración del cliente: Autenticación, Identidad remoto").
Establecer el tipo de identificación a **Dirección IP**Y de verificación Usar una dirección descubierto host remoto.

En la ficha de Verificación de Poderes, que se muestra en la Figura 13.26, "Configuración del cliente: Autenticación, Verificación de Poderes", llene
en el campo de Pre-Shared Key con la tecla que va junto con la dirección de correo electrónico introducido como Clave ID de cadena en la ficha de identidad local.

Ahora vuelve a la fase 1 de la ficha Inicio, ve en la Figura 13.27, "Configuración del cliente: Fase 1". Estos ajustes coincidirán con los establecidos en la fase del túnel servidor una sección. Establecer el tipo de cambio de agresivos, La Bolsa de DH **Grupo 2**, El algoritmo de cifrado para **3DES**, Algoritmo de hash a **SHA1**, Y la clave de la vida Límite para la **86400**.

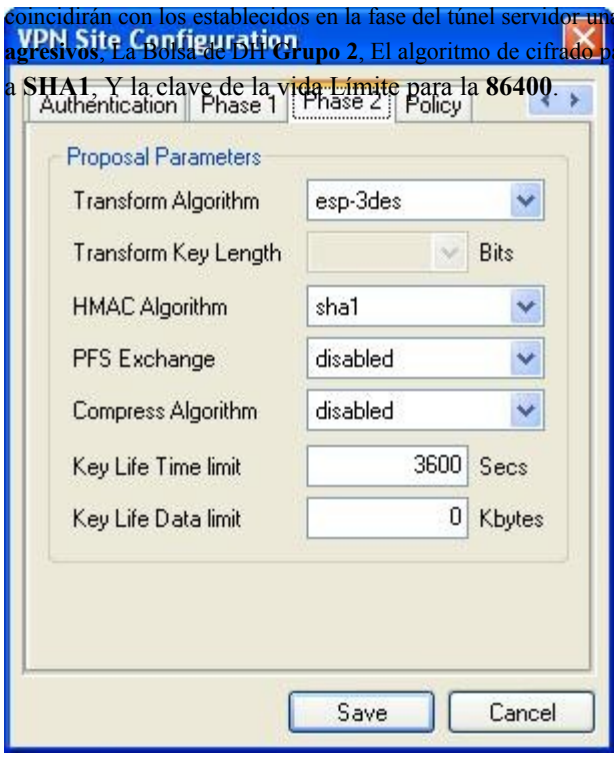


Figura 13.28. Configuración del cliente: Fase 2

La configuración de la Fase 2 ficha también serán los mismos que los establecidos en los clientes móviles Fase 2 sección, como puede verse en Figura 13.28, "Configuración del cliente: Fase 2". Establezca la Transformación

Algoritmo para **esp-3des**, El algoritmo HMAC es **SHA1**, PFS es **con discapacidad**, El algoritmo de compresión
es **con discapacidad**, Y la clave de la vida límite de tiempo es **3600**.

Por último, está la ficha Directiva, que se muestra en la Figura 13.29, "Configuración del cliente: Política". Controla lo que tráfico será enviado en el túnel. Desactive la opción Obtener Topología automáticamente, haga clic en Agregar botón.

En la pantalla de entrada de topología, se ve en la Figura 13.30, "Configuración del cliente: Políticas, Añadir Topología", que
necesidad de especificar qué subred estará en el otro extremo del túnel. Establecer el tipo de **Incluir**.
Para la dirección, entrar en la red detrás de pfSense en el otro lado, y la máscara de red que va
junto con él. Para nuestro ejemplo, que se **192.168.1.0** y **255.255.255.0** , respectivamente.
Haga clic en Aceptar.

Al hacer clic en Guardar, se le llevará de nuevo a la pantalla principal del cliente domada suave, y
usted tiene la oportunidad de cambiar el nombre de la conexión, como en la Figura 13.31, "Configuración del cliente: Nuevo Nombre de conexión ".

Es una buena idea para el nombre de la conexión después de la ubicación en la que se conecta. En este caso,
la llamó después de la oficina donde el túnel lleva como figura 13.32, "listo para usar la conexión" muestra.

Para conectarse a la VPN, haga clic una vez para seleccionarlo y, a continuación, haga clic en Conectar. La conexión VPN de diálogo van a aparecer y, a continuación, haga clic en el botón Conectar en allí también. Si el túnel está correctamente establecido, se indicará en la ventana. Figura 13.33, "Túnel Conectado" muestra la
salida de una conexión exitosa.

Figura 13.33. Conectado túnel

Ahora debería ser capaz de ponerte en contacto con los sistemas en el otro extremo del túnel. Si no ha salido bien o pasar el tráfico, vuelva a comprobar todas las opciones de ambos lados, ya que figuran en esta lista. De lo contrario, continúe con la sección de solución de problemas.

13.5.2.2. TheGreenBow IPSec de cliente

TheGreenBow IPSec Client es un comercial de cliente VPN para Windows que es compatible con pfSense. Las instrucciones para configurar este cliente con pfSense se puede encontrar en el VPN puerta de enlace de apoyo [http://www.thegreenbow.com/vpn_gateway.html] En la sección de su sitio web. Para obtener más información sobre la adquisición y configuración del cliente, visite su página web [http://www.thegreenbow.com]. Ellos ofrecen una prueba gratuita de 30 días del cliente para aquellos que buscan evaluar como una posible solución.

13.5.2.3. PNC cliente Entrada segura

La Secure Entry Client por NCP [http://www.ncp-e.com/en/solutions/vpn-products/secure-entrada client.html] Es otro cliente comercial IPsec para Windows, Windows Mobile, y Symbian. Como es compatible con los estándares, sino que también puede conectarse a los sistemas de pfSense.

13.5.2.4. SSH Centinela

SSH Sentinel es otro cliente de IPSec compatible con los estándares de Windows. Aunque Centinela SSH funciona con pfSense, su configuración es bastante complejo y el cliente libre disponible es de siete años de edad, después de haber sido puesto en libertad en 2002. Debido a estos factores, no se recomienda su uso, y el cliente domada suave se debe utilizar en su lugar.

13.5.2.5. IPSecuritas

IPSecuritas por Software Lobotomo [http://www.lobotomo.com/products/IPSecuritas/] Es un freeware cliente Mac OS X para IPsec que algunos usuarios han informado de trabajar con pfSense.

13.5.2.6. Los clientes de Linux

Hay algunos clientes Linux libremente disponibles, pero varían entre las distribuciones. Algunos son sólo interfaces con otros servicios como ipsec-tools, Pero debería funcionar siempre y cuando el cliente configuraciones son similares a la que se ha demostrado anteriormente.

13.5.2.7. Cisco VPN Client

El cliente VPN de Cisco no funciona actualmente con pfSense, ya que requiere de apoyo xauth. Esto debería funcionar con pfSense 2.0, sin embargo, desde xauth se encuentra allí.

13.6. Pruebas de conectividad IPsec

La prueba más fácil para un túnel IPsec es un ping de la estación de cliente que está detrás del router a otro en el lado opuesto. Si esto funciona, el túnel está en marcha y funcionando correctamente.

Como se menciona en Sección 13.4.4, "pfSense-inició tráfico e IPsec", tráfico iniciado desde pfSense normalmente no atraviesan el túnel sin un extra de enrutamiento, pero hay una rápida manera de probar la conexión desde la consola del router mediante el comando ping, mientras que la especificación de un dirección de origen con el `-S` parámetro. Sin utilizar `-S` o una ruta estática, los paquetes generados por el ping no tratará de atravesar el túnel. Esta sería la sintaxis para usar con una prueba apropiada:

#ping-S *<IP LAN Local> <IP remota LAN>*

Cuando el `IP LAN Local` es una dirección IP en una interfaz interna dentro de la subred local definición para el túnel, y la `IP remota LAN` es una dirección IP en el router remoto en el subred remota lista para el túnel. En la mayoría de los casos esto es simplemente la dirección IP de la LAN de la

respectivos routers pfSense. Teniendo en cuenta el ejemplo de sitio a sitio más arriba, esto es lo que tendría que escribir
para poner a prueba desde la consola del Sitio Un router:

#ping-S 192.168.1.1 10.0.10.1

Usted debe recibir respuestas de ping a la dirección LAN del sitio B, si el túnel está en marcha y de trabajo correctamente. Si usted no recibe respuestas, pase a la sección de solución de problemas (Sección 13.8, "Solución de problemas de IPsec").

13.7. IPsec y NAT-T

IPsec NAT-T encapsula el tráfico de protocolo ESP en el interior del puerto UDP 4500 el tráfico, porque ESP
con frecuencia causa dificultades cuando se utiliza en combinación con NAT. soporte de NAT-T se añadió durante un tiempo en pfSense 1.2.3, excepto que sacó errores en el subyacente ipsec-herramientas de software que las regresiones causado. Una regresión importante fue que la renegociación con algunos terceros IPsec dispositivos sería un fracaso. Después de considerables esfuerzos para solucionar el problema, soporte de NAT-T se tiró a eliminar las regresiones y recibe 1.2.3 liberado. Una instantánea 1.2.3-RC2 con NAT-T está disponible
para aquellos que deseen utilizarla, con la advertencia de que puede causar problemas de renegociación.

13.8. IPsec Solución de problemas

Debido a la naturaleza meticuloso de IPsec, no es raro que los problemas que surjan. Afortunadamente hay algunos básico (y algunas no tan básicas) pasos para solucionar problemas que se pueden emplear para rastrear a potenciales los problemas.

13.8.1. Túnel no establece

La causa más común de fracaso de las conexiones de túnel IPsec es una falta de coincidencia de configuración.
A menudo es algo pequeño, como un grupo DH establece en 1 en el lado A y 2 en la cara B, o tal vez una máscara de subred / 24, por un lado y 32 en el otro. Algunos routers (Linksys, por ejemplo) también les gusta esconderse detrás de ciertas opciones "avanzadas" botones o hacer suposiciones. Una gran cantidad de pruebas y error puede estar involucrado, y mucho de la lectura de registro, pero garantizando que ambas partes coinciden precisamente
ayudará a la mayoría.
Dependiendo de las conexiones a Internet en cada extremo del túnel, también es posible (especialmente con los clientes móviles) que un router que participan en un lado o el otro no controla correctamente IPsec el tráfico, sobre todo cuando se trata de NAT. Los problemas son en general con el protocolo ESP.
NAT Traversal (NAT-T) encapsula ESP en el puerto UDP 4500 para obtener el tráfico en torno a estas cuestiones, pero no está actualmente disponible en pfSense.

En el caso de un tiempo de espera de un cliente móvil, en primer lugar compruebe el estado del servicio en el Estado → Servicios.

Si se detiene el servicio, vuelva a comprobar que Permitir a los clientes móviles se comprueba en VPN → IPsec,

Clientes móviles ficha. Si el servicio está en ejecución, compruebe los registros del cortafuegos (Estado → Registros del sistema,

ficha Firewall) para ver si la conexión está siendo bloqueada, y si es así, agregue una regla para permitir el bloqueo tráfico.

13.8.2. Túnel establece, pero no pasa el tráfico

El principal sospechoso si aparece un túnel, pero no pasará el tráfico se las reglas del firewall IPsec.

Si usted está en un sitio y no puede llegar a sitio B, visita el sitio B router. Por el contrario, si usted está en Sitio B y no puede comunicarse con el sitio A, visita del sitio A. Antes de examinar las normas, asegúrese de revisar la los registros del firewall que se encuentran en estado → Registros del sistema, en la pestaña Firewall. Si usted ve bloqueado las entradas

participación de las subredes utilizadas en el túnel IPsec, a continuación, pasar al control de las normas. Si hay no hay entradas de registro que indica paquetes bloqueados, revisar la sección sobre IPsec enrutamiento consideraciones en Sección 13.4.2, "Enrutamiento y consideraciones puerta de entrada".

paquetes bloqueados en el IPsec o `enc0` interfaz de indicar que el túnel se ha establecido pero el tráfico está siendo bloqueado por las reglas en la interfaz IPsec. paquetes bloqueados en la LAN o de otro tipo interfaz interna puede indicar que una regla adicional puede ser necesaria en conjunto de reglas que la interfaz de permitir el tráfico de la subred interna hacia el extremo remoto del túnel IPSec. paquetes bloqueados en la WAN o interfaces WAN OPT impediría un túnel desde el establecimiento. Normalmente esto sólo sucede cuando el automático reglas VPN están deshabilitadas. Adición de una regla para permitir el protocolo ESP y el puerto UDP 500 desde que dirección IP remota debe permitir que el túnel de establecer. En el caso de túneles móviles, tendrá que permitir el tráfico de cualquier fuente para conectar a los puertos.

Reglas para la interfaz IPsec se puede encontrar en firewall → Reglamento, en la ficha de IPsec. Común errores incluyen el establecimiento de una regla para permitir sólo el tráfico TCP, lo que significa cosas como ICMP ping y DNS no funcionaría a través del túnel. Ver Capítulo 6, Servidor de seguridad Para obtener más información sobre cómo crear correctamente y solucionar problemas de reglas de firewall.

En algunos casos también puede ser posible que un desajuste ajuste también podría causar tráfico a fallar pasa por el túnel. En una ocasión, vi a una subred definida en un router no pfSense como 192.168.1.1/24, y en el lado pfSense se 192.168.1.0/24. El túnel establecido, pero el tráfico no pasaría hasta que la subred se corrigió.

También podría haber un problema con la forma en que los paquetes están siendo derrotados. Ejecución de un traceroute (tracert

en Windows) a una dirección IP en el lado opuesto del túnel puede ser esclarecedor. Repita la prueba de ambos lados del túnel. Verifica en el Sección 13.4.2, "Enrutamiento y puerta de enlace de las consideraciones" sección de este capítulo para obtener más información. Cuando se utiliza traceroute, verá que el tráfico que hace entrar y salir del túnel IPsec parece que faltan algunos saltos intermedios. Esto es

normal, y parte de cómo funciona IPSec. Tráfico que no tiene debidamente en entrar en un túnel IPsec parecen salir de la interfaz WAN y la ruta hacia el exterior a través de Internet, lo que apuntaría a ya sea un problema de enrutamiento como pfSense no ser la puerta de enlace (como en Sección 13.4.2, "Enrutamiento y consideraciones puerta de entrada "), Una subred incorrecta remoto especificado en la definición del túnel, o un túnel que se ha desactivado.

13.8.3. Hay algunos equipos en el trabajo, pero no todos

Si el tráfico entre máquinas sobre las funciones de VPN correctamente, pero algunos hosts no, esto es normalmente una de las cuatro cosas.

1. Falta, puerta de enlace predeterminada incorrecta o ignorado - Si el dispositivo no tiene un valor predeterminado puerta de enlace, o tiene uno que apunta a algo distinto de pfSense, no sabe cómo adecuadamente volver a la red remota en la VPN (ver Sección 13.4.2, "Enrutamiento y consideraciones puerta de entrada "). Algunos dispositivos, incluso con una puerta de enlace predeterminada se especifica, no utilice que la puerta de enlace. Esto se ha visto en varios dispositivos integrados, incluyendo cámaras IP y algunas impresoras. No hay nada que podamos hacer al respecto que, aparte de conseguir el software en el dispositivo fijo. Usted puede verificar esto ejecutando tcpdump en la interfaz interna del servidor de seguridad conectado a la red que contiene el dispositivo. Solución de problemas con tcpdump se trata en Sección 25.5, "Uso de tcpdump de la línea de comandos", Y un ejemplo IPsec específica puede se encuentra en Sección 25.5.3.2, "túnel IPSec no se conecta". Si usted ve el tráfico que va de la dentro de la interfaz en el servidor de seguridad, pero no las respuestas que vienen atrás, el dispositivo no está bien de enrutamiento el tráfico de respuesta (o podría ser que el bloqueo a través de un servidor de seguridad).
2. Máscara de subred incorrecta - Si la subred en uso en un extremo es 10.0.0.0/24 y el otro es 10.254.0.0/24, y un host tiene una máscara de subred incorrecta de 255.0.0.0 o / 8, que nunca será capaz de comunicarse a través de la VPN, ya que piensa que la subred remota VPN es parte de los locales enrutamiento de red y por lo tanto no funcionará correctamente.
3. Servidor de seguridad - si hay un firewall en el host de destino, puede que no sea permitir las conexiones.
4. Las reglas de firewall en pfSense - garantizar las reglas en ambos extremos permiten el tráfico de red deseada.

13.8.4. Se bloquea la conexión

Históricamente, IPsec no ha manejado con gracia paquetes fragmentados. Muchas de estas cuestiones han ha resuelto en los últimos años, pero puede haber algunos problemas persistentes. Si se bloquea o el paquete pérdida sólo se ven cuando se utiliza protocolos específicos (SMB, RDP, etc), la MTU WAN puede necesitar reducido. Una reducción de MTU se asegurará de que los paquetes que pasan por el túnel son de un tamaño que se puede transmitir todo. Un buen punto de partida sería 1300, y si funciona lentamente aumento la MTU hasta encontrar el punto de ruptura, a continuación, retroceder un poco de allá.

13.8.5. "Random" Túnel Desconecta / Fallas DPD en Routers integrados

Si usted experimenta caído túneles IPsec en un ALIX u otro hardware integrado, es posible que necesidad de desactivar el DPD en el túnel. Usted puede ser capaz de correlacionar los fracasos a los tiempos de alta ancho de banda de uso. Esto sucede cuando la CPU en un sistema de bajo consumo de energía está vinculada con el envío de tráfico IPsec o de otro modo ocupados. Debido a la sobrecarga de la CPU no puede tomar el tiempo para responder a solicitudes de DPD o ver una respuesta a una petición propia. Como consecuencia, el túnel dejará un cheque DPD y desconectarse.

13.8.6. IPsec Interpretación registro

El IPsec registros disponibles en estado → Registros del sistema, en la ficha IPsec contendrá un registro de el proceso de conexión del túnel. En esta sección, vamos a demostrar algunas de las entradas de registro típica, tanto buenas como malas. Los elementos principales que hay que buscar son las frases más importantes que indican que parte de una
conexión efectivamente trabajadas. Si ve "ISAKMP-SA establecido", eso significa que la fase 1 se completado con éxito y una Asociación de Seguridad fue negociado. Si "IPsec SA establecido" es visto, a continuación, la Fase 2 también ha sido completado y el túnel debería estar listo y trabajando en ese punto.

En los ejemplos siguientes, el túnel se inicia desde el sitio A.

13.8.6.1. Conexiones con éxito

Estos son ejemplos de los túneles de éxito, tanto en el modo principal y agresivo.

13.8.6.1.1. Túnel con éxito el modo principal

Registro de salida desde el sitio A:

```
[ToSiteB]: INFO: solicitud IPsec SA para 172.16.3.41 en cola debido a que
no se encuentran fase 1.

INFORMACIÓN: comenzar el modo de protección de identidad.
INFORMACIÓN: recibió Vendor ID: DPD
INFORMACIÓN: recibió roto Microsoft ID: FRAGMENTACIÓN
```

Registro de resultados de sitio B:

```
INFORMACIÓN: comenzar el modo de protección de identidad.
INFORMACIÓN: recibió roto Microsoft ID: FRAGMENTACIÓN
INFORMACIÓN: recibió Vendor ID: DPD
```

13.8.6.1.2. Túnel con éxito el modo agresivo

Registro de salida desde el sitio A:

```
[ToSiteB]: INFO: solicitud IPsec SA para 172.16.3.41 en cola debido a que
no se encuentran fase 1.

INFORMACIÓN: iniciar el modo agresivo.
INFORMACIÓN: recibió roto Microsoft ID: FRAGMENTACIÓN
INFORMACIÓN: recibió Vendor ID: DPD
NOTIFICACIÓN: no pudo encontrar el pskey adecuada, tratar de conseguir uno
por la dirección del otro extremo.
```

Registro de resultados de sitio B:

```
INFORMACIÓN: iniciar el modo agresivo.
INFORMACIÓN: recibió roto Microsoft ID: FRAGMENTACIÓN
INFORMACIÓN: recibió Vendor ID: DPD
NOTIFICACIÓN: no pudo encontrar el pskey adecuada, tratar de conseguir uno
por la dirección del otro extremo.
```

13.8.6.2. Ejemplos Error de conexión

Estos ejemplos muestran las conexiones no por varias razones. En particular, las partes interesantes de las entradas del registro se hará hincapié.

13.8.6.2.1. Conflicto de la Fase 1 de cifrado

Registro de salida desde el sitio A:

```
[ToSiteB]: INFO: solicitud IPsec SA para 172.16.3.41 en cola debido a que
no se encuentran fase 1.

INFORMACIÓN: comenzar el modo de protección de identidad.

INFORMACIÓN: eliminar la fase 2 del controlador.
ERROR: fase 1 de negociación fracasó por falta de tiempo para arriba.
96f516ded84edfca: 0000000000000000
```

Registro de resultados de sitio B:

```
INFORMACIÓN: comenzar el modo de protección de identidad.
INFORMACIÓN: recibió roto Microsoft ID: FRAGMENTACIÓN
INFORMACIÓN: recibió Vendor ID: DPD
```

ERROR: rechazada enctype: DB (apoyo n º 1: RRT # 1): Intercambio (apoyo n º 1: RRT # 1) = 3DES-CBC: AES-CBC

```
ERROR: no hay propuestas adecuadas que se encuentran.
ERROR: No se pudo obtener propuesta válida.
ERROR: no se pudo paquete pre-proceso.
ERROR: fase 1 de negociación fracasó.
```

En este caso, la entrada de registro que dice exactamente cuál era el problema: Este lado se fijó para el 3DES encriptación, y el lado remoto se ha establecido para AES. Establecer tanto para valores coincidentes y vuelva a intentarlo.

13.8.6.2.2. Conflicto de la Fase 1 Grupo de DH

En este caso, las entradas del registro será exactamente como el anterior, excepto que la línea se hizo hincapié en en lugar de:

Este error se puede corregir mediante la creación del grupo DH configuración en ambos extremos del túnel a una
correspondiente valor.

13.8.6.2.3. Conflicto de Pre-shared Key

Una de las claves no coinciden pre-compartida puede ser un poco más difícil de diagnosticar. Un error que indica el hecho de que
este valor no coincide no se imprime en el registro, en lugar podrás ver un mensaje como este:

```
[ToSiteB]: NOTIFICACIÓN: el paquete es retransmitido por 172.16.3.41 [500]
(1).
```

Si detecta un error similar al anterior, compruebe que las claves pre-compartidas coinciden en ambos extremos.

13.8.6.2.4. Conflicto de la Fase 2 de cifrado

Registro de salida desde el sitio A:

```
[ToSiteB]: INFO: solicitud IPsec SA para 172.16.3.41 en cola debido a que no se
encuentran fase 1.

INFORMACIÓN: comenzar el modo de protección de identidad.
INFORMACIÓN: recibió Vendor ID: DPD
INFORMACIÓN: recibió roto Microsoft ID: FRAGMENTACIÓN
```

ERROR: fatal NO-PROPUESTA-ELEGIDO mensaje de notificación, fase 1 debe ser eliminado.

Registro de resultados de sitio B:

```
INFORMACIÓN: comenzar el modo de protección de identidad.
INFORMACIÓN: recibió roto Microsoft ID: FRAGMENTACIÓN
INFORMACIÓN: recibió Vendor ID: DPD
```

ADVERTENCIA: pares AES:: trns_id coincidentes: mi 3DES
ERROR: no se repite
ERROR: no existe una política adecuada que se encuentran.
ERROR: no se pudo paquete pre-proceso.

En estas entradas de registro, se puede ver que la Fase 1 completó con éxito ("ISAKMP-SA establecido "), pero no durante la Fase 2. Por otra parte, afirma que no pudo encontrar un adecuado propuesta, y desde el sitio B registros podemos ver que esto se debió a los sitios que se establece para los diferentes
tipos de cifrado, AES, por un lado y 3DES por el otro.

13.8.6.2.5. Otra Fase 2 no coincidentes de Información

Algunos otros Fase 2 errores como los valores no coinciden o no coinciden PFS subredes remotas dar lugar a la salida del registro mismo. En este caso, hay pocos recursos, pero para ver cada opción de garantizar la configuración de coincidir en ambos lados.

Registro de salida desde el sitio A:

```
[ToSiteB]: INFO: solicitud IPsec SA para 172.16.3.41 en cola debido a que
no se encuentran fase 1.

INFORMACIÓN: comenzar el modo de protección de identidad.
INFORMACIÓN: recibió Vendor ID: DPD
INFORMACIÓN: recibió roto Microsoft ID: FRAGMENTACIÓN


[ToSiteB]: ERROR: 172.16.3.41 renunciar a conseguir IPsec SA por falta de
tiempo hasta que esperar.
```

Registro de resultados de sitio B:

```
INFORMACIÓN: comenzar el modo de protección de identidad.
INFORMACIÓN: recibió roto Microsoft ID: FRAGMENTACIÓN
INFORMACIÓN: recibió Vendor ID: DPD


ERROR: no existe una política que se encuentran: 192.168.30.0/24 [0] 192.168.32.0/24 [0] = cualquier
proto dir = en
ERROR: No se pudo obtener propuesta de respuesta.
ERROR: no se pudo paquete pre-proceso.
```

Los errores indican que las propuestas para la fase 2 no estuvo de acuerdo, y todos los valores en la Fase 2 sección debe ser revisado, así como las definiciones de subred remota.

Nota

En algunos casos, si una parte ha establecido en SLP **fuera**, Y el otro lado tiene un conjunto de valores,
el túnel todavía establecer y trabajo. El desajuste se muestra más arriba sólo se puede ver si el desajuste valores, por ejemplo **1** vs **5**.

13.8.6.3. Otros errores comunes

Algunos mensajes de error se pueden encontrar en el registro de IPsec. Algunas son inofensivas, y son los demás indicativos de posibles problemas. Por lo general, los mensajes de registro son bastante sencillas en su significado,

e indicar los diversos problemas que se establece un túnel con razones por qué. Hay algunos, sin embargo, que son un poco más oscuro.

```
20 de febrero racoon 10:33:41: Error: Error al paquete de pre-proceso.
20 de febrero 10:33:41 racoon: ERROR: No se pudo obtener sainfo.
```

Esto es más frecuente cuando las definiciones de subred local y / o remoto de forma incorrecta especificadas, especialmente si la máscara de subred se establece incorrectamente en un lado.

```
racoon: ERROR: El mensaje no debe ser encriptada.
```

Indica que puede haber un problema con el tráfico que llega desde el otro extremo del túnel.

Pruebe a reiniciar el servicio de mapache en el router lejos a tu lado por la navegación a Estado → Servicios y clic **Reinicie** junto al mapache.

```
racoon: ERROR: no puede iniciar el modo rápido, no hay ISAKMP-SA.
```

Puede indicar un problema con el envío de tráfico local en el túnel remoto, ya que un ISAKMP Asociación de Seguridad no se ha encontrado. Puede ser necesario reiniciar el servicio de racoon una o ambas partes a aclarar esto.

```
racoon: INFO: solicitud para el establecimiento de IPsec SA se puso en cola
debido a que no se encuentran fase 1.
```

Esto es normal, y generalmente se observa cuando un túnel se estableció por primera vez. El sistema intentará en primer lugar
completar una fase de una conexión con el otro lado y luego continuar.

```
racoon: INFO: no compatible PF_KEY mensaje REGISTRO
```

Esto no es dañino también, y se encuentra típicamente en el registro poco después de que comience el demonio racoon.

13.8.7. Avanzadas de depuración

Cuando la negociación está fallando, sobre todo cuando se conecta a dispositivos de terceros en los que IPsec no es tan fácil para que coincida con la configuración por completo entre las dos partes, a veces la única manera de
Para obtener información adecuada para resolver el problema consiste en ejecutar mapache en el primer plano de depuración
modo. Para ello, inicie sesión por primera vez en su firewall usando SSH y eligió la opción **8** en el menú de la consola
de un símbolo del sistema. Ejecutar los siguientes comandos.

#killall racoon

Ahora espera unos 5 segundos para el proceso de cerrar e iniciar de nuevo con el siguiente.

#racoon-F-d-v-f / var / etc / racoon.conf

La primera línea se detiene el proceso de racoon existentes. Se inicia el segundo racoon en primer plano (`-F`), Con la depuración (`-D`), El aumento de nivel de detalle (`-V`), Utilizando el archivo de configuración `/ Var / etc / racoon.conf` (`-F`). Correr en el primer plano hace que muestre sus registros en su SSH período de sesiones, para que pueda ver lo que está sucediendo en tiempo real. Para salir de mapache, pulse **Ctrl-C** y el servicio se interrumpirá. Después de terminar con la depuración, tendrá que empezar a racoon normalmente. La forma más sencilla de hacerlo es ver a Estado → Servicios en la interfaz web y haga clic en junto al mapache.

Nota

Este método de depuración es perjudicial para todos los IPsec en el sistema, cuando matar a racoon usted caerá todas las conexiones IPsec. Debido al volumen de registros que se tienen que ordenar a través de múltiples conexiones IPsec activa, mientras que depurar un problema con uno de ellos es más fácil si se puede desactivar los otros, mientras que solución de problemas. En general, este método de depuración se realiza sólo cuando se lleva una nueva conexión IPsec.

13.9. Configuración de dispositivos de terceros IPsec

Usted puede conectar cualquier dispositivo VPN de apoyo estándar IPsec con pfSense. Se está utilizando de la producción en combinación con equipos de numerosos vendedores ", y debería funcionar bien con cualquier dispositivo capaz de IPsec en la red. Dispositivos de conexión de dos proveedores diferentes puede ser un problema, independientemente de los vendedores involucrados debido a las diferencias de configuración entre los vendedores, en algunos casos errores en las implementaciones, y el hecho de que algunos de ellos utilizan extensiones propietarias. En esta sección se ofrece una orientación general sobre la configuración de IPsec VPN con equipos de terceros, así como ejemplos específicos sobre la configuración de cortafuegos Cisco PIX y IOS de los routers.

13.9.1. Orientaciones generales para dispositivos de terceros IPsec

Para configurar un túnel IPSec entre pfSense y un dispositivo de otro proveedor, el principal preocupación es garantizar que la fase de los parámetros 1 y 2 coinciden en ambos lados. Para la configuración opciones sobre pfSense, donde se le permite seleccionar múltiples opciones que debe seleccionar por lo general sólo una de esas opciones y asegurar el otro lado se encuentra el mismo. Los extremos deben negociar una opción compatible cuando se seleccionan varias opciones, sin embargo, que es con frecuencia una fuente de problemas cuando se conecta a dispositivos de terceros. Configurar los dos extremos de lo que usted cree son configuración de juego, y guardar y aplicar los cambios en ambos lados.

Una vez que usted cree que la configuración de partido en los dos extremos del túnel, intento de pasar el tráfico través de la VPN para activar su inicio, a continuación, ver sus registros de IPsec en ambos extremos para revisar la

negociación. Dependiendo de la situación, los registros de un extremo puede ser más útil que los desde el extremo opuesto, por lo que es bueno para comprobar y comparar ambas. Se encuentra el pfSense lado proporciona una mejor información en algunos casos, mientras que en otras ocasiones el otro dispositivo proporciona más útil de registro. Si la negociación fracasa, determinar si se trataba de la fase 1 o 2 que falló y bien revisar la configuración en consecuencia, como se describe en Sección 13.8, "IPsec Solución de problemas ".

13.9.2. Cisco PIX OS 6.x

La configuración siguiente sería para un Cisco PIX se ejecuta en 6.x como sitio B de la ejemplo de sitio a sitio de configuración en este capítulo. Ver Sección 13.4.1, "Sitio de ejemplo de sitio web configuración " Un sitio para la configuración de pfSense.

```
con sysopt permiso ipsec
ISAKMP habilitar fuera

! --- Fase 1
ISAKMP dirección de la identidad
ISAKMP una política de cifrado 3DES
ISAKMP política de un hash SHA
política de ISAKMP un grupo 2
ISAKMP política de un curso de la vida 86400
ISAKMP política de una autenticación previa al compartir


! --- Fase 2
cripto ipsec transformar-set 3dessha1 esp-3des-sha-esp hmac
PFSVPN lista de acceso IP permiten 10.0.10.0 255.255.255.0 192.168.1.0
255.255.255.0
Mapa cripto-dyn mapa 10 IPSec ISAKMP
mapa cifrado dyn-10 dirección mapa partido PFSVPN
cripto-mapa mapa din 10 que se pares 172.23.1.3
Mapa cripto-dyn mapa 10 que se transforman-set 3dessha1
mapa cifrado mapa dyn-10 que la asociación de seguridad-3600 segundo curso
de la vida
Mapa cripto-dyn mapa de interfaz fuera

! --- No nat-para asegurar las rutas a través del túnel
Nonat lista de acceso IP permiten 10.0.10.0 255.255.255.0 192.168.1.0
255.255.255.0
nat (interior) 0 Nonat lista de acceso
```

13.9.3. Cisco PIX OS 7.x, 8.x, y ASA

Configuración de las revisiones más recientes del sistema operativo para dispositivos PIX y ASA es similar a la de la
los más viejos, pero tiene algunas diferencias significativas. En el ejemplo siguiente sería para el uso de una PIX 7.xy corriendo OS o 8.x, o un dispositivo de ASA, como el sitio B en el ejemplo de sitio a sitio anterior en este capítulo. Ver Sección 13.4.1, "de la web a la configuración del sitio de ejemplo" para el correspondiente Una configuración del sitio.

```
ISAKMP cifrado permiten exterior

! --- Fase 1
cripto política ISAKMP 10
  autenticación previa al compartir
  Encriptación 3DES
  hash SHA
  el grupo 2
  86.400 de por vida

túnel grupo 172.23.1.3 tipo ipsec-L2L
túnel grupo 172.23.1.3 ipsec-atributos XyZ9 abc123 pre-compartida-clave% $
7qwErty99

! --- Fase 2
cripto ipsec transformar-set 3dessha1 esp-3des-sha-esp hmac

cripto outside_map mapa discurso del 20 de partido PFSVPN
mapa cifrado outside_map 20 pares conjunto 172.23.1.3
cripto outside_map mapa 20 establece transformar-set 3dessha1
mapa cifrado outside_map interfaz externa

! --- No nat-para asegurar las rutas a través del túnel

nat (interior) 0 Nonat lista de acceso
```

13.9.4. Cisco IOS de routers

Esto muestra un router de Cisco IOS basadas en el sitio B de la configuración de ejemplo de sitio a sitio anterior en el capítulo. Vea la sección Sección 13.4.1, "de la web a la configuración del sitio de ejemplo" para el sitio A configuración de pfSense.

```
! --- Fase 1
cripto política ISAKMP 10
  3des ENCR
  autenticación previa al compartir
```

```
  el grupo 2
ISAKMP criptografía de clave XyZ9 abc123% $ 7qwErty99 dirección 172.23.1.3
no xauth-

! --- Fase 2
access-list 100 permit 192.168.1.0 0.0.0.255 IP 10.0.10.0 0.0.0.255
access-list 100 IP permiten 10.0.10.0 192.168.1.0 0.0.0.255 0.0.0.255
cifrado 3DES IPSec transformar-set-SHA esp-3des-sha-esp hmac
mapa cifrado PFSVPN 15 IPSec ISAKMP
  conjunto de pares 172.23.1.3
  conjunto transformar-set 3DES-SHA
  coincidir con la dirección 100

! --- Asignar el mapa de cifrado para la interfaz WAN
interfaz FastEthernet0 / 0
  cripto mapa PFSVPN

! --- No Nat-por lo que este tráfico se realiza a través del túnel, no de
la WAN
ip nat dentro de la fuente FastEthernet0 interfaz de ruta, mapa Nonat / 0
sobrecarga
access-list 110 deny ip 192.168.1.0 0.0.0.255 0.0.0.255 10.0.10.0
lista de acceso IP 110 permite 10.0.10.0 0.0.0.255 cualquier
mapa de rutas Nonat permiso de 10
  coincidir con la dirección IP 110
```

Capítulo 14. PPTP VPN

pfSense puede actuar como un servidor PPTP VPN como una de sus tres opciones de VPN. Este es un atractivo opción ya que el cliente se construye en cada versión de Windows y OS X lanzado en el pasado década. También puede proporcionar los servicios de pasarela a un servidor interno de PPTP.

Para una discusión general de los distintos tipos de redes privadas virtuales disponibles en pfSense y sus pros y sus contras, ver Capítulo 12, Redes privadas virtuales.

14.1. PPTP Advertencia de seguridad

Si no lo ha hecho, usted debe leer Sección 12.2.7, "criptográficamente segura" sobre VPN la seguridad. PPTP se utiliza mucho, pero no es la solución de VPN más seguras disponibles.

14.2. PPTP y reglas de firewall

De forma predeterminada, cuando se tiene la redirección de PPTP o el servidor PPTP habilitado, reglas ocultas cortafuegos se añadirán automáticamente a la WAN para permitir el tráfico TCP 1723 y GRE de cualquier fuente para la dirección de destino. Puede desactivar este comportamiento en pfSense 1.2.3 y versiones posteriores de comprobación Deshabilitar todas las auto-agregó VPN cuadro de normas en Sistema → Avanzado. Es posible que desee hacer esto si usted conoce a sus clientes PPTP se conecta únicamente de determinadas redes remotas. Este evita posibles abusos de servidores de Internet arbitrarios, pero en las implementaciones de los usuarios son móviles y se conecta desde numerosos lugares, es imposible conocer todas las subredes los usuarios se procederá de lo que apriete el conjunto de reglas no es práctico y causar dificultades a los sus usuarios.

14.3. PPTP y Multi-WAN

Desafortunadamente debido a la forma PPTP obras, y la forma en PF funciona con el protocolo GRE, sólo es posible ejecutar un servidor PPTP en la interfaz WAN primaria

14.4. PPTP Limitaciones

El código de seguimiento del estado en el software de servidor de seguridad subyacentes PF para el protocolo GRE sólo puede el seguimiento de una sola sesión por IP pública por servidor externo. Esto significa que si usted utiliza PPTP VPN conexiones, sólo una máquina interna se pueden conectar simultáneamente a un servidor PPTP en la

De Internet. Un millar de máquinas se pueden conectar simultáneamente a un millar de diferentes servidores PPTP,
pero sólo una vez en un único servidor. El único trabajo disponible todo es de uso múltiple
IPs públicas en el cortafuegos, uno por cliente, o para usos múltiples IPs públicas en el exterior PPTP
servidor. Esto no es un problema con otros tipos de conexiones VPN.

Esta misma limitación también significa que si se habilita el servidor PPTP o la funcionalidad de redirección,
ningún cliente NAT a su dirección IP WAN se puede conectar a cualquier servidor fuera de PPTP.
El trabajo en torno a esto es NAT acceso de sus clientes de Internet de salida a un público distinto
dirección IP.

Estas dos limitaciones son capaces de ser trabajados en torno en la mayoría de entornos, sin embargo la fijación
esta es una gran prioridad para la versión 2.0 de pfSense. En el momento de escribir esto, el trabajo de desarrollo
que está sucediendo para eliminar esta limitación, aunque no se sabe si tendrá éxito.

14.5. Configuración del servidor PPTP

Para configurar el servidor PPTP, primero vaya a VPN → PPTP. Seleccione Habilitar el servidor PPTP.

14.5.1. Direccionamiento IP

Usted tendrá que decidir qué direcciones IP a utilizar para el servidor PPTP y clientes. La
rango de dirección a distancia es generalmente una parte de la subred LAN, como 192.168.1.128/28 (0.128
a través de 0.143). A continuación, seleccione una dirección IP fuera del rango de la dirección del servidor, tales como
192.168.1.144 como se muestra en Figura 14.1, "Direccionamiento IP PPTP".

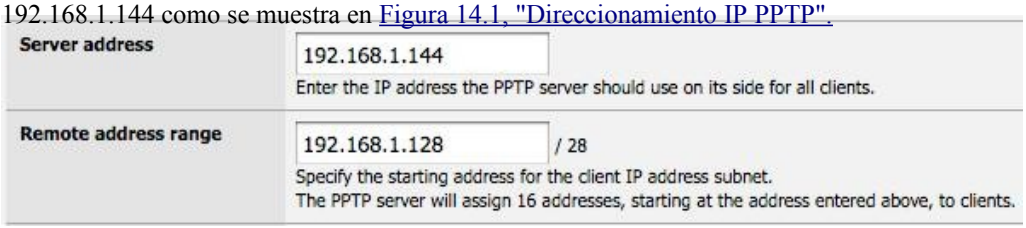


Figura 14.1. PPTP direccionamiento IP

Nota

Esta subred no tiene que estar contenido dentro de una subred existentes en el router.
Usted puede usar un conjunto completamente diferente de direcciones IP si se desea.

14.5.2. Autenticación

Usted puede autenticar a los usuarios de la base de datos de usuarios locales, oa través de RADIUS. RADIUS permite conectarse a otro servidor de su red para proporcionar autenticación. Esto puede ser usado para autenticar usuarios de PPTP de Microsoft Active Directory (véase Sección 24.1, "RADIUS Autenticación con Windows Server ") así como numerosos servidores RADIUS de otro tipo que puedan.

Si se usa RADIUS, consulte el uso de un servidor RADIUS para la autenticación y la caja de relleno en el Servidor RADIUS y el secreto compartido. Para la autenticación utilizando la base de datos de usuarios locales, deje que casilla sin marcar. Usted tendrá que agregar a los usuarios en la ficha de usuario de la VPN → PPTP pantalla a menos que utilice RADIUS. Ver Sección 14.5.6, "Añadir usuario" a continuación para obtener más detalles sobre la construcción- en el sistema de autenticación.

14.5.3. Requerir cifrado de 128 bits

Usted debe exigir el cifrado de 128 bits cuando sea posible. La mayoría de los clientes PPTP apoyo de 128 bits cifrado, por lo que este debe estar bien en la mayoría de entornos. PPTP es relativamente débil a 128 bits, y significativamente más que a los 40 y 56 bits. A menos que sea absolutamente necesario, nunca debe usar algo menos de 128 bits con PPTP.

14.5.4. Guardar los cambios para iniciar servidor PPTP

Después de completar los elementos antes mencionados, haga clic en Guardar. Esto guardará la configuración y poner en marcha el servidor PPTP. Si se autentifica a los usuarios con la base de datos de usuarios locales, haga clic en en la ficha Usuarios y entrar a los usuarios allí.

14.5.5. Configurar reglas de firewall para clientes PPTP

Vaya a Servidor de seguridad → Reglas y haga clic en la ficha PPTP VPN. Estas reglas de control de tráfico lo Se permite de clientes PPTP. Hasta que se agrega una regla de firewall aquí, todo el tráfico iniciado desde relacionada clientes PPTP se bloquearán. Tráfico inicia desde la LAN a los clientes PPTP controla mediante las reglas de firewall LAN. Al principio es posible que desee agregar una regla que todos los aquí para propósitos de prueba como se muestra en Figura 14.2, "las reglas de firewall VPN PPTP", y una vez que compruebe funcionalidad, restringir el conjunto de reglas a su gusto.

Figura 14.2. PPTP VPN Firewall de Regla

14.5.6. Adición de usuarios

Adición de usuarios a través de RADIUS puede variar de una aplicación a otra. Este hecho hace más allá del alcance de esta sección, sino que debe ser cubierto en la documentación de la particular servidor RADIUS que es empleado.

Adición de usuarios a pfSense incorporado en PPTP sistema de usuarios es muy fácil. En primer lugar, haga clic en VPN → PPTP,
y luego en la pestaña Usuarios. Se le presentará con una pantalla de usuarios vacía como se muestra en Figura 14.3, "Los usuarios de PPTP Tab". Haga clic en el botón para añadir un usuario.

Figura 14.3. PPTP usuario Tab

Después de hacer clic, la página de edición de usuario aparecerá. Rellenarlo con el nombre de usuario y contraseña para un usuario, como en Figura 14.4, "Adición de un usuario PPTP". También podrán participar en una asignación de IP estática
si lo desea.

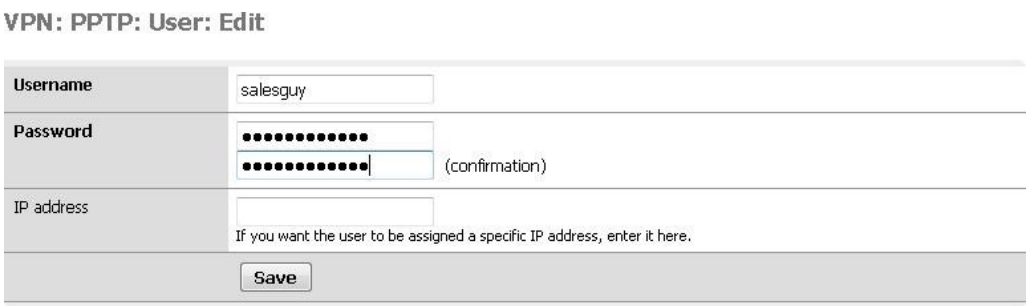


Figura 14.4. Adición de un usuario PPTP

Haga clic en Guardar y, a continuación la lista de usuarios retorno (Figura 14.5, "Aplicar los cambios PPTP"),

Pero antes de
el cambio entrará en vigor, el botón Aplicar cambios primero hay que hacer clic.

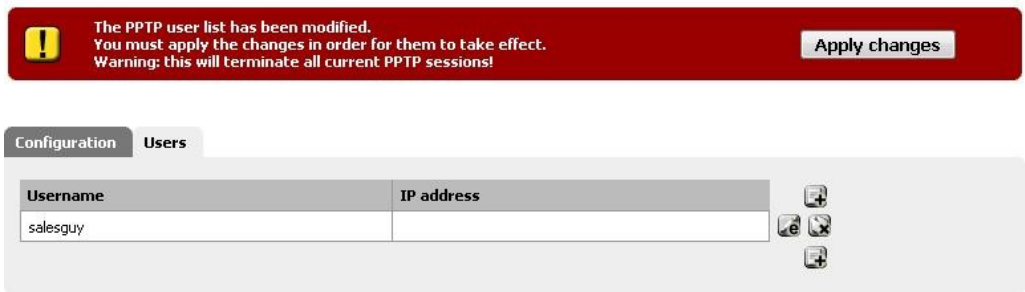


Figura 14.5. Aplicar los cambios PPTP

Repita este proceso para cada usuario que desea agregar, finalmente tendrá un lugar lleno
mirando la lista de usuarios, como en Figura 14.6, "Lista de Usuarios PPTP".

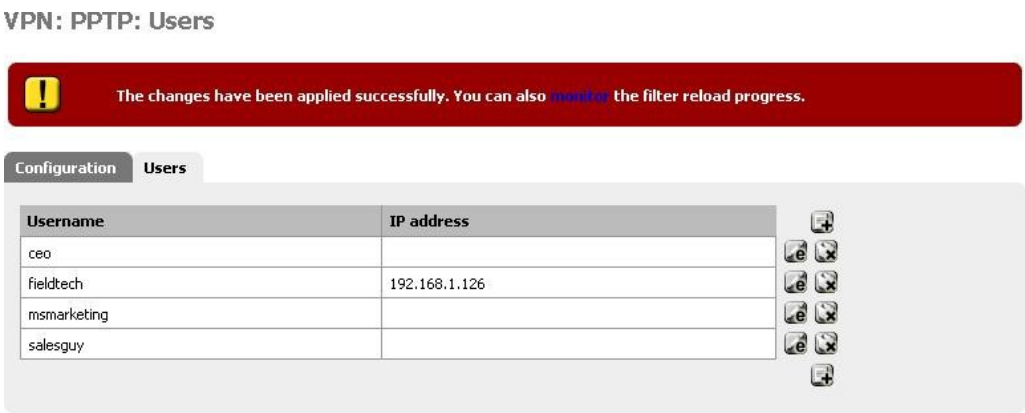


Figura 14.6. Lista de Usuarios PPTP

Si usted necesita para editar un usuario existente, haga clic en. Los usuarios pueden ser eliminados por clic.

14.6. PPTP configuración del cliente

Ahora que su servidor PPTP está configurado y listo, tendrá que configurar PPTP clientes. Las secciones siguientes proporcionan instrucciones sobre la configuración de Windows XP, Windows Vista y Mac OS X para conectarse a un servidor PPTP.

14.6.1. Windows XP

Abra el Panel de control, y haga doble clic en Conexiones de red (Figura 14.7, "Red Conexiones ").

Figura 14.7. Conexiones de red

En Tareas de red, haga clic en Crear una conexión nueva (Figura 14.8, "Tareas de red"). En el pantalla de bienvenida del asistente, haga clic en Siguiente.

Figura 14.8. Tareas de red

Seleccione Conectarse a la red de mi lugar de trabajo, como en la Figura 14.9, "Conexión lugar de trabajo", y haga clic en Siguiente.

Seleccione Conexión de red privada virtual, como en la Figura 14.10, "Conectar a VPN", a continuación, haga clic en Siguiente.

Escriba un nombre para la conexión en nombre de la empresa, al igual que en la Figura 14.11, "Conexión "Nombre, y haga clic en Siguiente.

Introduzca la dirección IP WAN del router remoto pfSense bajo el nombre de host o direcciones IP, al igual que Figura 14.12, "La conexión de host", y haga clic en Siguiente, haga clic en Finalizar (Figura 14.13, "Acabado la conexión ").

Ahora tiene un PPTP entrada de acceso telefónico que funciona como cualquier otro Dail-up. Una solicitud de el nombre de usuario y contraseña, al igual que en la Figura 14.14, "Conexión de diálogo", se mostrará cuando la conexión inicial se intenta. Lo mejor es no conectar todavía, sin embargo. Cancelar este cuadro de diálogo si aparece y vuelve a intentarlo después de seguir el resto de esta sección.

Figura 14.15. Propiedades de la conexión

Hay algunos otros ajustes que necesita revisarse y ajustarse tal vez. Desde dentro de la Red Conexiones, haga clic en el icono de la conexión PPTP, haga clic en Propiedades (Figura 14.15, "Propiedades de la conexión").

Haga clic en la ficha de seguridad (Figura 14.16, "Ficha Seguridad"). Bajo Verificar mi identidad como sigue, asegúrese de que Requerir contraseña asegurado que se elija. Asegúrese también de que Requerir cifrado de datos (Desconectar si no hay) esté marcada.

Ahora haga clic en la ficha Redes. Como se puede ver en la Figura 14.17, "Ficha de red", el tipo de de VPN desplegable por defecto **Automática**. Lo que esto realmente significa es "probar cosas hasta que algo las obras. "PPTP es lo último que Windows intentará, y habrá un retraso de hasta 30 segundos o más mientras espera a que las otras opciones para el tiempo de espera, así que lo más probable es que desee seleccionar **PPTP** aquí para evitar que la demora y cualquier complicación que pueda surgir de la metodología automática de Windows.

De forma predeterminada, esta conexión se enviará todo el tráfico a través de la conexión PPTP como su puerta de enlace. Esto puede o puede no ser conveniente, dependiendo de la configuración deseada. Este comportamiento es configurables, sin embargo. Para cambiar esto, haga doble clic en Protocolo Internet (TCP / IP) y haga clic en el botón Opciones avanzadas. Ahora desactive Usar puerta de enlace predeterminada en la red remota como en la figura 14.18, "Remote Gateway Marco", a continuación, haga clic en Aceptar en todas las ventanas abiertas. Con esta opción sin marcar, sólo el tráfico con destino a la subred de la conexión PPTP atravesar el túnel.

Ahora la conexión PPTP sólo enviará el tráfico destinado a la subred a través de la VPN. Si necesidad de enrutar el tráfico de forma selectiva, vea Sección 14.10, "PPTP enrutamiento trucos".

14.6.2. Windows Vista

Figura 14.19. Vista Conexiones de red

Haga clic en el icono indicador de conexión de red en la bandeja del sistema junto al reloj, a continuación, haga clic en Conectar o Desconectar como se ve en Figura 14.19, "Conexiones de red Vista".

Haga clic en Configurar una conexión o red (Figura 14.20, "Configuración de una conexión"), A continuación, haga clic en Conectar
a un lugar de trabajo (Figura 14.21, "Conectar a un lugar de trabajo") Y luego en Siguiente.

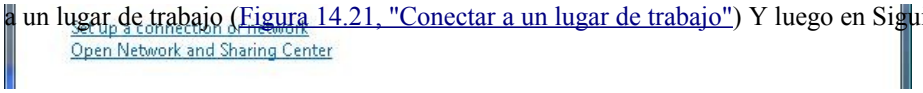


Figura 14.20. Configuración de una conexión

Figura 14.21. Conectar a un lugar de trabajo

Si se le solicita, seleccione No, crear una nueva conexión, y haga clic en Siguiente.

Haga clic en Usar mi conexión a Internet (VPN) (Figura 14.22, "Conectar con VPN").

Figura 14.22. Conectarse a través de VPN

En la siguiente pantalla, se muestra en la Figura 14.23, "Configuración de la conexión", Escriba la dirección IP

WAN del mando a distancia
router pfSense en Dirección de Internet.

Escriba un nombre para la conexión con el nombre de Destino.

Compruebe No Connect Now y haga clic en Siguiente.

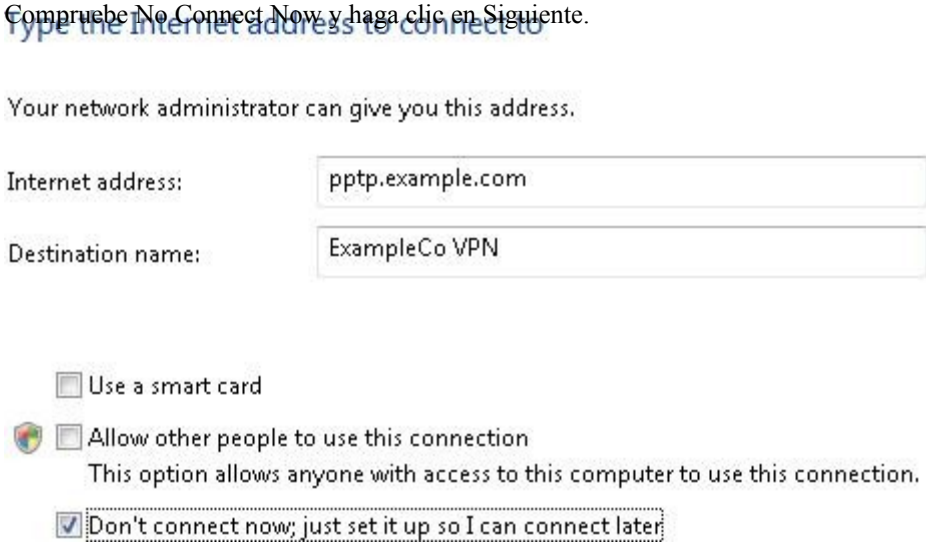


Figura 14.23. Configuración de la conexión

Escriba el nombre de usuario y contraseña, como en Figura 14.24, "Configuración de la autenticación", A continuación, haga clic en Crear. Una pantalla como Figura 14.25, "La conexión está listo" debe aparecer lo que indica que la conexión se ha creado.

Figura 14.24. Configuración de autenticación

Figura 14.25. La conexión está listo

Usted debe ahora tener una PPTP entrada de acceso telefónico que funciona como cualquier otro Dail-up.

Rápidamente

acceder haciendo clic en el icono indicador de conexión de red en la bandeja del sistema, haga clic en Conectar o Desconectar, elija la conexión VPN y haga clic en Conectar.

Sin embargo, antes de conectar por primera vez, hay algunas otras opciones para corroborar. En primer lugar,

haga clic en el icono indicador de conexión de red en la bandeja del sistema, y haga clic en Conectar o Desconectar. Haga clic derecho sobre la conexión VPN que se acaba de crear, a continuación, haga clic en Propiedades como se muestra en la Figura 14.26, "Obtener propiedades de la conexión".

Cambie a la ficha de seguridad (Figura 14.27, "Configuración de VPN de Seguridad"). Bajo verificar mi identidad
de la siguiente manera, asegúrese de que Requerir contraseña asegurado que se elija. Asegúrese también de que los datos requieren
cifrado (desconectar si no hay) esté marcada.

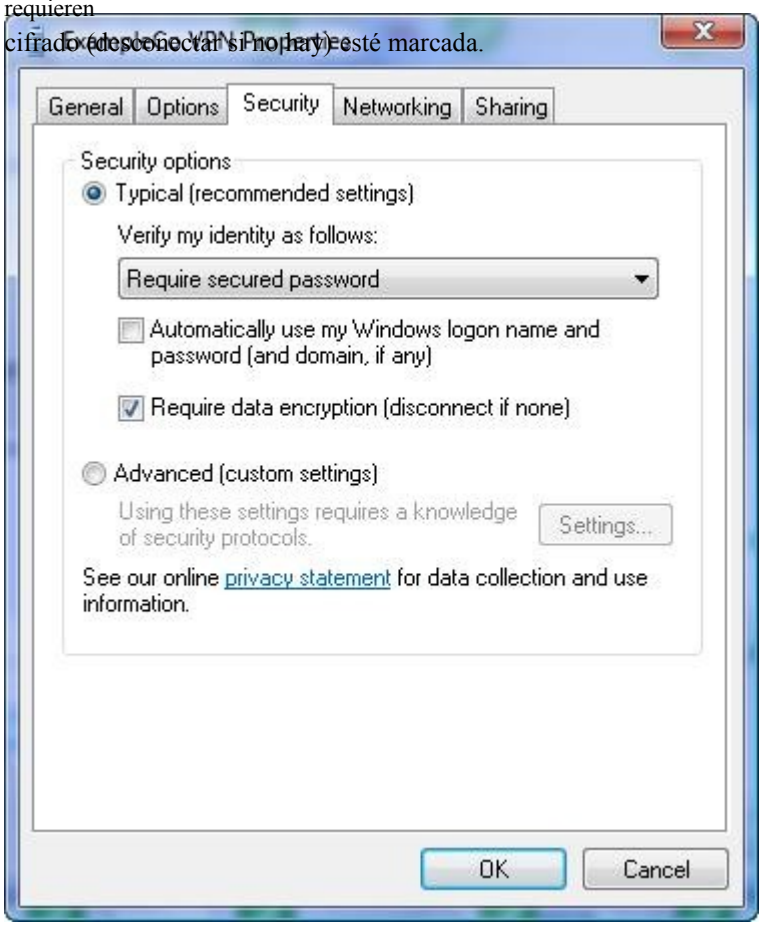


Figura 14.27. VPN Configuración de seguridad

Ahora cambie a la ficha Funciones de red (Figura 14.28, "Configuración de Redes VPN"). Es probable que
la mejor manera de desactivar Protocolo de Internet versión 6 (TCP/IPv6) en este momento.

El tipo de VPN desplegable por defecto **Automática**. Lo que esto realmente significa es "probar cosas hasta que
algo funciona. "PPTP es lo último que Windows intentará, y habrá un retraso de hasta

30 segundos o más mientras espera a que las otras opciones para el tiempo de espera, así que lo más probable es que desee seleccionar
PPTP aquí para evitar que el retraso y las complicaciones que pudieran surgir de la automática de Windows metodología.

Al igual que con Windows XP, esta conexión se enviará todo el tráfico a través de la conexión PPTP como su puerta de enlace. Esto puede o puede no ser conveniente, dependiendo de la configuración deseada. Si quiere todo el tráfico para cruzar el túnel, pase el resto de esta sección. De lo contrario, haga clic en Internet Protocol Version 4 (TCP/IPv4) y haga clic en Propiedades.

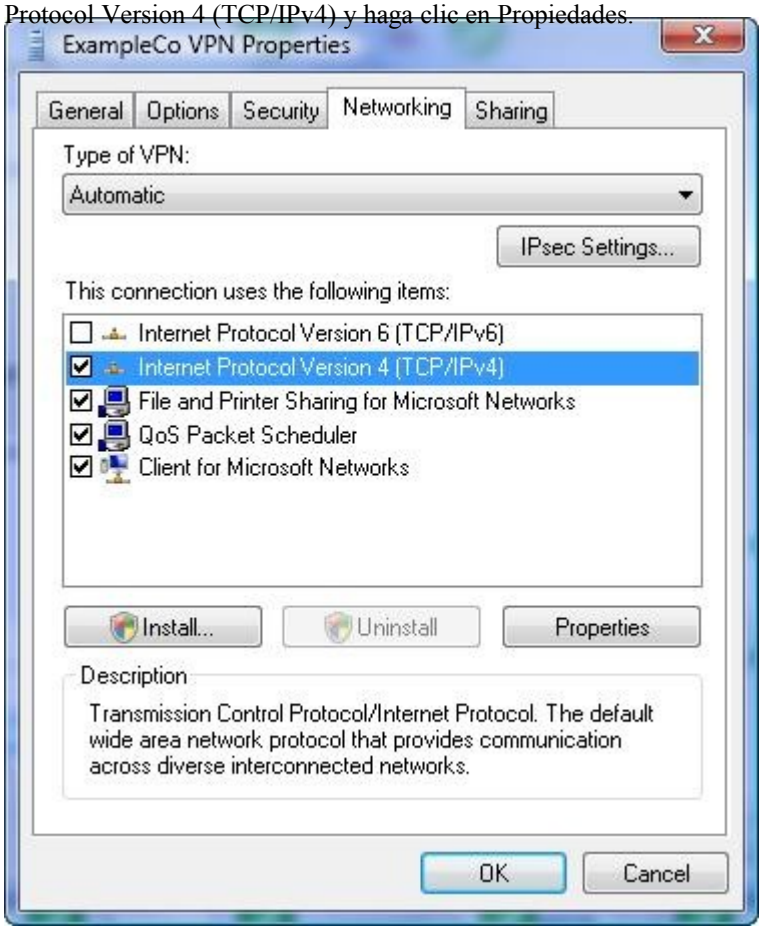


Figura 14.28. VPN Configuración de Redes

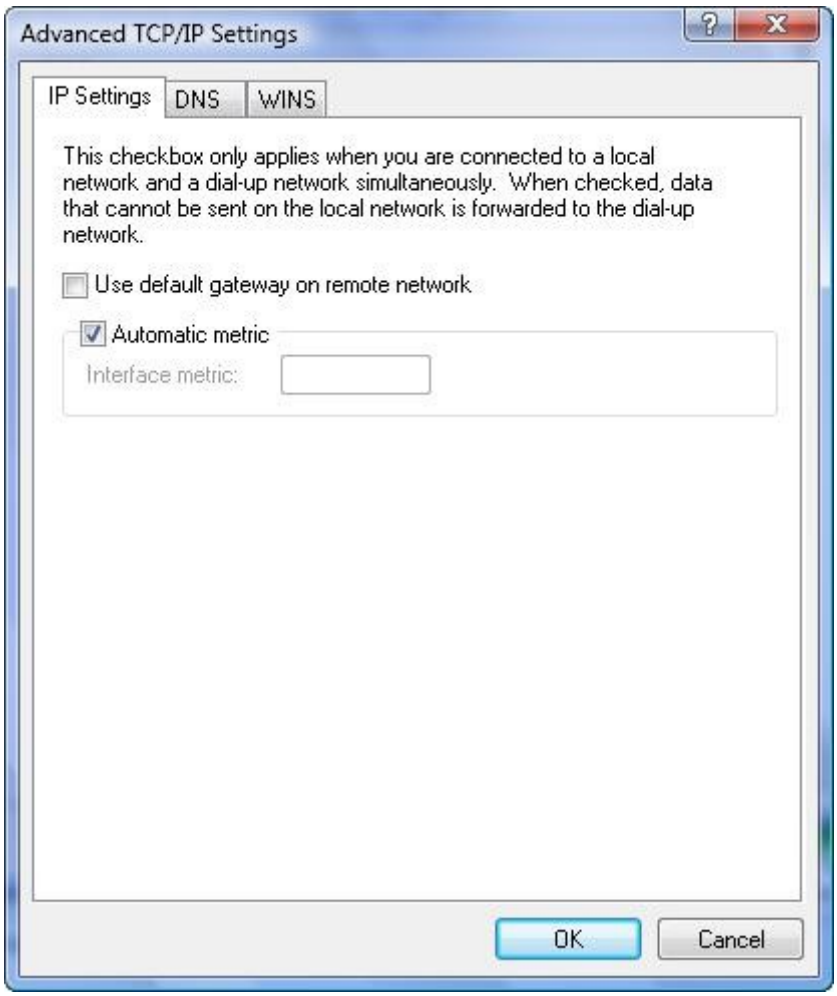


Figura 14.29. VPN Gateway

Haga clic en el botón Opciones avanzadas y, a continuación, desactive Usar puerta de enlace predeterminada en la red a distancia como se muestra en Figura 14.29, "puerta de enlace VPN". Haga clic en Aceptar o en Cerrar en todas las ventanas que se abrieron justo.

Ahora la conexión PPTP sólo enviará el tráfico destinado a la subred a través de la VPN. Si necesidad de enrutar el tráfico de forma selectiva, vea Sección 14.10, "PPTP enrutamiento trucos".

14.6.3. Windows 7

El cliente PPTP procedimiento de configuración en la versión de lanzamiento (RTM) de Windows 7 es prácticamente idéntica
para Windows Vista.

14.6.4. Mac OS X

Abra Preferencias del Sistema, a continuación, haga clic en Ver → Red. Haga clic en el signo más en la parte inferior de la lista
de los adaptadores de red para agregar una nueva conexión, que puede verse en Figura 14.30, "Agregar conexión de red".

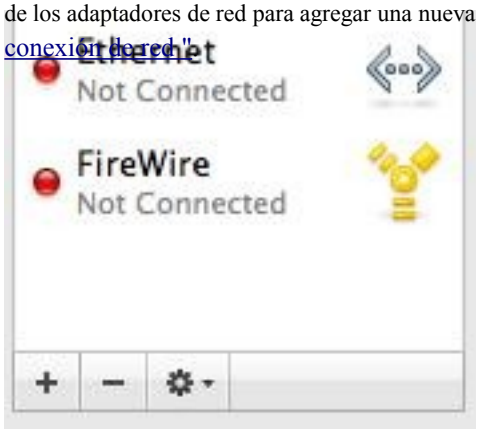


Figura 14.30. Agregar una conexión de red

En la caída de la interfaz de abajo, seleccione VPN y VPN de tipo seleccione PPTP. Rellene el nombre del servicio como que desee y haga clic en Crear. Estas opciones se muestran en la Figura 14.31, "Agregar conexión PPTP VPN"

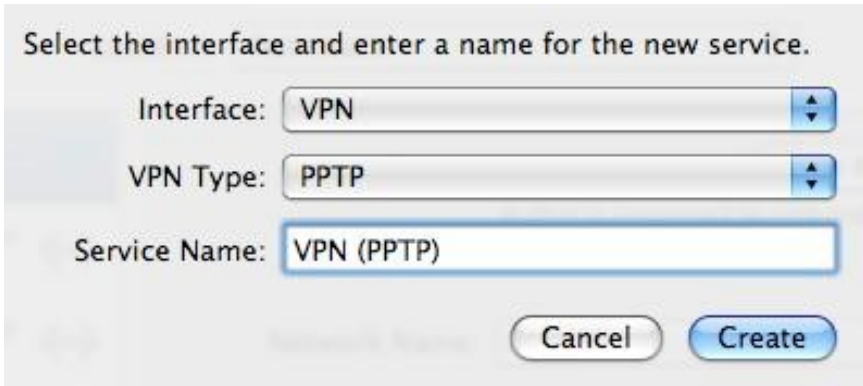


Figura 14.31. Añadir PPTP VPN conexión

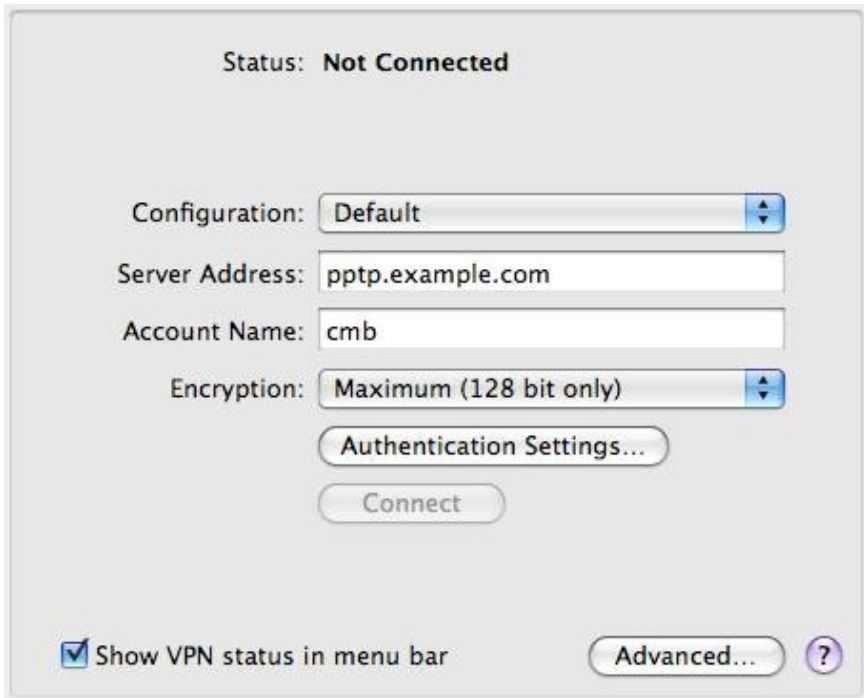


Figura 14.32. Configurar la conexión PPTP VPN

Esto le llevará de nuevo a la pantalla de red donde haya terminado la configuración de la VPN PPTP conexión. Rellene el nombre de la dirección del servidor de cuenta, y elija máximo (128 bits) para Cifrado. Un ejemplo se muestra en la Figura 14.32, "Configuración de conexión PPTP VPN". A continuación, haga clic en el botón Opciones avanzadas.

La pantalla se ha avanzado una serie de opciones, algunas de ellas se muestra en la Figura 14.33, "Avanzada opciones ", aunque sólo una es posible que desee considerar un cambio. La Enviar todo el tráfico a través de VPN caja de conexión está desactivada por defecto. Si quieres todo el tráfico del cliente al atravesar el VPN mientras está conectado, marque esta casilla. Haga clic en Aceptar cuando haya terminado.

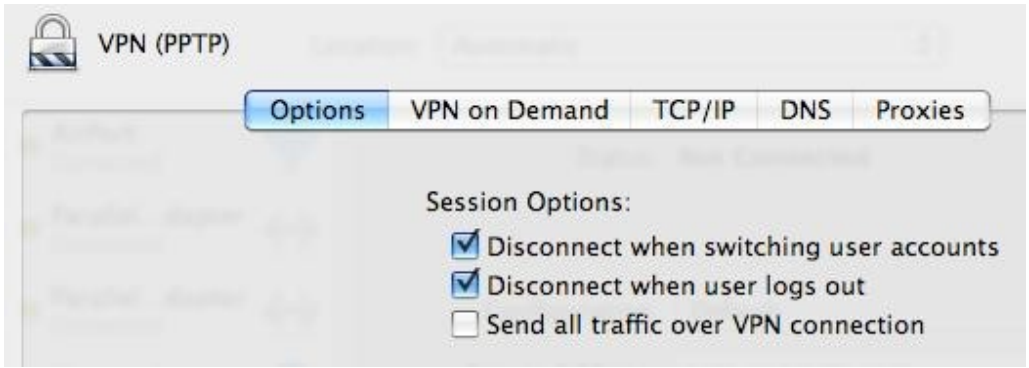


Figura 14.33. Opciones avanzadas

Desde que me registré Mostrar estado de VPN en la barra de menú como se muestra en Figura 14.32, "Configuración de VPN PPTP conexión ", Mi conexión ahora se muestra en la parte superior de la pantalla. Para conectarse, haga clic en el nombre de su conexión como la que se observa en Figura 14.34, "Conectar a PPTP VPN".

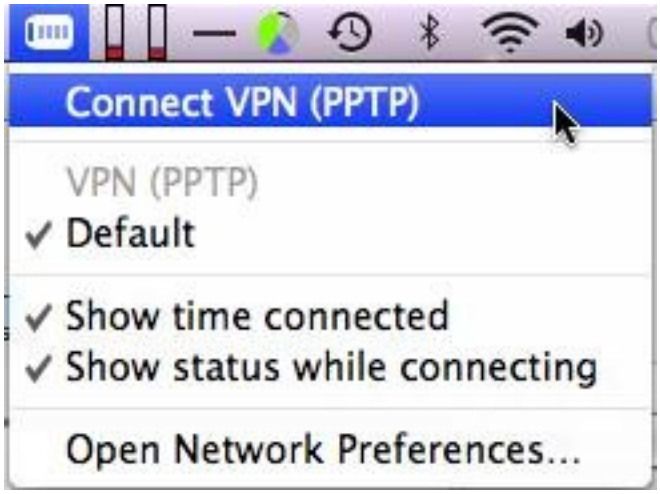


Figura 14.34. Conectar con PPTP VPN

14.7. Aumentar el límite de usuarios simultáneos

Es posible aumentar el límite de usuarios simultáneos de la predeterminada codificado 16, aunque sólo a través de opciones ocultas config.xml. Para aumentar su límite, vaya a los Diagnósticos → Copia de seguridad / Restaurar la pantalla, y haga clic en Descargar configuración. Abra la copia de seguridad XML descargado en un texto editor y desplácese hacia abajo para <pptp>.

```
<pptp>
  <n_pptp_units>16</ N_pptp_units>
  <pptp_subnet>28</ Pptp_subnet>
```

Como se puede ver arriba, la configuración predeterminada para 16 clientes en un / 28 de subred se encuentra en esa sección.
Con el fin de permitir a más clientes, debe ajustar tanto el número de conexión y la subred. En el siguiente ejemplo, no sería de 32 conexiones de clientes, y un bloque de 32 direcciones IP que se utiliza. Tenga en cuenta que esto no es una subred tradicionales en sí, sino un medio de especificar un rango dentro de una más grande de la red. Por eso, todas las direcciones IP en la "subred" definición se pueden utilizar.

```
<pptp>
<n_pptp_units>32</ N_pptp_units>
<pptp_subnet>27</ Pptp_subnet>
```

14.8. PPTP redirección

redirección PPTP permite reenviar el tráfico PPTP destinado a la WAN IP a un interno
servidor PPTP. Para activarla, seleccione Redirigir conexiones entrantes PPTP e introduce tu interior
servidor PPTP IP en el cuadro de la redirección de PPTP. Esto es funcionalmente equivalente a la adición de Puerto
Adelante de las entradas para el puerto TCP 1723 y el protocolo GRE a su servidor interno de PPTP, que
se puede hacer en lugar si lo prefiere. Su existencia es en gran parte del control sobre m0n0wall, donde el
IPFilter subyacente no admite el reenvío del protocolo GRE. Se ha mantenido por
de familiaridad usuarios m0n0wall 'con la función, y algunos usuarios prefieren la facilidad de una sola entrada
en lugar de dos entradas de puerto hacia adelante.
Las reglas de firewall para el protocolo GRE y el puerto TCP 1723 se agregan automáticamente a la red WAN.
No es necesario entrar en cualquier regla de firewall cuando se usa la redirección de PPTP, a menos que tenga Deshabilitar
todo ello sumado auto-VPN normas comprueba en Sistema → Avanzado.

14.9. PPTP Solución de problemas

Esta sección trata de pasos para solucionar problemas de los problemas más habituales se encuentran los usuarios con PPTP.

14.9.1. No se puede conectar

En primer lugar, garantizar el equipo cliente está conectado a Internet. Si eso sucede, tome nota de
el error que está recibiendo por parte del cliente. Windows (excepto Vista) proporcionará un código de error
que le ayudará considerablemente en la reducción a los problemas potenciales. Windows Vista eliminado
esto y por lo tanto, hace que sea difícil de solucionar adecuadamente errores de conexión, pero por suerte la
los mismos códigos de error que han existido por más de una década están de vuelta en Windows 7 (beta y RC).
Solución de problemas con Vista no es recomendable.
Para aquellos clientes que utilizan no son de Windows, las áreas problemáticas son generalmente los mismos, aunque
puede tener que probarlos todos para determinar el problema específico.

14.9.1.1. Error 619

Error 619 significa algo en el camino se está rompiendo el tráfico GRE. Esto es casi siempre
causado por el firewall del cliente está detrás. Si el cliente está también detrás de pfSense, primero asegúrese de que
ninguno de los objetivos señalados en la Sección 14.4, "Limitaciones PPTP" aplicar. Si el servidor de seguridad de la
cliente está detrás de otro producto, es posible que necesite habilitar pasarela PPTP o un lugar similar
para PPTP para funcionar, si se puede en absoluto. En algunos casos, como proveedores de servicios inalámbricos 3G
asignar privado
Direcciones IP a los clientes, se le pegan con la elección de otra opción VPN.

14.9.1.2. Error 691

Error 691 se produce por un nombre de usuario o contraseña no válidos. Esto significa que el usuario no está entrando en
el nombre de usuario o contraseña en el cliente PPTP. Corrija el nombre de usuario o contraseña, en correspondencia con la información configurada en la base de datos de usuarios locales para PPTP, o en la servidor RADIUS.

14.9.1.3. Error 649

Usted puede ver el error 649 cuando la autenticación de RADIUS en un servidor de Microsoft Windows con NIC. Esto significa que la cuenta no tiene permiso para marcar, y la causa será probable una de las tres cosas.

1. Dial en conjunto de permisos con "Denegar el acceso" - vaya a las propiedades de la cuenta del usuario en Active Directorio de Usuarios y equipos y haga clic en la ficha Marcado. Dependiendo de su NIC preferido de configuración, tendrá que o bien **Permitir el acceso** o **Control de acceso a través de directiva de acceso remoto**.
2. contraseña del usuario ha caducado - si la contraseña del usuario ha caducado, no puede iniciar sesión en más de PPTP.
3. Incorrecta configuración de IAS - Puede que haya configurado las políticas de acceso remoto en IAS como de tal manera que los usuarios no están autorizados para ser conectado.

14.9.2. Relacionada con PPTP, pero no puede pasar el tráfico

Asegúrese de que haya agregado las reglas del cortafuegos a la interfaz de PPTP VPN como se describe en Sección 14.5.5, "Configurar las reglas de firewall para clientes PPTP".

Asegúrese también de la subred remota a través de la VPN es diferente de la subred local. Si usted está tratando de conectarse a una red 192.168.1.0/24 a través de VPN y la subred local donde el cliente está relacionada también 192.168.1.0/24, el tráfico destinado a la subred nunca atravesar la VPN porque es en la red local. Por eso es importante elegir una LAN relativamente oscuro subred utilizando las VPN, como se explica en Sección 4.2.4, "Configuración de la interfaz LAN".

14.10. PPTP enrutamiento trucos

Si sólo desea seleccionar subredes que se encaminará a través del túnel PPTP, todavía se puede hacer con algunos comandos de ruta personalizada en el cliente. La siguiente técnica funciona en Windows XP, Vista y Windows 7, pero probablemente se puede modificar para trabajar más en cualquier plataforma. Esto supone que ya ha configurado el cliente para no enviar todo el tráfico a través de la conexión (es decir, no utilizando la puerta de enlace remota).

En primer lugar, el cliente PPTP debe asignar una dirección estática en el perfil de usuario. Esto se puede hacer
utilizando el built-in de autenticación, oa través de RADIUS. Esta dirección estática debe estar fuera de la Piscina asignación general ya que esta no es una reserva.

El truco es para enrutar el tráfico destinado a las subredes a distancia para la dirección asignada PPTP. Este hará que el tráfico de las subredes para viajar en el túnel al otro lado. No se limita a las subredes que son inmediatamente accesibles en el otro lado, ya sea, como cualquier subred se puede utilizar. Esto es útil si quieres también el acceso a la ruta de un sitio de terceros a través del túnel VPN también.

Estos comandos se pueden escribir en una línea de comandos, pero son más a gusto en un archivo por lotes, como en este ejemplo:

```
@ Echo off
route add 192.168.210.0 máscara 255.255.255.0      192.168.1.126
route add    10.99.99.0 máscara 255.255.255.0      192.168.1.126
route add    172.16.1.0 máscara 255.255.252.0      192.168.1.126
pausa
```

En ese ejemplo, *192.168.1.126* es la dirección IP estática asignada a este particular, el cliente PPTP nombre de usuario. Estos comandos de la ruta que los tres subredes especificadas a través de la conexión PPTP, además de la subred para la conexión en sí. La pausa es opcional, pero puede ayudar a asegurar que todas las rutas se han añadido con éxito. El archivo por lotes se tienen que ejecutar cada vez que el se establece la conexión.

Nota

En Windows Vista y Windows 7, estos comandos deben ser ejecutados como Administrador. Si ha creado un acceso directo a este archivo por lotes, sus propiedades pueden ser alterado por lo que siempre se ejecuta de esa manera. Alternativamente, usted puede hacer clic derecho sobre el
por lotes de archivos y seleccione Ejecutar como administrador.

14.11. PPTP Registros

Un registro de eventos de inicio de sesión y cierre de sesión se mantiene en estado de → Registros del sistema, en la ficha PPTP.

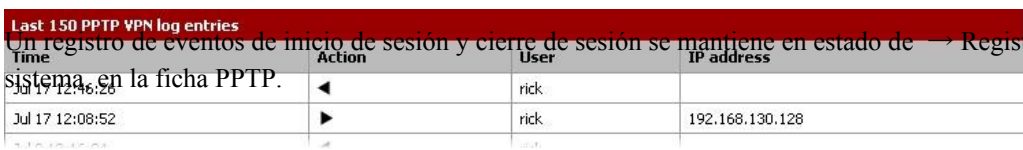


Figura 14.35. PPTP Registros

Como se observa en Figura 14.35, "PPTP Registros", cada inicio de sesión y cierre de sesión deben registrarse con un
fecha y hora y nombre de usuario, y cada entrada también se mostrará la dirección IP asignada a la PPTP cliente.

Capítulo 15. OpenVPN

OpenVPN es una fuente abierta solución SSL VPN que puede ser utilizado tanto para el cliente de acceso remoto y el sitio para conectividad de sitio. OpenVPN apoya a los clientes en una amplia gama de sistemas operativos incluyendo todos los BSD, Linux, Mac OS X, Solaris y Windows 2000 y versiones posteriores. Todos los con OpenVPN, si el acceso remoto o un sitio a otro, consiste en un servidor y un cliente. En el caso de las VPN sitio a sitio, un servidor de seguridad actúa como el servidor y el otro como cliente. Lo hace No importa qué servidor de seguridad posee estas funciones. Normalmente el firewall de la ubicación principal la voluntad de proporcionar conectividad de servidor para todos los lugares remotos, cuyos servidores de seguridad están configurados como clientes.

Esto es funcionalmente equivalente a la configuración opuesta - la ubicación principal configurada como un cliente que se conecta a los servidores que se ejecutan en los servidores de seguridad en los lugares remotos.

Hay dos tipos de métodos de autenticación que se pueden utilizar con OpenVPN: clave compartida y X.509. Para la clave compartida, se genera una clave que se utilizará en ambos lados. X.509 se describe más en la siguiente sección.

Tenga en cuenta que mientras que OpenVPN es una VPN SSL, no es un "sin cliente" SSL VPN en el sentido de que proveedores comerciales cortafuegos comúnmente se refieren a ella. Tendrá que instalar el cliente OpenVPN en todos sus dispositivos cliente. En realidad no hay solución VPN es verdaderamente "sin cliente", y esta es la terminología nada más que una estratagema de marketing. Para mayor discusión a fondo en SSL VPN, este mensaje de Mateo novios, un desarrollador de herramientas de IPsec y pfSense, de los archivos de listas de correo proporciona excelente información: http://marc.info/?l=pfsense-support&m=121556491024595&w=2.

Para una discusión general de los distintos tipos de redes privadas virtuales disponibles en pfSense y sus pros y sus contras, ver Capítulo 12, Redes privadas virtuales.

15.1. Introducción básica a la clave pública X.509 Infraestructura

Una de las opciones de autenticación para OpenVPN es utilizando las teclas X.509. Una discusión a fondo de X.509 y PKI está fuera del alcance de este libro, y es el tema de una serie de libros enteros para los interesados en obtener más información. Esta sección proporciona una comprensión muy básica que necesita para configuración de OpenVPN. Este es el medio preferido de ejecutar las VPN de acceso remoto, ya que le permite revocar el acceso a las máquinas individuales. Con las llaves en la residencia, tienes que crear un servidor único y el puerto para cada cliente, o distribuir la misma clave para todos los clientes. El primero se a ser una pesadilla de gestión, y el segundo es problemático en el caso de una clave comprometida. Si un equipo cliente se ve comprometida, robada o perdida, o de lo contrario desea revocar el acceso de una persona, debe volver a emitir la clave compartida para todos los clientes. Con una implementación de PKI, si un

cliente

está en peligro, o el acceso debe ser revocado por cualquier otra razón, simplemente puede revocar esa certificado de cliente. No hay más clientes se ven afectados.

Con PKI, por una parte una autoridad de certificación (CA) se crea. Este CA entonces todos los signos de la persona certificados en su PKI. certificado de la CA se utiliza en los servidores OpenVPN y clientes verificar la autenticidad de los certificados utilizados. certificado de la CA se puede utilizar para verificar la firma en los certificados, pero no para firmar los certificados. Firma de los certificados requiere la clave privada del CA (`ca.key` cuando se utiliza easy-rsa, discutido más adelante en este capítulo). La privacidad de los particulares CA clave es lo que garantiza la seguridad de la PKI. Cualquier persona con acceso a la clave privada de la CA puede generar certificados para ser utilizados en la PKI, por lo que debe mantenerse segura. Esta clave no es distribuidos a los clientes o servidores.
Asegúrese de que nunca se copia más archivos a los clientes que se necesitan, ya que esto puede resultar en la seguridad de la PKI se vea comprometida. Las secciones posteriores de este capítulo describen los archivos que los clientes necesitan para conectar, y cómo generar los certificados.

15.2. La generación de claves y certificados OpenVPN

OpenVPN utiliza certificados o claves compartidas para cifrar y descifrar el tráfico. En esta sección se muestra cómo para generar una clave compartida o certificados para su uso con OpenVPN. Las secciones posteriores describen cómo uso de estas claves o certificados.

15.2.1. La generación de claves compartidas

clave compartida es el método preferido para un sitio a otro conexiones OpenVPN. Para generar una responsabilidad compartida
clave, vaya a Diagnósticos → Comandos y ejecutar el siguiente comando:

#openvpn - genkey - secreto / tmp / shared.key

A continuación, para mostrar la clave, ejecute lo siguiente:

#cat / tmp / shared.key

La clave se verá algo como esto:

```
#
# 2048 bits clave estática OpenVPN
#
----- BEGIN clave estática OpenVPN V1 -----
6ade12d55caacbbc5e086ccb552bfe14
```

```
4ca7f08230b7e24992685feba9842a03
44ee824c6ac4a30466aa85c0361c7d50
19878c55e6f3e7b552e03a807b21bad5
ce0ca22d911f08d16b21ea1114e69627
f9e8a6cd277ad13b794eef5e1862ea53
e7b0cba91e8f120fa983bdd8091281f6
610bf8c7eb4fed46875a67a30d25896f
0010d6d128ad607f3cbe81e2e257a48a
82abfca3f8f85c8530b975dca34bcfe4
69f0066a8abd114f0e2fbc077d0ea234
34093e7d72cc603d2f47207585f2bdec
ed663ad17db9841e881340c2b1f86d0a
45dc5b24823f47cc565196ceff4a46ca
34fc074959aa1ef988969cfdd6d37533
e5623222373d762a60e47165b04091c2
FIN ----- OpenVPN estática clave V1 -----
```

Copiar la clave y pegarla en la configuración de OpenVPN.

Después de copiar la clave, usted querrá eliminarlo. Para ello, ejecute:

#rm / tmp / shared.key

15.2.2. Generación de Certificados

Para las configuraciones de OpenVPN X.509, primero tiene que generar los certificados. Si usted tiene una PKI existente tendrá que usarlo, y esta sección no será relevante para usted. La mayoría de pfSense los usuarios no tienen una X.509 PKI existente, y es el medio más fácil de establecer un el fácil guiones rsa siempre con OpenVPN.

15.2.2.1. La determinación de un hogar para easy-rsa

Si ya dispone de una BSD o Linux, puedes descargar la última versión de OpenVPN en ese sistema, extraerlo, y se encuentra el `easy-rsa` carpeta bajo el extraídos OpenVPN carpeta. Lo mismo ocurre con los sistemas Windows, la instalación de OpenVPN también instala fácil de RSA, por incumplimiento bajo `C: \ Archivos de programa \ OpenVPN \ easy-rsa`. También puede usar easy-rsa directamente en pfSense.

Si usted prefiere que se ejecute en una máquina virtual, el Herramientas pfSense dispositivo virtual [http://www.pfsense.org / toolsvm] Incluye las secuencias de comandos de fácil rsa.

Los despliegues PKI más graves de este tipo que se ejecuta en un sistema dedicado de
físicamente lugar seguro que no está conectado a cualquier red en todo, con las teclas de copiado según sea necesario
con almacenamiento extraíble. En la mayoría de pequeña o mediana no sea viable, y rara vez
hacer. Tenga en cuenta que un compromiso de la PKI compromete la integridad de todo su
infraestructura de OpenVPN, por lo que mantener en un sistema garantizado adecuadamente el nivel de riesgo en
su red.

15.2.2.2. Generación de certificados utilizando pfSense

Usted puede utilizar easy-rsa en pfSense para generar sus llaves OpenVPN. Los archivos de easy-rsa incluido
con OpenVPN asumir la presencia de la shell bash, que los sistemas operativos BSD no
incluyen de forma predeterminada, por lo que un paquete personalizado fácil de RSA ha sido puesto a disposición de los desarrolladores de pfSense
si desea utilizarlo en su servidor de seguridad. Usted necesitará SSH habilitado en el firewall para un uso fácil-
RSA. Para instalarlo, simplemente ejecuta lo siguiente desde un símbolo del período de sesiones SSH del sistema:

#buscar-o - http://files.pfsense.org/misc/easyrsa-setup.txt | / bin / sh

Esto descargará los archivos, extraer, y quitar el archivo descargado. Después de hacer esto,
se le solicitará que ejecute el siguiente paso de forma manual. Copiar y pegar la última línea que aparecen a generar los certificados.

Nota

Si usted ha pasado por este proceso anteriormente, repitiendo este acabará con todos los
los certificados existentes!

#cd / root/easyrsa4pfsense & &. / PFSENSE_RUN_ME_FIRST

La primera le pedirá su ubicación y organización de la información, para ser utilizado
cuando se genera la autoridad de certificación y los certificados de inicial, y como por defecto cuando
la creación de certificados adicionales en el futuro. A continuación, crear su entidad emisora de certificados,
un certificado de servidor, y un certificado de cliente. Estos archivos se pueden encontrar en el `/ Root / easyrsa4pfsense/keys /` de la guía.

15.2.2.2.1. Creación de una clave de cliente

Para crear una clave de cliente nuevo, ejecute los siguientes comandos, donde username es el nombre de la
cliente (sustituto de la persona *nombre de usuario* aqui).

#cd / root/easyrsa4pfsense
#vars fuente

#. / Build-key *nombre de usuario*

15.2.2.2.2. Creación de una contraseña protegida clave de cliente

El proceso para crear una contraseña protegida clave de cliente es todo lo mismo que una sin contraseñas protegidas clave. Para ello, ejecute los siguientes comandos:

#cd / root/easyrsa4pfsense
#vars fuente
#. / Build-key-pass *nombre de usuario*

La contraseña especificada al crear la clave tendrá que ser introducida por el usuario en cada
con OpenVPN.

15.2.2.2.3. Copia de llaves en el servidor de seguridad

Después de crear las llaves, se necesita un medio de transferencia para su uso en el servidor y el cliente configuraciones. Para las claves utilizadas en pfSense, ya sea en una configuración de servidor o cliente, más fácil forma es utilizar el comando cat en una sesión SSH y copiar el resultado. Por ejemplo, para obtener el contenido del certificado de la CA, ejecute:

#cat / root/easyrsa4pfsense/keys/ca.crt

Copia y pega la salida en el cuadro de certificado de CA. ¿Qué certificado de archivos para entrar en cada uno cuadro de la configuración de OpenVPN se expone más adelante en este capítulo.

Para los clientes no en pfSense, tendrá que descargar los archivos de certificado correspondiente de la del sistema. Esto se puede hacer uso de SCP, según lo descrito en Sección 4.5.2, "Secure Shell (SSH)" o en la interfaz web de los Diagnósticos → pantalla de comandos. Rellene el nombre de archivo adecuado en el archivo para descargar la caja, tales como `/ Root/easyrsa4pfsense/keys/ca.crt` para el CA certificado, y haga clic en Descargar. Repita para cada archivo necesario. Otra alternativa es hacer copias de seguridad en todo el directorio easy-rsa como se describe en la siguiente sección, y extraer la copia de seguridad para recuperar los archivos necesarios.

15.2.2.2.4. Copia de seguridad fácil de rsa

La `easyrsa4pfsense` carpeta no es una copia de seguridad cuando se copia de seguridad de su archivo de configuración.
Usted desea conseguir una copia de seguridad de esta carpeta, como una pérdida de los datos de la `teclas` directorio hará
es imposible generar nuevas llaves y revocar las claves existentes. La configuración actual no le dejar de trabajar, pero perder la posibilidad de añadir o retirar las llaves te dejará pegado a recrear todas las llaves y volver a emitir a sus clientes. La forma más sencilla de copia de seguridad fácil de RSA está utilizando el paquete de copia de seguridad a la ruta de copia de seguridad `/ Root/easyrsa4pfsense` como se muestra en Figura 15.1,

"Copia de seguridad fácil de RSA". El paquete de copia de seguridad es objeto de mayor análisis en Sección 5.6, "Archivos de copia de seguridad y
Directorios con el paquete de copia de seguridad ".

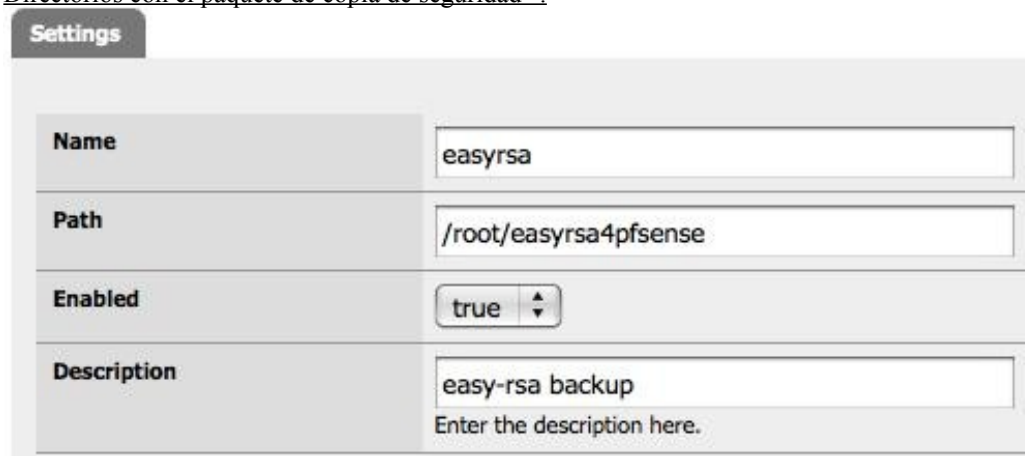


Figura 15.1. easy-rsa de copia de seguridad

15.2.2.3. Uso de easy-rsa

Si usted prefiere usar easy-rsa en un sistema que no sea pfSense, hay algunos pasos adicionales que debe
se sigue que el paquete easyrsa4pfsense maneja de forma automática. Estas medidas son aplicables a
Los sistemas BSD y Linux, aunque el proceso en Windows es básicamente el mismo. Si utiliza Windows,
se refieren a la `LÉAME.txt` en el `easy-rsa` carpeta para obtener más información, y también puede
siga estos pasos en su mayor parte. Para empezar, descargar y extraer de OpenVPN http://
openvpn.net. Dentro de la carpeta extraída se encuentra el `easy-rsa` carpeta. Para Windows,
después de ejecutar la instalación de OpenVPN, se encuentra el `easy-rsa` carpeta en la `C: \ Program Files \ OpenVPN \`.

15.2.2.3.1. Configuración de la información en Vars

Hay un archivo llamado `vars` incluido en el `easy-rsa` carpeta. Abra este archivo en un editor de texto y ir hasta el final del archivo. Verá algo como lo siguiente.

```
exportación KEY_COUNTRY =EE.UU.
exportación KEY_PROVINCE =Kentucky
exportación KEY_CITY =Louisville
exportación KEY_ORG = "pfSense"
```

`exportación KEY_EMAIL = "`*pfSense @ localhost*"

Puede editar estos para que coincida con su ubicación, organización y correo electrónico, aunque también se pueden dejar como es que si quieres que tu los certificados que se crean utilizando esta información. Guardar `vars` después de hacer los cambios que desee.

15.2.2.3.2. Crea tu CA

En primer lugar, vars ejecutar source para cargar las variables de entorno fácil de RSA. A continuación, ejecute. / Clean-all para garantizar usted está comenzando con un medio ambiente limpio. Una vez creada la entidad emisora, nunca haga funcionar la limpieza todos los ya que se eliminará su CA y certificados de todos.

#**vars fuente**

#**. / Limpieza de todos los**
#

Ahora ya está listo para ejecutar. / Build-ca, el comando que crea la entidad emisora. Tenga en cuenta los campos son ya se rellenará con lo que ha entrado en `vars` con anterioridad. Usted puede simplemente presionar Enter en cada del sistema.

#**. / Build-ca**

```
Generar un poco la clave privada RSA 1024
.....++++++
.....++++++
escritura nueva clave privada a 'ca.key'
-----
Estás a punto de pedir que introduzca la información que se incorporarán
en su solicitud de certificado.
Lo que usted está a punto de entrar es lo que se llama un nombre completo o
una DN.
Hay muy pocos campos, pero que pueden dejar algunas en blanco
Para algunos campos no habrá un valor predeterminado,
Si introduce '.', El campo se dejará en blanco.
-----
Nombre País (código de 2 letras) [EE.UU.]:
Estado o Provincia Nombre (nombre completo) [Kentucky]:
Nombre de la localidad (por ejemplo, de la ciudad) [Louisville]:
Nombre de la organización (por ejemplo, de la empresa) [pfSense]:
Unidad organizativa Nombre (por ejemplo, la sección) []:
Nombre común (por ejemplo, su nombre o nombre de host de su servidor) []:
Correo electrónico [pfSense @ localhost] Dirección:
#
```

15.2.2.3.3. La generación de la clave de DH

A continuación, va a generar la clave de DH ejecutando. / Build-dh. Se advierte que tomará mucho tiempo, sin embargo, que depende de la velocidad de su procesador. Esto toma menos de 5 segundos en un procesador Intel Core
2 Quad Q6600, pero puede tardar varios minutos en 500 MHz y una CPU lenta.

#**. / Build-dh**

```
Generación de parámetros de DH, de 1024 bits de largo segura del generador
principal, 2
Esto va a tardar mucho tiempo

.............+..............+..................... .....................
.................. ..........................+.+...................
.....................+..............+... ..........................
.................+.............................. .............. ......
....+.++*++*++*
```

15.2.2.3.4. Generación de un certificado de servidor y la clave

Ahora tiene que crear un certificado y la clave para el servidor OpenVPN usando el ./build-key- de comandos del servidor seguido por el nombre que utilizará para hacer referencia al servidor (sólo cosmético).

#**. / Build-key-servidor** ***servidor***

```
Generar un poco la clave privada RSA 1024
.................++++++
........++++++
escritura nueva clave privada a 'server.key'
-----
Estás a punto de pedir que introduzca la información que se incorporarán
en su solicitud de certificado.
Lo que usted está a punto de entrar es lo que se llama un nombre completo o
una DN.
Hay muy pocos campos, pero que pueden dejar algunas en blanco
Para algunos campos no habrá un valor predeterminado,
Si introduce '.', El campo se dejará en blanco.
-----
Nombre País (código de 2 letras) [EE.UU.]:
Estado o Provincia Nombre (nombre completo) [Kentucky]:
Nombre de la localidad (por ejemplo, de la ciudad) [Louisville]:
Nombre de la organización (por ejemplo, de la empresa) [pfSense]:
Unidad organizativa Nombre (por ejemplo, la sección) []:
Nombre común (por ejemplo, su nombre o nombre de host de su servidor) []:
```



```
Correo electrónico [pfSense @ localhost] Dirección:
```

```
Por favor ingrese los siguientes «extra» atributos
para ser enviado con la petición del certificado
Un desafío clave []:
Un opcional nombre de la empresa []:
Mediante la configuración de / home/cmb/easyrsa4pfsense/openssl.cnf
Comprobar que la solicitud coincide con la firma
Firma ok
El nombre completo del sujeto es el siguiente
countryName: IMPRIMIR: 'EE.UU.'
stateOrProvinceName: IMPRIMIR: 'Kentucky'
localityName: IMPRIMIR: "Louisville"
organizationName: IMPRIMIR: "pfSense '
commonName: IMPRIMIR: 'servidor'
EmailAddress: IA5String: "pfSense @ localhost '
Los certificados habrán de ser certificadas hasta el 18 de enero 2019
07:18:22 GMT (3650 días)
Firma el certificado? [Y / n]: y


1 de cada 1 solicitudes de certificados certificado, nos comprometemos?
[Y / n] y
Escriba una base de datos con las nuevas entradas
Actualización de Base de Datos
#
```

15.2.2.3.5. Generar certificados de cliente

Usted tendrá que crear un certificado para cada cliente con el comando build-key seguido por el nombre de clave. El siguiente ejemplo muestra la creación de una clave de cliente para el usuario *cmb*. Usted puede el nombre de la clave de cliente sin embargo que usted desea. Con el mismo nombre de la persona que va a utilizar la tecla por lo general tiene más sentido. Para las conexiones de cliente que residen en servidores de seguridad, es posible que desea utilizar el nombre de host del servidor de seguridad que se utilice la tecla.

#**.** / **Build-key** ***cmb***

```
Generar un poco la clave privada RSA 1024
.................................................. .++++++
.............................++++++
escritura nueva clave privada a 'cmb.key'
-----
Estás a punto de pedir que introduzca la información que se incorporarán
en su solicitud de certificado.
Lo que usted está a punto de entrar es lo que se llama un nombre completo o
una DN.
Hay muy pocos campos, pero que pueden dejar algunas en blanco
```

```
Para algunos campos no habrá un valor predeterminado,
Si introduce '.', El campo se dejará en blanco.
-----
Nombre País (código de 2 letras) [EE.UU.]:
Estado o Provincia Nombre (nombre completo) [Kentucky]:
Nombre de la localidad (por ejemplo, de la ciudad) [Louisville]:
Nombre de la organización (por ejemplo, de la empresa) [pfSense]:
Unidad organizativa Nombre (por ejemplo, la sección) []:
Nombre común (por ejemplo, su nombre o nombre de host de su servidor) []:
cmb
Correo electrónico [pfSense @ localhost] Dirección:

Por favor ingrese los siguientes «extra» atributos
para ser enviado con la petición del certificado
Un desafío clave []:
Un opcional nombre de la empresa []:
Mediante la configuración de / home/cmb/easyrsa4pfsense/openssl.cnf
Comprobar que la solicitud coincide con la firma
Firma ok
El nombre completo del sujeto es el siguiente
countryName: IMPRIMIR: 'EE.UU.'
stateOrProvinceName: IMPRIMIR: 'Kentucky'
localityName: IMPRIMIR: "Louisville"
organizationName: IMPRIMIR: "pfSense '
commonName: IMPRIMIR: "CMB"
EmailAddress: IA5String: "pfSense @ localhost '
Los certificados habrán de ser certificadas hasta el 18 de enero 2019
07:21:04 GMT (3650 días)
Firma el certificado? [Y / n]: y


1 de cada 1 solicitudes de certificados certificado, nos comprometemos? [Y
/ n] y
Escriba una base de datos con las nuevas entradas
Actualización de Base de Datos
#
```

Tendrá que repetir este proceso para cada cliente que se desplegó. Para los usuarios añadidos en el futuro, puede ejecutar esta de nuevo en cualquier momento.

15.3. Opciones de configuración de OpenVPN

Esta sección describe todas las opciones disponibles con OpenVPN y cuando es posible que desee o necesitan para su uso. Las secciones siguientes cubren ejemplos de configuración de sitio a sitio y remotas VPN de acceso con OpenVPN, con las opciones más comunes y una configuración mínima.

15.3.1. opciones de configuración del servidor

En esta sección se describe cada opción de configuración en el servidor OpenVPN pantalla de edición.

15.3.1.1. Deshabilitar este túnel

Marque esta casilla y haga clic en Guardar para conservar la configuración, pero no permitir que el servidor.

15.3.1.2. Protocolo

Seleccione TCP o UDP aquí. A menos que haya una razón que usted debe utilizar TCP, tales como la capacidad de bypass muchos firewalls mediante la ejecución de un servidor OpenVPN en el puerto TCP 443, que puedes usar UDP. Es Siempre es preferible utilizar los protocolos de conexión al túnel de tráfico. TCP es la conexión orientado, con entrega garantizada. Cualquier pérdida de paquetes son retransmitidos. Esto puede sonar como un buena idea, pero el rendimiento se degrada significativamente en las conexiones de Internet muy cargado, o con la pérdida de paquetes constante, debido a las retransmisiones de TCP. Con frecuencia se tienen el tráfico TCP en el túnel. Cuando usted tiene TCP envuelto alrededor de TCP, cuando un paquete se pierde, tanto la pérdida de paquetes TCP exterior e interior será retransmitido. sucesos poco frecuentes de esto será imperceptible, pero la pérdida recurrente, el rendimiento significativamente inferior al si se utiliza UDP. Usted realmente no desea la pérdida de paquetes encapsulados de tráfico VPN a retransmitido. Si el tráfico dentro del túnel requiere la entrega confiable, se utiliza un protocolo tales como TCP, que asegura que ya se encargará de su propia retransmisión.

15.3.1.3. IP dinámica

Al marcar esta casilla añade la opción de configuración del flotador en la configuración de OpenVPN. Este permite a los clientes conectados a mantener su conexión si sus cambios de propiedad intelectual. Para los clientes en Internet conexiones donde los cambios de propiedad intelectual con frecuencia, o los usuarios móviles que normalmente se mueven entre diferentes conexiones a Internet, tendrá que marcar esta opción. Cuando el cliente IP es estática o raramente cambia, no usar esta opción ofrece una mejora de la seguridad minúscula.

15.3.1.4. Puerto local

El puerto local es el número de puerto que utilizará OpenVPN para escuchar. Sus reglas de firewall necesidad de permitir el tráfico de este puerto, y que éste debe ser especificado en la configuración del cliente. El puerto para cada servidor debe ser único.

15.3.1.5. Dirección de billar

Este es el conjunto de direcciones que se asignará a los clientes a conectar. El servidor de final de la configuración de OpenVPN utilizará la primera dirección de este grupo por su extremo de la conexión, y asignar direcciones adicionales a los clientes conectados.

15.3.1.6. Use direcciones IP estáticas

Si marca esta opción, el servidor no asigna direcciones IP a los clientes. Por lo general esto no se utilizará, aunque es útil en combinación con opciones personalizadas para algunos hacks como el uso de puente.

15.3.1.7. Red local

Este campo especifica la ruta, en su caso, se empuja a los clientes conectarse a este servidor. Si usted necesita impulsar las rutas de más de una subred, introduzca la primera subred aquí y ver Sección 15.10, "Custom opciones de configuración " para obtener información sobre cómo agregar el resto de las subredes.

15.3.1.8. Remoto de la red

Si una subred se especifica aquí, una ruta a la subred a través del otro lado de esta conexión OpenVPN se agregó. Esto se utiliza para el sitio de conectividad de sitio, y no para los clientes móviles. Usted puede Sólo entrar en una subred aquí. Si necesita añadir más de una subred remota, escriba la primera vez aquí y ver Sección 15.10, "Personalizar las opciones de configuración" para obtener información sobre cómo agregar el restantes subredes.

15.3.1.9. De cliente a cliente VPN

Si los clientes necesitan comunicarse entre sí, marque esta opción. Sin esta opción, Sólo puede enviar el tráfico al servidor (y de cualquier red conectada para el que tiene una ruta).

15.3.1.10. Criptografía

Aquí es donde puede seleccionar el sistema de cifrado de cifrado que se utiliza para esta conexión. El valor predeterminado es BF-CBC, que es Blowfish 128 bits de cifrado de bloques de encadenamiento. Esto es por defecto de OpenVPN, y es

una buena elección para la mayoría de los escenarios. Una situación común en el que lo desea, puede cambiar esta es
cuando se utiliza un acelerador de cifrado de hardware, como `glxsb` integrado en el hardware ALIX, o una `hifn` tarjeta. En estos casos, usted verá un mayor rendimiento mediante el uso de un hardware cifrado acelerado. Por ALIX u otro hardware con `glxsb`, Elija **AES-CBC-128**. Por `hifn` hardware, optó por cualquiera de los 3DES o AES opciones. Ver Sección 15.10.3, "El uso de hardware aceleradores criptográficos " Para obtener más información sobre el uso de aceleradores criptográficos.

15.3.1.11. Método de autenticación

Aquí se selecciona cualquiera de PKI o clave compartida, en función de que va a utilizar. Sección 15.2, "La generación de claves y certificados OpenVPN" discute estas opciones con más detalle.

15.3.1.12. Clave compartida

Cuando se utiliza autenticación de clave compartida, se pega la clave compartida aquí.

15.3.1.13. PKI Opciones

Las siguientes cinco opciones están disponibles para la configuración cuando se utiliza la autenticación PKI. La primera cuatro son obligatorios.

15.3.1.13.1. Certificado de CA

Pegue el certificado de CA aquí (`ca.crt` cuando se utiliza easyrsa).

15.3.1.13.2. Certificados de servidor

Pegue el certificado del servidor aquí (`server.crt` cuando se utiliza easyrsa).

15.3.1.13.3. Servidor de claves

Pegue el servidor de claves aquí (`server.key` cuando se utiliza easyrsa).

15.3.1.13.4. DH parámetros

Pegue el DH parámetros aquí (`dh1024.pem` cuando se utiliza easyrsa).

15.3.1.13.5. CRL

CRL está en la lista de revocación de certificados. Si alguna vez tiene que revocar el acceso a una o más de sus certificados, un archivo de CRL PEM se crea que se pegan aquí. Este archivo se llama `crl.pem`

cuando se utiliza easyrsa. Este archivo es una lista completa de todos los certificados revocados, por lo que el contenido de este
campo se sustituye, no anexados, al revocar certificados.

15.3.1.14. Opciones de DHCP

Hay ocho diferentes opciones de DHCP que se pueden configurar. Estas opciones se comportan de la misma como cuando se configura en un servidor DHCP.

15.3.1.14.1. Nombre de dominio DNS

Esto especifica el nombre de dominio DNS que se asignará a los clientes. Para garantizar la resolución de nombres funciona
adecuada para las máquinas de su red local, cuando se utilice la resolución de nombres DNS, debe especificar su nombre de dominio DNS interno aquí. Para Microsoft entornos de Active Directory, este debe por lo general ser su nombre de dominio de Active Directory.

15.3.1.14.2. Del servidor DNS

Aquí se especifica los servidores DNS para ser utilizado por el cliente mientras está conectado a este servidor. Para Microsoft entornos de Active Directory, este debe especificar su DNS de Active Directory servidores para la resolución de nombre propio y la autenticación cuando se conecta a través de OpenVPN.

15.3.1.14.3. Del servidor WINS

Especificar los servidores WINS que se utilizarán, en su caso.

15.3.1.14.4. NBDD servidor

Esta opción es para el servidor de distribución de datagramas NetBIOS, que es típicamente no se utiliza.

15.3.1.14.5. Servidor NTP

Este campo especifica la opción DHCP 47, principal servidor NTP. Puede ser una dirección IP o FQDN.

15.3.1.14.6. NetBIOS nodo de tipo

El tipo de nodo NetBIOS controla cómo los sistemas de Windows funcionará cuando NetBIOS resolver nombres. Por lo general, bien para salir de este a **ninguno** a aceptar por defecto de Windows.

15.3.1.14.7. NetBIOS alcance

Introduzca el ámbito de NetBIOS aquí si es aplicable. Por lo general se deja en blanco.

15.3.1.14.8. Deshabilitar NetBIOS

Esta opción deshabilita NetBIOS sobre TCP / IP en el cliente, y por lo general no se establece.

15.3.1.15. Lzo compresión

Esta casilla de verificación permite la compresión lzo para el tráfico de OpenVPN. Si se marca esta casilla, el tráfico que cruza la conexión OpenVPN se comprimen antes de ser encriptados. Este ahorra en el uso de ancho de banda para muchos tipos de tráfico, a expensas de utilización de la CPU tanto en el servidor y el cliente. En general, este impacto es mínimo, y sugiero que permite esto para casi cualquier uso de OpenVPN a través de Internet. Para las conexiones de alta velocidad, tales como el uso de OpenVPN en un estado latente de velocidad LAN, WAN de alta baja, o una red local inalámbrica, esto puede no ser deseable, ya que el retraso añadido por la compresión puede ser más que el retraso guardan en que se transmite el tráfico. Si casi todo el tráfico que cruza la conexión OpenVPN es ya encriptada (como SSH, SCP, HTTPS, entre muchos otros protocolos), no debe permitir que compresión lzo ya que los datos cifrados no es compresible y la compresión lzo ocasionar que los datos un poco más para ser transferido de lo que sería sin compresión. Lo mismo es cierto si el tráfico VPN es casi en su totalidad los datos que ya está comprimido.

15.3.1.16. Las opciones de personalización

Si bien la interfaz web de pfSense soporta todas las opciones más comúnmente utilizadas, OpenVPN es muy potente y flexible y en ocasiones puede querer o necesitar utilizar las opciones que no están disponibles en la interfaz web. Usted puede llenar en estas opciones de personalización aquí. Estas opciones se describen más en Sección 15.10, "Personalizar las opciones de configuración".

15.3.1.17. Descripción

Introduzca una descripción para esta configuración del servidor, para su referencia.

15.4. Configuración remota de acceso

En esta sección se describe el proceso para configurar un X.509 basados en la solución de acceso remoto VPN con OpenVPN.

15.4.1. Determinar un esquema de direccionamiento IP

Además de las subredes internas que se desea que los clientes de acceso, tiene que elegir una subred IP a utilizar para las conexiones OpenVPN. Esta es la subred llena en menos de interfaz IP en el servidor

de configuración. clientes conectados recibirá una dirección IP dentro de esta subred, y el extremo del servidor de la conexión también recibe una dirección IP de esta subred, donde el cliente dirige el tráfico de subredes encaminado a través de la conexión OpenVPN. Como siempre la hora de elegir subredes internas para una sola ubicación, esta subred debe ser CIDR resumibles con las subredes internas. En el ejemplo red 172.31.54.0/24 representado aquí utiliza para LAN, y 172.31.55.0/24 para OpenVPN. Estos dos redes se resumen con 172.31.54.0/23, haciendo rutas más fáciles de manejar. CIDR resumen se detalla en el Sección 1.7.5, "de resumen CIDR".

15.4.2. Ejemplo de red

Figura 15.2, "ejemplo de red de acceso remoto OpenVPN" muestra la red configurada en el presente ejemplo.

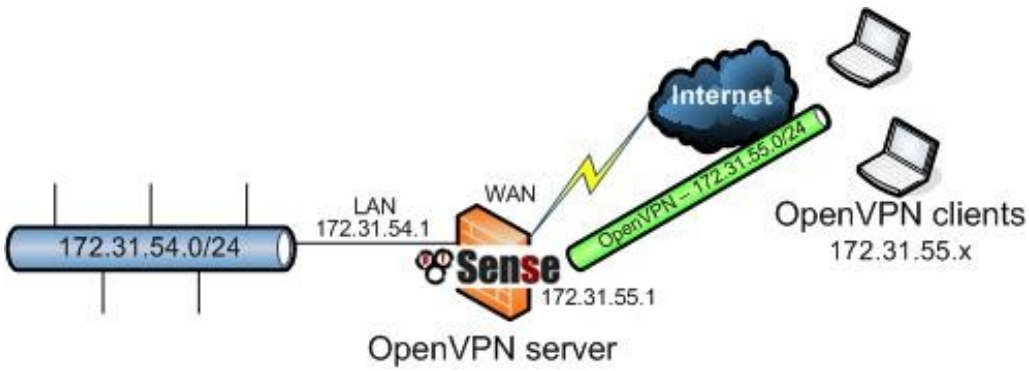


Figura 15.2. OpenVPN ejemplo de red de acceso remoto

15.4.3. Configuración del servidor

Examinar para VPN → OpenVPN y haga clic en la pestaña de servidores para agregar un nuevo servidor OpenVPN.
La mayoría de las opciones se dejarán en sus valores predeterminados. A continuación tendrá que ser configurado.

- Dirección Local - especificar la subred que se utiliza para los clientes OpenVPN aquí. Para este ejemplo, que es **172.31.55.0/24**.
- Método de autenticación - bajando la página un poco antes de pasar una copia de seguridad, es necesario cambiar el método de autenticación de **Clave compartida** a **PKI**.
- Red local - volver a la página y especificar la red local como la red accesible a los clientes a través de la VPN. En este ejemplo que se LAN, por lo que **172.31.54.0/24** es

especificado aquí. subredes adicionales se puede especificar con el **ruta** opción personalizada descrito en Sección 15.10, "Las opciones de configuración".

- certificado de CA - pegar el `ca.crt` archivo de fácil rsa aquí.
- Certificado de Servidor - pegar el `server.crt` archivo de fácil rsa aquí.
- Clave de servidor - pegar el `server.key` archivo de fácil rsa aquí.
- DH parámetros - pegar el `dh1024.pem` archivo de fácil rsa aquí.
- lzo compresión - a menos que esta VPN es usado con una alta velocidad, conexión de baja latencia como una red local cableada o inalámbrica, tendrá que marcar esta casilla para permitir lzo compresión.
- Descripción - completar la descripción aquí para su consulta.

Estas son las opciones de mínimos para la mayoría de las configuraciones de servidor. Las opciones adicionales puede ser deseable o necesario en algunas circunstancias. Consulte Sección 15.3, "OpenVPN Opciones de configuración " Para obtener más información sobre las opciones disponibles.

Cuando termine de configurar las opciones como desee, haga clic en Guardar para terminar la configuración del servidor. pfSense se iniciará el servidor OpenVPN tan pronto como haga clic en Guardar.

15.4.3.1. Que permita el tráfico al servidor OpenVPN

A continuación, agregue una regla de firewall para permitir el tráfico en el servidor OpenVPN. Vaya a Servidor de seguridad → Reglas, 
y en la pestaña WAN, a continuación, haga clic en. Para la configuración de este ejemplo, el protocolo **UDP** será elegido, con **cualquier** origen, destino **Dirección WAN**, Y el puerto de destino **1194**. Esta regla es representado en Figura 15.3, "Servidor OpenVPN WAN regla".

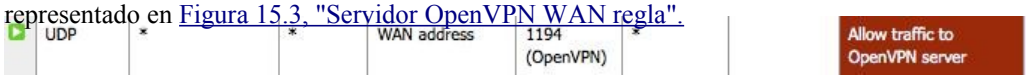


Figura 15.3. servidor OpenVPN WAN regla

Si usted sabe que las direcciones de origen de sus clientes se conectan desde, puede especificar un origen de la red o alias en lugar de dejar el servidor abierto a toda la Internet. Esto es por lo general imposible cuando tienes clientes móviles. No hay mucho riesgo de salir de esto sin embargo abierta, como con la autenticación basada en certificados que tienen menor riesgo de compromiso que basada en contraseñas

soluciones que son susceptibles a ataques de fuerza bruta. Esto supone una falta de agujeros de seguridad en OpenVPN
sí, que hasta la fecha tiene un historial de seguridad sólida trayectoria.

15.4.4. De instalación del cliente

Con la configuración del servidor completo, OpenVPN necesita ahora ser instalado en el cliente
del sistema. La misma instalación de OpenVPN puede funcionar como cliente o servidor, por lo que sólo hay una rutina de instalación. Funciona como se indica en los datos suministrados, que se
cubiertos en la siguiente sección. En esta sección se ofrece un panorama general de la instalación en varias común sistemas operativos.

15.4.4.1. La instalación de Windows

El proyecto OpenVPN ofrece un instalador para Windows 2000 y Windows 7,
descargable desde http://openvpn.net/index.php/open-source/downloads.html. En el momento de este escrito, la mejor versión para la mayoría de los usuarios de Windows es 2.1_rc19. La serie 2.1, aunque todavía no clasificada como estable, ha demostrado ser estable en su uso en producción de ancho e incluye una construida en GUI. La actual versión estable 2.0.9 (lo que se ejecuta en pfSense) no incluye una interfaz gráfica de usuario de Windows. Los 2,1 cliente es totalmente compatible y estable con la versión 2.0.x que se ejecutan en pfSense. La instalación es muy sencillo, simplemente aceptar todos los valores predeterminados. La instalación creará una nueva Área Local Conexión en el sistema de `tonel` interfaz. Esta interfaz se conectará cuando el
VPN está conectado, y si no muestran como desconectado. Sin configuración de esta interfaz es necesario, ya que su configuración se tiró desde el servidor OpenVPN.

Nota

En Windows Vista y Windows 7 con UAC (User Account Control) activado,
derecho que debe hacer clic en el icono de OpenVPN GUI y haga clic en Ejecutar como administrador para que funcione. Puede conectarse sin derechos administrativos, pero no puede agregar la la ruta necesaria para dirigir el tráfico en la conexión OpenVPN, dejándolo inutilizable. También puede ajustar las propiedades del acceso directo para iniciar el programa siempre como administrador. Esta opción se encuentra en la ficha Compatibilidad del acceso directo propiedades.

15.4.4.2. Mac OS X Clientes e instalación

Hay tres opciones de cliente para Mac OS X. Se trata de la simple comando OpenVPN cliente de línea.
La mayoría de los usuarios prefieren un cliente gráfico, y hay dos opciones disponibles para OS X. Tunnelblick es una opción gratuita disponible para su descarga en http://www.tunnelblick.net. Lo he utilizado en el pasado con éxito. Otra opción de interfaz gráfica de usuario es el cliente de Viscosidad comerciales disponibles en http://

www.viscosityvpn.com. En el momento de escribir estas líneas, que cuesta USD $ 9 por un solo escaño. Si se utiliza
OpenVPN con frecuencia, la viscosidad es un cliente mucho más agradable y bien vale la pena el costo.

Ambos Tunnelblick y viscosidad son fáciles de instalar, sin opciones de configuración durante la
la instalación.

15.4.4.3. Instalación de FreeBSD

Si usted tiene una instalación de FreeBSD acción, usted puede encontrar OpenVPN en los puertos. Para instalarlo, simplemente ejecuta:

#cd / usr puertos / / security / openvpn & & make install clean

15.4.4.4. Instalación de Linux

instalación de Linux pueden variar en función de su distribución preferida y el método de gestión
instalaciones de software. OpenVPN está incluido en los repositorios de paquetes de Linux más importantes
distribuciones. Con todas las diferentes posibilidades entre las distribuciones de innumerables y adecuada
información ya disponible en otras fuentes en línea, este libro no cubre los detalles. Simplemente
de búsqueda de Internet para su elección y distribución de "**la instalación de OpenVPN**"Para encontrar
de la información.

15.4.5. Configuración del cliente

Después de instalar OpenVPN, tiene que copiar los certificados para el cliente y crear el cliente
archivo de configuración.

15.4.5.1. Copia de los certificados

Tres archivos de easy-rsa se necesitan para cada cliente: el certificado de CA, el certificado de cliente,
y la clave de cliente. El certificado de la CA es `ca.key` en el directorio easy-rsa llaves. Del cliente
certificado y la clave se denominan con el nombre del cliente se utiliza cuando se generaron. El certificado
para el usuario *jperez* es `jdoe.crt` y la clave es `jdoe.key`. Copiar `ca.crt`,*nombre de usuario*`. Crt` y
nombre de usuario`. Clave` a la OpenVPN `config` directamente en el cliente.

15.4.5.2. Crear Configuración

Después de copiar los certificados para el cliente, el cliente OpenVPN archivo de configuración debe ser
creado. Esto se puede hacer con cualquier editor de archivos de texto sin formato, como el Bloc de notas en Windows. La
siguiente muestra las opciones más utilizadas.

```
cliente
dev tun
udp proto
a distancia openvpn.example.com 1194
ping 10
resolv-retry infinita
nobind
persist-key
persisten-tun
ca ca.crt
cert nombre de usuario. Crt
clave nombre de usuario. Clave
tirar
3 verbo
comp-lzo
```

La **a distancia** línea especifica el host y el puerto del servidor remoto OpenVPN. Una dirección IP o FQDN se puede especificar aquí. La **proto** línea especifica el protocolo utilizado por el OpenVPN conexión. Cambie esta línea por **proto tcp** si elige TCP en lugar de UDP para su servidor OpenVPN. La **ca**,**cert**, Y **clave** líneas deberán modificarse en consecuencia para cada cliente.

15.4.5.2.1. La distribución de configuración y claves a los clientes

La forma más fácil de distribuir las claves y la configuración de OpenVPN para clientes es el paquete en un archivo zip, o auto-extraíble con cremallera para la extracción automática de `C: \ Archivos de programa \ OpenVPN \ Config`. Esto debe ser transmitida con seguridad para el usuario final, y nunca debe ser pasado por alto no son de confianza de redes sin encriptar.

15.4.5.3. Configuración de la viscosidad

Cuando se utiliza el cliente de viscosidad, no es necesario crear manualmente la configuración del cliente OpenVPN archivo como se describe en la sección anterior. La viscosidad proporciona una herramienta de configuración de interfaz gráfica de usuario que se utiliza para generar la base de configuración de OpenVPN cliente se muestra en la sección anterior. En primer lugar, copia del certificado de la CA, certificado de cliente y el cliente clave para una carpeta de su elección en el Mac. Estos archivos se importarán en la viscosidad, y después se pueden borrar. Asegúrese de que esta carpeta se mantiene segura, o que los archivos borrados una vez finalizada la configuración de la viscosidad. A continuación, inicie la viscosidad para iniciar la configuración.

Haga clic en el icono del candado añadido a la barra de menús en la parte superior de la pantalla, y haga clic en Preferencias para comenzar la configuración como se muestra en la Figura 15.4, "Preferencias de Viscosidad".

Haga clic en el signo más en la parte inferior derecha de la pantalla Preferencias de conexión y haga clic en Nuevo, como se muestra
en la Figura 15.5, "Viscosidad Agregar conexión".

En la primera pantalla de configuración (Figura 15.6, "Configuración de Viscosidad: General"), escriba un nombre para su conexión, la dirección IP o nombre de host del servidor OpenVPN, el puerto que se utiliza,
y el protocolo. De verificación Habilitar la compatibilidad de DNS si ha especificado servidores DNS en el servidor de configuración. Haga clic en la ficha Certificados cuando haya terminado.

En la ficha Certificados (Figura 15.7, "Configuración de Viscosidad: Certificados"), la entidad emisora y el usuario certificados y la clave de usuario debe ser especificado. Los archivos se pueden descargar en cualquier lugar de la sistema de archivos Mac. Después de descargarlos, haga clic en Seleccionar junto a cada una de las tres cajas para elegir el archivo correspondiente para cada uno. El cuadro de TLS de autenticación se deja en blanco. Haga clic en la pestaña Opciones cuando haya terminado.

En la ficha Opciones (Figura 15.8, "Configuración de Viscosidad: Opciones"), de verificación Usar lzo Compresión si lo ha activado en el servidor. Las opciones restantes pueden ser dejados en su valores por defecto. Haga clic en la ficha Funciones de red para continuar.

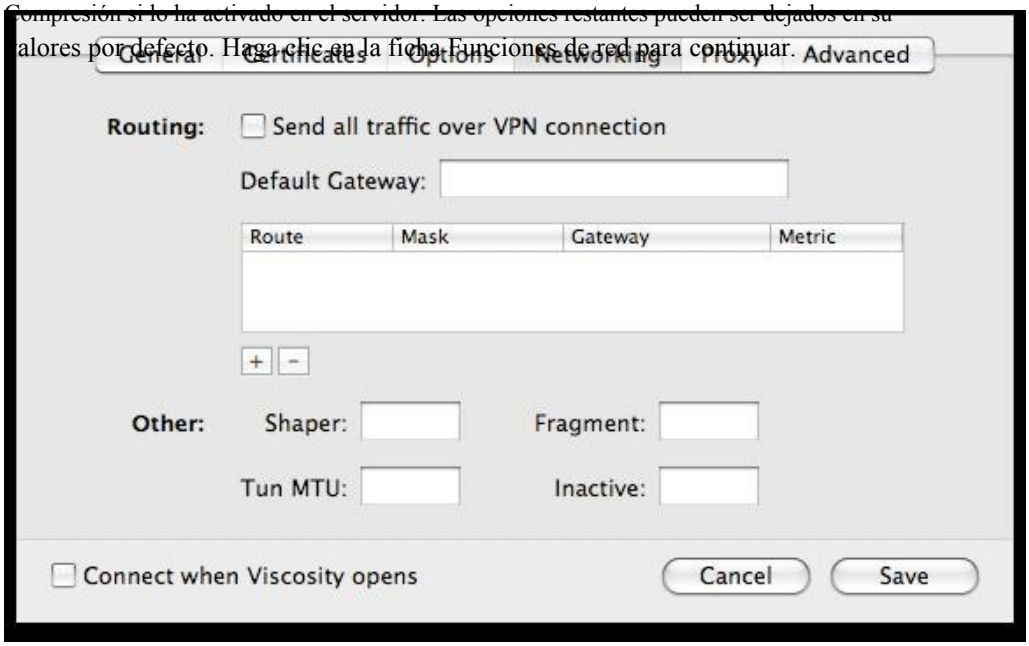


Figura 15.9. Configuración Viscosidad: Redes

En la ficha Funciones de red (Figura 15.9, "Configuración de Viscosidad: Redes"), La principal
opción de interés es la Letra de todo el tráfico sobre la caja de comprobar la conexión VPN. Si desea enviar todos los

tráfico a través de la VPN, marque esta casilla. Las pestañas de configuración restante puede no tenerse en cuenta
en casi todas las configuraciones. Cuando termine, haga clic en Guardar para terminar de agregar el nuevo OpenVPN de configuración.

Ahora tendrás tu acaba de agregar la configuración de OpenVPN se muestra en la pantalla Preferencias.
Cierre la pantalla Preferencias, haga clic en el candado en la barra de menús, y el nombre de la VPN
para conectarse, como se muestra en Figura 15.10, "Viscosidad conectar".

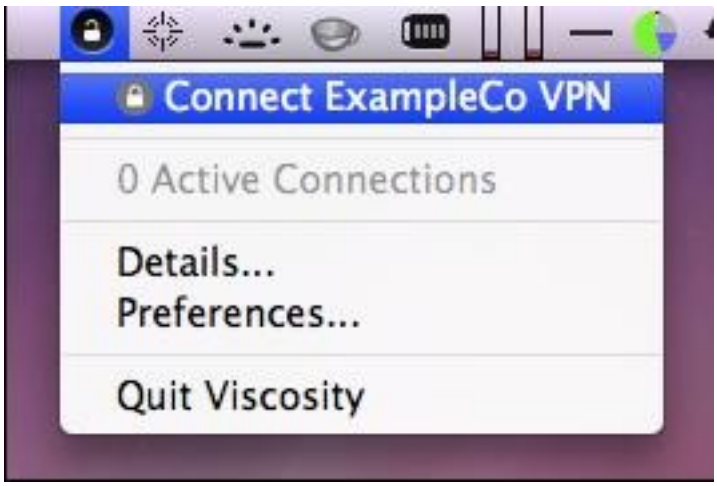


Figura 15.10. Viscosidad conectar

Después de unos segundos, el candado en la barra de menú cambiará a verde para mostrar que ha conectado correctamente.
Al hacer clic en él, y hacer clic en Detalles, como se muestra en la Figura 15.11, "menú de viscosidad", se puede ver información sobre la conexión.

En la primera pantalla (Figura 15.12, "los detalles de viscosidad"), verá el estado de la conexión, conectado
tiempo, la IP asignada al cliente, y la IP del servidor. Un gráfico de ancho de banda se muestra en
la parte inferior de la pantalla, mostrando el rendimiento dentro y fuera de la interfaz de OpenVPN.

Al hacer clic en el botón arriba / abajo las flechas en el centro de la pantalla de detalles, puede ver más
las estadísticas de tráfico de red. Esto muestra el tráfico enviado dentro del túnel (TUN / TAP de entrada y salida), como así como el total de tráfico TCP o UDP enviados incluyendo la sobrecarga del túnel y cifrado. Por
conexiones con los paquetes principalmente pequeñas, la sobrecarga es considerable con todas las soluciones VPN.
Las estadísticas se muestran en la Figura 15.13, "detalles Viscosidad: Estadísticas de tráfico" son de sólo unos cuantos pings
atravesar la conexión. El tráfico enviado en la educación de la conexión también se cuenta aquí, así que

la sobrecarga inicial es mayor de lo que será después de haber sido vinculado durante algún tiempo. Además, el
típico de tráfico VPN tendrá mayor tamaño de los paquetes de 64 bytes pings, haciendo que el total de gastos y la diferencia entre estos dos números considerablemente menor.

Al hacer clic en el icono de tercero en el centro de la pantalla muestra los detalles del archivo de registro OpenVPN (Figura 15.14, "detalles Viscosidad: Registros"). Si usted tiene algún problema de conexión, revise los registros aquí para ayudar a determinar el problema. Véase también Sección 15.11, "Solución de problemas OpenVPN".

15.5. Sitio para Ejemplo de configuración de la web

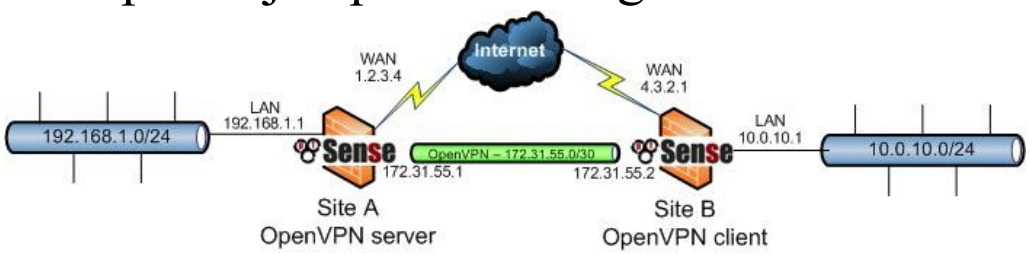


Figura 15.15. OpenVPN sitio de ejemplo a la red de sitio

En esta sección se describe el proceso de configuración de un sitio a la conexión del sitio con claves compartidas. Cuando la configuración de un sitio a otro con OpenVPN, un servidor de seguridad será el servidor y el otro será el cliente. Por lo general, su ubicación principal será el lado del servidor y las oficinas remotas actuarán como clientes, aunque lo contrario es funcionalmente equivalente. Además de las subredes de ambos extremos, como en el acceso remoto de configuración de OpenVPN, habrá una subred dedicada en utilizar para la interconexión entre las redes de OpenVPN. La configuración de ejemplo que se describe aquí se representa en Figura 15.15, "sitio OpenVPN ejemplo a la red de sitio".

172.31.55.0/30 se utiliza como el conjunto de direcciones. El túnel OpenVPN entre los dos servidores de seguridad recibe una IP en cada extremo de la subred, como se ilustra en el diagrama. Los siguientes secciones se describe cómo configurar la parte del servidor y el cliente de la conexión.

15.5.1. Configuración del lado del servidor

Examinar para VPN → OpenVPN y haga clic en la pestaña Servidor. Los siguientes campos están configurados, con todo lo demás a la izquierda en valores predeterminados.

• Dirección de billar - Ingrese **172.31.55.0/30** aquí.

• Control remoto de la red - Ingrese **10.0.10.0/24** aquí.

• clave compartida - Pegar en la clave compartida para esta conexión aquí. Instrucciones en la generación de claves compartidas se proporciona en Sección 15.2.1, "La generación de claves compartidas".

• Descripción - Introduce algo aquí para describir la conexión.

Eso es todo lo que debe estar configurado para el servidor OpenVPN para funcionar en este escenario.
Haga clic en Guardar.

A continuación, tendrá que añadir una regla de firewall en la WAN que permite acceder al servidor OpenVPN. Especificar el protocolo **UDP**, IP de origen como la dirección IP del cliente si tiene una dirección IP estática, o **cualquier** si su
IP es dinámica. Destino es el **Dirección WAN**, Y el puerto de destino es **1194** en este caso.
Figura 15.16, "sitio OpenVPN ejemplo de regla de firewall sitio de la WAN" muestra la regla de firewall utilizados para este ejemplo.

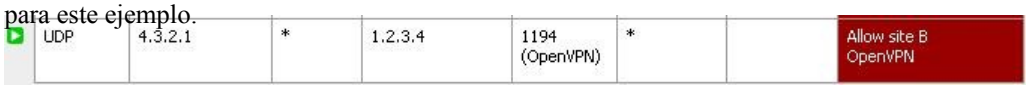


Figura 15.16. OpenVPN sitio de ejemplo de regla de firewall sitio WAN

Aplicar cambios después de la regla de firewall se agrega, y la configuración del servidor ha terminado.

15.5.2. Configuración del lado del cliente

Por el lado del cliente, vaya a VPN → OpenVPN y haga clic en la ficha de cliente. Los siguientes los campos están configurados, con todo lo demás a la izquierda en valores predeterminados.

• Dirección de servidor - Introduzca la dirección IP pública o nombre de host del servidor OpenVPN aquí.

• Control remoto de la red - Ingrese **192.168.1.0/24** aquí.

• clave compartida - Pegar en la clave compartida para la conexión de aquí, utilizando la misma clave que en el del lado del servidor.

• Descripción - Introduce algo aquí para describir la conexión.

Después de rellenar los campos, haga clic en Guardar. La configuración del cliente es completa. Ningún firewall normas son necesarias en el lado del cliente porque el cliente sólo inicia las conexiones salientes. La servidor nunca inicia las conexiones con el cliente.

Nota

Con acceso remoto configuraciones de PKI, con frecuencia no define las rutas y otras opciones de configuración en la configuración del cliente, sino más bien impulsar los opciones desde el servidor al cliente. Con despliegues clave compartida, debe definir rutas y otros parámetros en ambos extremos, según sea necesario (como se describió anteriormente, y más adelante en Sección 15.10, "Personalizar las opciones de configuración"), No puede empujar a el cliente al servidor utilizando las claves compartidas.

15.5.3. Prueba de la conexión

La configuración se ha completado y la conexión se activa inmediatamente después de guardar en el lado cliente. Intente hacer ping a través al extremo remoto para verificar la conectividad. Si surgen problemas, se refieren a Sección 15.11, "Solución de problemas OpenVPN".

15.6. Filtrado y NAT con OpenVPN Conexiones

De forma predeterminada, pfSense añade normas a la `tonel` o `puntee` interfaces siendo utilizado por OpenVPN para permitir todo el tráfico desde los clientes conectados OpenVPN. Si desea filtrar el tráfico de OpenVPN clientes, tienes que comprobar deshabilitar todas las reglas VPN agregó automáticamente en Sistema → Avanzada (véase Sección 12.3, "Reglas del cortafuegos y redes privadas virtuales" antes de hacer esto para examinar las ramificaciones). A continuación, asignar la interfaz de OpenVPN en una interfaz OPT y configurar en consecuencia. En esta sección describe cómo llevar a cabo tanto el filtrado y NAT para los clientes OpenVPN.

15.6.1. Interfaz de configuración y asignación de

Examinar a las interfaces → Asignar y asignar el adecuado `tonel` o `puntee` interfaz como un OPT interfaz. Si sólo tiene una conexión OpenVPN y no está utilizando un puente como se describe en Sección 15.9, "Conexiones en puente OpenVPN", La interfaz de OpenVPN se `tun0`. Si tener varias conexiones, y la necesidad de NAT o filtran el tráfico entrante de clientes OpenVPN, tendrá que especificar el dispositivo a utilizar para cada conexión en el campo de opciones personalizadas. Esto se describe en Sección 15.10.2, "Especificación de la interfaz". Usted tendrá una interfaz OPT por servidor OpenVPN y cliente configurado en el sistema. Figura 15.17, "Asignar tun0 interfaz" muestra `tun0` asignado como OPT1.

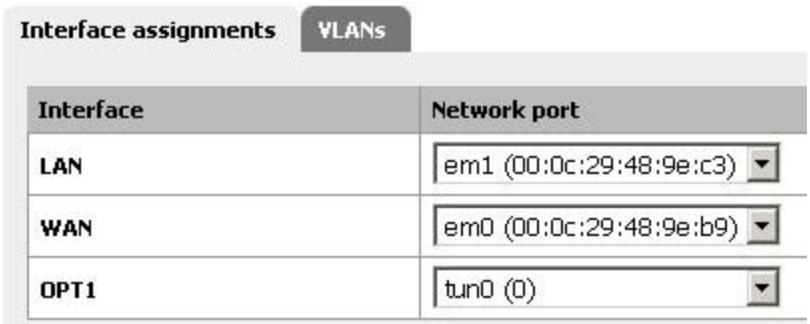


Figura 15.17. Asignar tun0 interfaz

Ahora vaya a la página de la interfaz previamente asignado, Interfaces → OPT1 para el ejemplo de la Figura 15.17, "Asignar tun0 interfaz". En primer lugar comprobar la interfaz Active cuadro en la parte superior de la página, y escriba una descripción adecuada en el campo Descripción. En el IP cuadro de dirección introducir **ninguno**. Este es un truco que no configure la información IP en la interfaz, que es necesario, ya que OpenVPN se debe configurar estos ajustes en la `tun0` interfaz. Haga clic en Guardar para aplicar estos cambios. Esto no hace nada para cambiar la funcionalidad de OpenVPN, simplemente hace que la interfaz disponible para regla de firewall y NAT fines.

15.6.2. Filtrado con OpenVPN

Ahora que tiene la interfaz de OpenVPN asignado, vaya al servidor de seguridad → Reglas y haga clic en el ficha de la interfaz de OpenVPN que acaba de asignar. Aquí usted puede agregar reglas de firewall al igual que cualquier otra interfaz que se aplicarán al tráfico iniciado por los clientes OpenVPN. Recuerde que a menos que comprobar la Deshabilitar todas las auto-agregó VPN cuadro de normas en Sistema → Avanzada, permiten a todas las reglas de la interfaz se agregó que anulará las normas que se aplican aquí. Para obtener más información sobre las reglas del cortafuegos, consulte Capítulo 6, Servidor de seguridad.

15.6.3. NAT con OpenVPN

Si simplemente quieres NAT sus clientes OpenVPN para su WAN IP para que puedan acceder a Internet utilizando la conexión OpenVPN, necesita habilitar avanzada de salida NAT y especificar una Salida NAT regla para su dirección de subred Alberca (s). Ver Sección 7.6, "NAT Saliente" de más detalles sobre salida NAT.

Con la interfaz de OpenVPN asignado, NAT reglas también se puede aplicar lo mismo que con cualquier otra interfaz. Esto es útil cuando hay que conectar dos subredes en conflicto. Si tiene dos

redes que utilizan una subred LAN 192.168.1.0/24 que usted necesita para conectarse a través de una VPN sitio a sitio,
no pueden comunicarse a través de VPN con NAT (o puente, como se explica en Sección 15.9, "Conexiones OpenVPN puente", Pero que realmente sólo deberán utilizarse para clientes móviles y no sitio para conexiones de sitio). Los hosts de una subred 192.168.1.0/24 nunca llegar al otro extremo de la VPN para comunicarse con la subred 192.168.1.0/24 a distancia, debido a que la red es siempre tratadas como locales. Sin embargo, con NAT, usted puede hacer la función de extremo remoto, como si se tratara de usar una subred IP diferente.

Nota

Esto funciona bien para muchos protocolos, pero para algunos que son comúnmente deseables a través de conexiones VPN, principalmente SMB / CIFS para compartir archivos entre Windows los ejércitos, no funcionará en combinación con NAT. Si está usando un protocolo que no es capaz de funcionar con NAT, ésta no es una solución viable.

Figura 15.18, "Sitio al sitio con subredes en conflicto" muestra un ejemplo donde ambos extremos son utilizando la misma subred. Después de asignar la `tonel` interfaz para una interfaz opcional en ambos lados, como
se describe en Sección 15.6.1, "la asignación de interfaz y configuración", 01:01 NAT se puede aplicar.

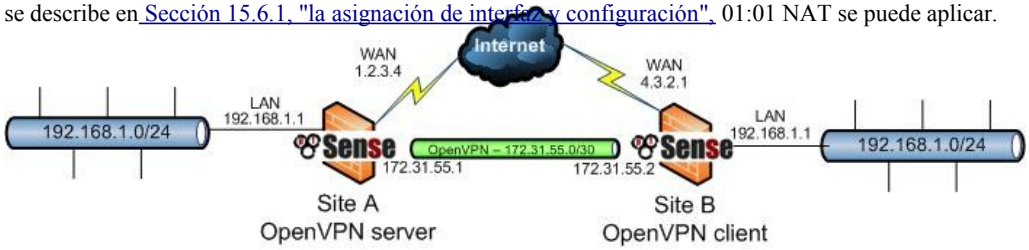


Figura 15.18. Un sitio a otro con subredes en conflicto

El tráfico desde el sitio A se traducirá a 172.16.1.0/24, y el sitio B se traducirán a 172.17.1.0/24. Una entrada de NAT 01:01 se añadirá en cada extremo de traducir toda la / 24 gama. Para llegar a un sitio desde el sitio B, 172.16.1.x direcciones IP se utilizan. El último octeto de la 192.168.1.x IP será traducido al último octeto en el 172.16.1.x traducida IP, por lo que para llegar a 192.168.1.10 Un sitio desde el sitio B, utilizaría 172.16.1.10 lugar. Para llegar a 192.168.1.50 en el Sitio B desde El sitio A, deberá utilizar 172.17.1.50 lugar. Figura 15.19, "Sitio de configuración de un NAT 1:1" y Figura 15.20, "Sitio B configuración de NAT 1:1" muestra la configuración de 01:01 NAT para cada lado, donde el `tonel` interfaz se asigna como OPT2.

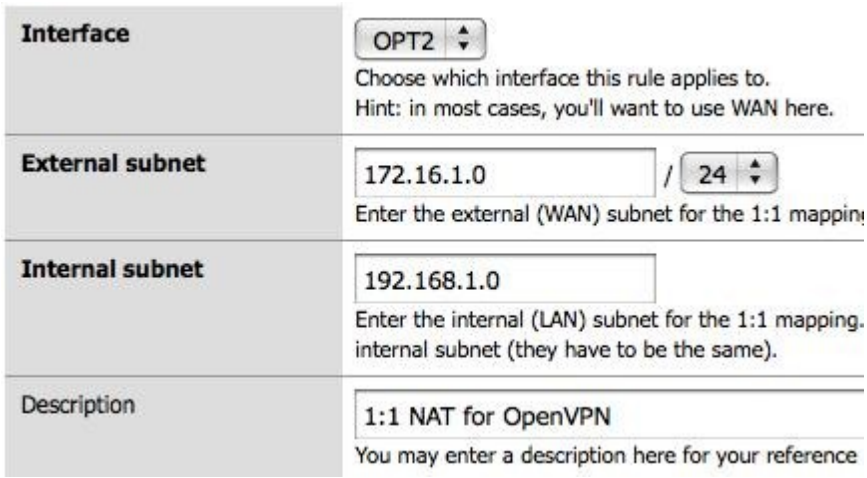


Figura 15.19. Un sitio de configuración de NAT 01:01

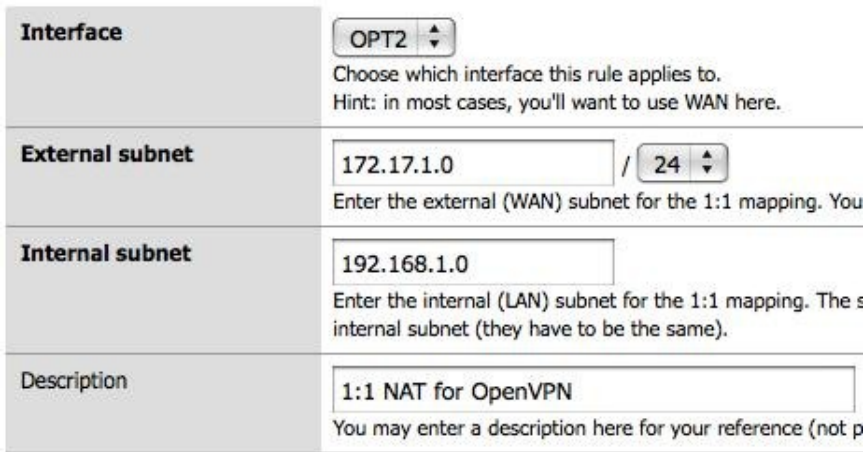


Figura 15.20. Sitio B 01:01 configuración de NAT

En la configuración de OpenVPN en ambos lados, en la red a distancia debe ser especificado como el subred IP traducida, no como 192.168.1.0/24. En este ejemplo, la red remota en el sitio A es 172.17.1.0/24 y 172.16.1.0/24 en el sitio B.

Después de aplicar los cambios de configuración de NAT y la configuración de la red remota en consecuencia en ambos lados, las redes serán capaces de comunicarse utilizando las subredes traducido.

15.7. OpenVPN y Multi-WAN

OpenVPN es multi-WAN capaz, con algunas salvedades en algunas circunstancias. Esta sección cubre consideraciones multi-WAN con el servidor OpenVPN y configuraciones de cliente.

15.7.1. OpenVPN y servidores multi-WAN

servidores OpenVPN puede ser usado con cualquier conexión WAN, aunque los medios de hacerlo se varían dependiendo de los detalles de su configuración.

15.7.1.1. OpenVPN servidor mediante TCP

Mientras que el TCP no es generalmente el protocolo preferido para OpenVPN, como se describe anteriormente en este capítulo, a través de TCP hace multi-WAN OpenVPN más fácil de configurar. OpenVPN servidores que utilizan TCP funciona correctamente en todas las WAN, donde las reglas del firewall para permitir el paso a la OpenVPN servidor. Se necesita una regla en cada interfaz WAN.

15.7.1.2. OpenVPN servidor usando UDP

servidores OpenVPN con UDP también multi-WAN capaz, pero con algunas salvedades que no son aplicables con TCP, ya que las funciones multi-WAN del pf manera de enrutamiento. Cada WAN debe tener su propio servidor OpenVPN. Usted puede utilizar los mismos certificados para todos los servidores. Sólo dos partes de la configuración de OpenVPN debe cambiar.

15.7.1.2.1. Dirección Pool

Cada servidor debe tener un único conjunto de direcciones que no se superponga con ningún otro grupo de direcciones o internos de subred.

15.7.1.2.2. Costumbre local Opción

Cada servidor OpenVPN debe especificar la IP de la interfaz WAN utilizado por el servidor con la **locales** opción personalizada. El siguiente ejemplo muestra cómo configurar OpenVPN para WAN IP 1.2.3.4.

locales 1.2.3.4

Para las conexiones con IP dinámica, un nombre de host como alternativa se puede especificar. Los siguientes muestra un ejemplo para openvpn.example.com nombre de host.

openvpn.example.com locales

15.7.1.2.3. Conmutación por error automática para los clientes

Varios servidores remotos se pueden configurar en los clientes OpenVPN. Si el primer servidor no puede ser alcanzado, la segunda se utilizará. Esto puede ser usado en combinación con un OpenVPN multi-WAN implementación del servidor para proporcionar conmutación por error automática para los clientes. Si los servidores son OpenVPN
que se ejecutan en IP 1.2.3.4 y 4.3.2.1, tanto a través del puerto 1194, el **a distancia** las líneas de su cliente archivo de configuración será la siguiente.

```
1.2.3.4 remoto 1194
4.3.2.1 remoto 1194
```

Para los clientes configurados en pfSense, la primera **a distancia** está configurado por las opciones dadas en el Interfaz gráfica de usuario. El segundo **a distancia** se especifica en el campo de opciones personalizadas.

15.7.2. OpenVPN clientes y Multi-WAN

clientes OpenVPN configurado en el servidor de seguridad seguirá el sistema de la tabla de enrutamiento al hacer la conexión con el servidor OpenVPN. Esto significa que por defecto, todos los clientes el uso de la WAN interfaz. Para utilizar una interfaz WAN OPT, debe introducir una ruta estática para dirigir el tráfico a la extremo remoto de la conexión OpenVPN.

Figura 15.21, "Ejemplo de ruta estática para el cliente OpenVPN en OPT WAN" ilustra la estática la ruta necesaria para utilizar el interfaz de WAN2 acceder a un servidor OpenVPN que se ejecutan en IP 1.2.3.4, en la puerta de enlace de la interfaz WAN2 es 172.31.1.1.

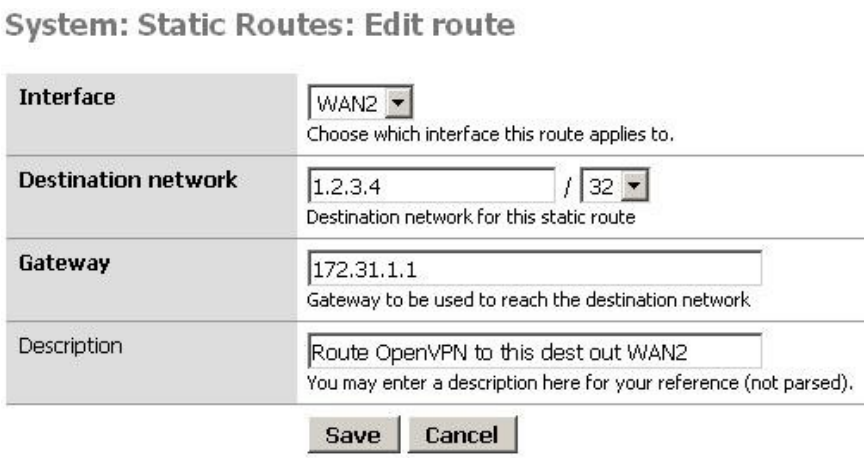


Figura 15.21. Ejemplo estática de las rutas de OpenVPN Client en OPT WAN

15.8. OpenVPN y CARP

OpenVPN es interoperable con la carpa. Para proporcionar una solución de alta disponibilidad con OpenVPN CARP, configurar los clientes para conectarse a un VIP CARP, y configurar el servidor OpenVPN para utilizar el período de investigación con la CARP **locales** opción de configuración a medida. En 1.2.x pfSense, el OpenVPN configuración no se puede sincronizar con el servidor de seguridad secundaria, por lo que debe introducir manualmente que en ambos servidores de seguridad. El estado de la conexión no se conserva entre los hosts, de modo que los clientes deben volver a conectar después de conmutación por error, pero OpenVPN detectará el error de conexión y vuelva a conectar dentro de un minuto más o menos de conmutación por error. CARP se discute en Capítulo 20, Firewall de redundancia y Alto Disponibilidad.

15.9. Conexiones en puente OpenVPN

Las configuraciones de OpenVPN discutido hasta este punto han sido enviados, con `tonel` interfaces. Esta suele ser la forma preferible de conectar clientes VPN, pero OpenVPN ofrece también la opción de utilizar `puntee` interfaces y clientes puente directamente en su LAN o de otro interno red. Esto puede hacer que los clientes remotos parecen estar en su red local. Sin embargo, el pfSense GUI no fue diseñado para dar cabida a tales escenarios. No ha sido un truco usado por algunos personas, pero tiene problemas significativos. Una opción útil estará disponible en algún momento - de verificación http://doc.pfsense.org/index.php/OpenVPN_Bridging para la información más reciente sobre OpenVPN puente.

Las 15.10 horas. Opciones de configuración personalizada

OpenVPN ofrece docenas de opciones de configuración, muchos más allá de los más utilizados campos que se presentan en la interfaz gráfica de usuario. Por ello, el cuadro de opciones de configuración personalizada existe. Usted puede llenar en un número ilimitado de opciones de configuración adicionales, separados por punto y coma. Esta sección cubre las opciones de uso más frecuente a medida de forma individual. No son muchos más, aunque rara vez se necesita. La OpenVPN página del manual [Http://openvpn.net/index.php/open-source/documentation/manuals/65-openvpn-20x-manpage.htmlDetalles] a todos. Ejercicio cuidado al añadir opciones de personalización, no hay validación de entrada que se aplica para garantizar la validez de opciones que se utilizan. Si una opción no se utiliza correctamente, el cliente OpenVPN o el servidor no se inicie. Puede ver los registros de OpenVPN en Estado → Los registros del sistema en la ficha OpenVPN para garantizar las opciones que se utilizan son válidas. Cualquier otra opción no válida se traducirá en un mensaje de registro `Opciones de error: opción no reconocida o parámetro que falta (s)` seguido por la opción que provocó el error.

15.10.1. Opciones de ruta

Para agregar rutas adicionales para un determinado cliente o servidor OpenVPN, se utiliza el **ruta** personalizado opciones de configuración. En el ejemplo siguiente se agrega una ruta para 10.50.0.0/24.

ruta 10.50.0.0 255.255.255.0

Para añadir varias rutas, separadas con un punto y coma:

10.50.0.0 255.255.255.0 ruta; ruta 10.254.0.0 255.255.255.0

La **ruta** opción de configuración se utiliza para añadir rutas a nivel local. Para un servidor OpenVPN configuración con PKI, también puede empujar rutas adicionales a los clientes. Para impulsar las vías de 10.50.0.0/24 y 10.254.0.0/24 a todos los clientes, utilice la siguiente opción de configuración personalizada.

push "route 10.50.0.0 255.255.255.0" empujar "la ruta 10.254.0.0 255.255.255.0 "

15.10.1.1. La reorientación de la puerta de enlace predeterminada

OpenVPN también le permite cambiar la puerta de enlace predeterminada del cliente para el OpenVPN conexión, por lo que todo el tráfico desde el cliente es empujado a través de la VPN. Esto es grande para no confiables redes locales, tales como puntos de acceso inalámbrico, ya que proporciona protección contra numerosos ataques de que son un riesgo en redes no confiables. Para ello, agregue la opción personalizada siguientes:

push "redirect-gateway DEF1"

También puede escribir esto como una opción personalizada en el cliente mediante el uso de **redireccionamiento de puerta de enlace** **DEF1** sin especificar **empuje**. (Nota: la opción es las letras "**def**"Seguido por el dígito, no la letra "L".)

15.10.2. Especificación de la interfaz

OpenVPN servidores y los clientes utilizan una interfaz de tipo túnel para cada conexión. Esto es todo automáticamente a cargo de pfSense, pero puede especificar el nombre del dispositivo a utilizar. Algunos usuarios prefiere especificar esto, por ejemplo, para asignar la interfaz de OpenVPN en una interfaz opcional en pfSense reglas para el filtrado se puede aplicar a tráfico entrante OpenVPN. Para ello, agregar un opción como **dev tun0**. Cada cliente y el servidor OpenVPN necesita usar un dispositivo único, por lo que la siguiente configuración posterior OpenVPN especificaría **dev tun1**, El incremento de un para cada servidor adicional o cliente.

15.10.3. Uso de aceleradores de hardware criptográfico

Si usted tiene un acelerador de cifrado de hardware tales como `hifn` a bordo de la tarjeta o `glxsb` en el plataforma ALIX, añadir la opción personalizada **motor cryptodev** para tomar ventaja de este hardware con OpenVPN. También debe utilizar un algoritmo de cifrado con el apoyo de su acelerador. Por `glxsb`, Que sólo es AES-CBC-128. Moderno Hifn tarjetas como la Soekris vpn1411 apoyo 3DES y 128 192, y 256 bits AES.

15.10.4. Especificar la dirección IP que puede utilizar

La **locales** opción personalizada le permite especificar la dirección IP del servicio OpenVPN va a utilizar. Esto puede ser una dirección IP, tales como **locales 1.2.3.4**, O un nombre de dominio completo, tales como:

myopenvpn.dyndns.org locales

Esto se utiliza sobre todo en escenarios multi-WAN, como se describe en Sección 15.7, "OpenVPN y Multi-WAN ", o en combinación con personalidades CARP.

15.11. Solución de problemas de OpenVPN

Si encuentra problemas al intentar utilizar OpenVPN, esta sección proporciona información sobre la solución de los problemas más comunes se encuentran los usuarios.

15.11.1. Hay algunos equipos en el trabajo, pero no todos

Si el tráfico entre máquinas sobre las funciones de VPN correctamente, pero algunos hosts no, esto es normalmente una de las cuatro cosas.

1. Falta, puerta de enlace predeterminada incorrecta o ignorado - Si el dispositivo no tiene una puerta de enlace predeterminada,
   o tiene uno que apunta a algo distinto de pfSense, no sabe cómo llegar adecuadamente
   de nuevo a la red remota en la VPN. Algunos dispositivos, incluso con una puerta de enlace predeterminada se especifica,
   no usar esa puerta de enlace. Esto se ha visto en varios dispositivos integrados, incluyendo IP
   cámaras y algunas impresoras. No hay nada que podamos hacer al respecto que, aparte de conseguir el
   software en el dispositivo fijo. Usted puede verificar esto ejecutando tcpdump en el interfaz en el interior
   del servidor de seguridad conectado a la red que contiene el dispositivo. Solución de problemas con
   tcpdump
   se trata en Sección 25.5, "Uso de tcpdump desde la línea de comando". Si usted ve el tráfico que va
   a cabo dentro de la interfaz en el firewall, pero no las respuestas que vienen atrás, el dispositivo no está correctamente
   enrutamiento del tráfico de su respuesta (o podría ser que el bloqueo a través de un servidor de seguridad).
2. Máscara de subred incorrecta - Si la subred en uso en un extremo es 10.0.0.0/24 y el otro es
   10.254.0.0/24, y un host tiene una máscara de subred incorrecta de 255.0.0.0 o / 8, que nunca será capaz de
   comunicarse a través de la VPN, ya que piensa que la subred remota VPN es parte de los locales
   enrutamiento de red y por lo tanto no funcionará correctamente.
3. Servidor de seguridad - si hay un firewall en el host de destino, puede que no sea permitir las conexiones.
4. Las reglas de firewall en pfSense - garantizar las reglas en ambos extremos permiten el tráfico de red deseada.

15.11.2. Verifica en el OpenVPN registros

Vaya a Estado → Los registros del sistema y haga clic en la ficha OpenVPN para ver el OpenVPN registros.
Al conectar, OpenVPN registrará algo similar a lo siguiente (el siguiente número
`openvpn` será diferente, es el ID del proceso del proceso de OpenVPN hacer la conexión).

```
openvpn [32194]: UDPv4 vínculo remoto: 1.2.3.4:1194
openvpn [32194]: La conexión entre pares iniciado con 192.168.110.2:1194
openvpn [32194]: inicialización secuencia completa
```

Si no ve el `vínculo remoto` y `Pares de conexión iniciada` Mensajes
al tratar de conectar, la causa es probable que sea incorrecta configuración del cliente, por lo que el cliente es
no intentar conectar con el servidor correcto, incorrecto o reglas de bloqueo de firewall del cliente
conexión.

15.11.3. Asegúrese de que no se superponen conexiones IPsec

Debido a los lazos manera IPsec en el kernel de FreeBSD, cualquier acceso a una conexión IPsec se pongan en

venta
las subredes locales y remotas que se da cuando IPsec es activado (incluso si no está) hará que
el tráfico no se enrutan a través de la conexión OpenVPN. Las conexiones IPsec especificando
las mismas redes locales y remotas debe estar deshabilitada.

15.11.4. Verifica en el sistema de la tabla de enrutamiento

Examinar para diagnóstico → Rutas y revisión de las rutas agregó. Para VPN sitio a sitio, usted debe ver las rutas de la red remota (s) a la correspondiente `tonel` o `puntee` interfaz. Si las rutas falta o incorrecta, tu red local, red remota, o de opciones de personalización no son configurado correctamente. Si está utilizando una configuración de clave compartida y no PKI, asegúrese de que usted no está el uso de "empujar" los comandos en vez agregar rutas a ambos extremos el uso de "ruta" opciones de personalización, como en Sección 15.10.1, "Opciones de ruta".

15.11.5. Prueba de diferentes puntos de vista

Si la conexión se muestra como en los registros, pero no funciona en su LAN, prueba de la servidor de seguridad propio, en primer lugar mediante la interfaz en el interior se utiliza para la conexión OpenVPN (normalmente LAN) como la fuente de ping. Si eso no funciona, SSH en el servidor de seguridad y seleccione la opción 8 para un símbolo del sistema. Ejecutar **ping *x.x.x.x*** en la línea de comandos, en sustitución de *x.x.x.x* con un IP en el lado remoto de la VPN. Esto hará que el tráfico que se iniciará a partir de la IP de la `tonel` interfaz que es utilizado por OpenVPN. Esto puede ayudar a reducir problemas de enrutamiento en el red remota.

15.11.6. Trace el tráfico con tcpdump

Uso de tcpdump para determinar donde el tráfico se ve y donde no se es uno de los más útiles técnicas de solución de problemas. Comience con la interfaz interna (comúnmente LAN) en el lado donde el tráfico se está iniciando, el progreso a la `tonel` interfaz en dicho servidor de seguridad, entonces el `tonel` interfaz en el servidor de seguridad a distancia, y finalmente dentro de la interfaz en el servidor de seguridad a distancia. Determinar dónde el tráfico se ve y donde no se puede ayudar en gran medida en la reducción de hasta dónde está el problema encuentra. Captura de paquetes se trata en detalle en Capítulo 25, Captura de paquetes.

Capítulo 16. Traffic Shaper

De tráfico, o la red de calidad de servicio (QoS), es un medio de dar prioridad a la red el tráfico que atraviesa el servidor de seguridad. Sin tráfico, los paquetes son procesados en un primer / primero a partir de su firewall. Calidad de servicio ofrece un medio de dar prioridad a distintos tipos de tráfico, asegurando que los servicios de alta prioridad reciben el ancho de banda que necesitan antes de menor servicios prioritarios. La asistente Traffic Shaper en pfSense le da la capacidad para configurar rápidamente QoS para comunes escenarios y reglas personalizadas también se pueden crear para tareas más complejas. Para simplificar, el sistema de tráfico en pfSense también puede ser denominado como el "shaper", y el acto de tráfico la formación puede ser llamado "la formación".

16.1. Traffic Shaping Básico

Para aquellos de ustedes que no están familiarizados con el tráfico, es algo así como un guardia de seguridad en un exclusivo del club. El VIP (Very paquetes importantes) siempre que sea en primera y sin tener que esperar. El regulares paquetes tienen que esperar su turno en la fila, y "no deseables" los paquetes pueden estar fuera hasta después de la verdadera fiesta ha terminado. Al mismo tiempo, el club se mantiene a la capacidad y la sobrecarga nunca. Si hay más VIP venir más tarde, algunos paquetes regulares pueden necesitar ser arrojado a mantener el lugar de conseguir demasiado lleno de gente.

La forma en que la formación se lleva a cabo en pf, y por lo tanto pfSense, puede ser un poco contra-intuitivo en un primer momento debido a que el tráfico debe ser limitado en un lugar donde pfSense en realidad puede controlar la flujo. El tráfico entrante de Internet va a un host de la LAN (descargar) es en realidad forma de salir de la interfaz LAN del sistema de pfSense. De la misma manera, el tráfico va desde la LAN a Internet (subir) tiene la forma al salir de la WAN.

Hay colas de tráfico, y el tráfico de las normas de darles forma. Las colas son el ancho de banda en y las prioridades están realmente asignados. normas de tráfico configuración de control de la cantidad de tráfico se le asigna en las colas. Reglas para el trabajo formador de manera similar a las reglas del firewall, y permitir que se pongan en venta similares características. Si un paquete coincide con una regla modelador, se le asignará en las colas especificado por esa regla.

16.2. Lo que el Traffic Shaper puede hacer por usted

La idea básica de tráfico, subir y bajar las prioridades de los paquetes, es simple. Sin embargo, el número de formas en que este concepto puede ser aplicado es enorme. Estos son sólo algunos ejemplos comunes que han demostrado ser populares entre nuestros usuarios.

16.2.1. Mantenga navegación suave

enlaces asimétricos, donde la velocidad de descarga es diferente de la velocidad de subida, son comunes en estos días, especialmente con DSL. Algunos enlaces son tan fuera de balance que la descarga máxima la velocidad es casi inalcanzable, porque es difícil enviar ACK suficiente (reconocimiento) paquetes para mantener el tráfico que fluye. paquetes ACK se devuelven al remitente por el receptor host para indicar que los datos se recibió con éxito, y para señalar que está bien de enviar más. Si el remitente no recibe ACK de manera oportuna, TCP mecanismos de control de congestión entrará en funcionamiento y reducir la velocidad de la conexión.

Usted puede haber notado esta situación antes: Al cargar un archivo a través de ese vínculo, la navegación y la descarga se ralentiza o se detiene. Esto sucede porque la parte de carga del circuito está lleno de la carga de archivos, hay poco espacio para enviar los paquetes ACK que permiten descargas seguir fluyendo. Mediante el uso de la talladora de dar prioridad a los paquetes ACK, se puede lograr más rápido, más estable velocidades de descarga en los enlaces asimétricos.

Esto no es tan importante en los vínculos simétricos en la carga y la velocidad de descarga son las mismas, pero aún puede ser desriable si el ancho de banda de salida disponible es muy utilizado.

16.2.2. Mantenga VoIP llamadas claras

Si su voz sobre IP pide utilizar el mismo circuito que los datos, carga y descarga a continuación, puede degradar la calidad de la llamada. pfSense puede priorizar el tráfico de llamadas por encima de otros protocolos, y garantizar que el pide hacerlo a través de claridad sin romper, incluso si usted es el streaming de vídeo de alta definición de Hulu, al mismo tiempo. En lugar de la llamada ruptura, la velocidad de las transferencias de otros se reducido para dejar espacio para las llamadas.

16.2.3. Reducir el retraso de juego

También hay opciones para dar prioridad al tráfico asociadas a juegos en red. Al igual que en dar prioridad a las llamadas de VoIP, el efecto es que incluso si se descarga durante el juego, la respuesta momento del juego aún debe ser casi tan rápido como si el resto de su conexión se espera.

16.2.4. Mantenga las aplicaciones P2P en la comprobación

Al reducir la prioridad de tráfico asociados a puertos conocidos peer-to-peer, puede estar más fácil sabiendo que, incluso si los programas están en uso, que no pueden frenar el tráfico de su red. Debido a su menor prioridad, otros protocolos se verá favorecida por el tráfico P2P, que se limitará cuando cualquier otro servicio que necesita el ancho de banda.

16.3. Limitaciones del hardware

De tráfico se realiza con la ayuda de `Altq`. Desafortunadamente, sólo un subconjunto de todo ello apoyado tarjetas de red son capaces de usar estas características porque los controladores deben ser alterados para apoyar la formación. Las tarjetas de red siguientes son capaces de utilizar de tráfico, según el hombre Página `altq (4)`:

`edad (4)`,`cerveza (4)`,`uno (4)`,`ath (4)`,`Aue (4)`,`awi (4)`,`AEC (4)`,`bfe (4)`,`bge (4)`, `CC (4)`,`de (4)`,`ed (4)`,`em (4)`,`ep (4)`,`fxp (4)`,`gema (4)`,`hme (4)`,`ipw (4)`,`iwi (4)`, `jme (4)`,`-le (4)`,`msk (4)`,`mxge (4)`,`mi (4)`,`educación no formal (4)`,`NPE (4)`,`NVE (4)`,`ral (4)`, `Re (4)`,`rl (4)`,`ron (4)`,`sf (4)`,`sis (4)`,`sk (4)`,`ste (4)`,`stge (4)`,`udav (4)`, `naturales (4)`,`GVE (4)`,`vr (4)`,`wi (4)`, Y `xl (4)`.

16.4. Limitaciones de la Traffic Shaper aplicación en 1.2.x

Envolviendo una interfaz gráfica de usuario de todo el tráfico subyacente en la configuración de los componentes de pfSense demostrado ser un muy
funcionalidad difícil tarea, y falta en el sistema subyacente en algunas zonas también se limita su capacidades. La aplicación que existe en 1.2.x funciona bien, dentro de sus límites. El tráfico formador en pfSense 2.0 ha sido reescrito para hacer frente a estas limitaciones.

16.4.1. Sólo dos de interfaz de apoyo

El shaper sólo funciona correctamente con las implementaciones que consta de dos interfaces LAN y WAN. Multi-WAN, y redes con interfaces OPT otros no funcionan como se desea. El formador en 2.0 da cabida a múltiples interfaces correctamente.

16.4.2. El tráfico a la interfaz LAN afectados

El tráfico a la IP LAN está en la cola de la misma manera que el tráfico que atraviesa el firewall. Así que si su interfaz web utiliza el protocolo HTTPS, y la cola de conformador de tráfico de HTTPS se llena, se retrasará su el tráfico a la interfaz de gestión de la misma que si su solicitud HTTPS iban a salir a la De Internet. Si utiliza ping a la IP LAN de un sistema de seguimiento, puede ver un retraso significativo y la inquietud por esta misma razón.

Por extensión también se aplica a otros servicios ofrecidos por el router pfSense. Los usuarios de los calamares paquete de proxy dado cuenta de que sus clientes locales recibieron datos del proxy sólo a la velocidad de su red WAN, y por lo que nunca pareció ser el almacenamiento en caché de datos. De hecho, fue el almacenamiento en caché de datos, pero también la configuración del tráfico, al mismo tiempo.

16.4.3. No hay inteligencia de las aplicaciones

El molde no es capaz de diferenciar realmente entre los protocolos. Tráfico que utiliza el puerto TCP 80 se considera como HTTP, si es realmente HTTP o es una aplicación P2P utilizando el puerto 80. Esto puede siendo un problema importante en algunos entornos.

16.5. Configuración de la Traffic Shaper Con la Asistente

Se recomienda que configure el conformador de tráfico por primera vez con el asistente, que le guiará en el proceso. Debido a la complejidad de las colas de la talladora y las normas, no es una buena idea para tratar de empezar de cero por su cuenta. Si necesita reglas personalizadas, paso a paso el asistente y aproximarse a lo que usted necesita, entonces hacen las reglas personalizadas después. Cada será la configuración de pantalla única colas, y las reglas que controlan lo que el tráfico se asigna a los colas. Si desea configurar todo manualmente, basta con especificar la velocidad WAN la primera pantalla, a continuación, haga clic en Siguiente en todas las pantallas restantes sin tener que configurar nada.

16.5.1. Inicio del Asistente

Para empezar a utilizar el Asistente para Traffic Shaping, haga clic en el Servidor de seguridad → Traffic Shaper. El asistente se iniciará automáticamente como en Figura 16.1, "Inicio del Asistente para Shaper". Si ha completado el asistente de configuración de antes, o tiene reglas personalizadas, en su lugar aparecerá la lista de las normas de shaper. Para borrar las reglas existentes talladora y empezar de cero, haga clic en la ficha Asistente EZ Shaper que relanzará el asistente de pre-llenado con su configuración actual. Al término de cada pantalla de la asistente, haga clic en Siguiente para continuar a la siguiente página.

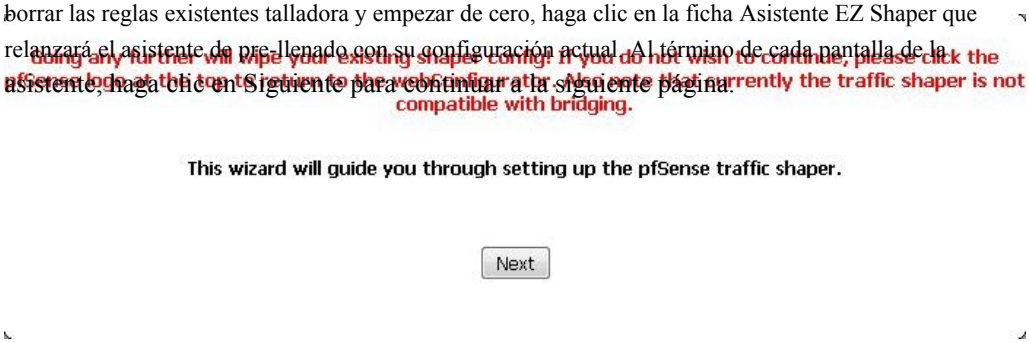


Figura 16.1. Inicio del Asistente para Shaper

16.5.2. Redes y velocidades

Esta pantalla, como se muestra en Figura 16.2, "Configuración Shaper", es donde se configura el interfaces de red que será el interior y exterior, desde el punto de vista del formador, a lo largo de con las velocidades de carga y descarga. Dependiendo de tu tipo de conexión, la velocidad del enlace real no puede ser la velocidad real de utilización. En el caso de PPPoE, usted tiene no sólo de arriba PPPoE, pero también de cabeza del enlace de red subyacente ATM se utiliza en la mayoría de las implementaciones de PPPoE. Según algunos cálculos, entre la cabeza del cajero automático, PPPoE, IP y TCP, puede perder hasta un 13% de la velocidad del enlace anunciado.

En caso de duda de lo que establezca la velocidad, ser un poco conservador. Reducir en 10 a 13% y el trabajo el camino de vuelta hacia arriba. Si usted tiene un 3Mbit / s de línea, se establece alrededor de 2700 y probarlo. Siempre se puede modifica la cola de los padres resulta más tarde y ajustar la velocidad. Si la ponemos bajo, la conexión estar al máximo en exactamente la velocidad que ha establecido. Mantenga empujando hacia arriba más alto hasta que ya no recibe cualquier beneficio de rendimiento.

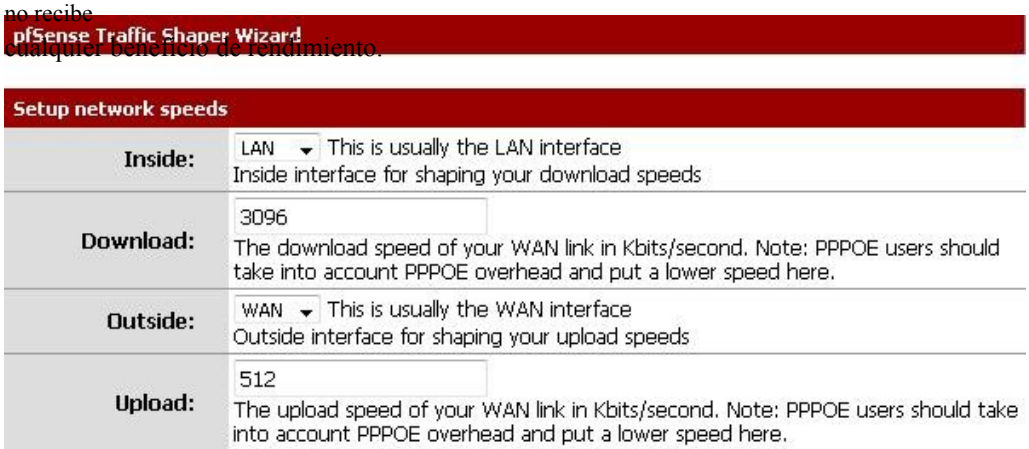


Figura 16.2. Modelador de configuración

16.5.3. Voz sobre IP

Hay varias opciones disponibles para manejar el tráfico de llamadas VoIP, que se muestra en Figura 16.3, "La Voz sobre IP ". La primera opción, la prioridad del tráfico de voz sobre IP, se explica por sí mismo. Permitirá la priorización del tráfico VoIP y este comportamiento puede ser ajustado por la configuración de otros a continuación. Hay pocos proveedores bien conocidos, incluyendo Vonage, VoicePulse, PanasonicTDA, y servidores de Asterisk. Si usted tiene un proveedor diferente, puede elegir **Genérico**, O anular

este valor con el campo de direcciones mediante la introducción de la IP de su teléfono VoIP o un alias que contiene
las direcciones IP de todos sus teléfonos.

También puede elegir la cantidad de ancho de banda para garantizar a sus teléfonos VoIP. Esto
varían en función de la cantidad de teléfonos que tiene, y cuánto ancho de banda de cada sesión se utilizan.

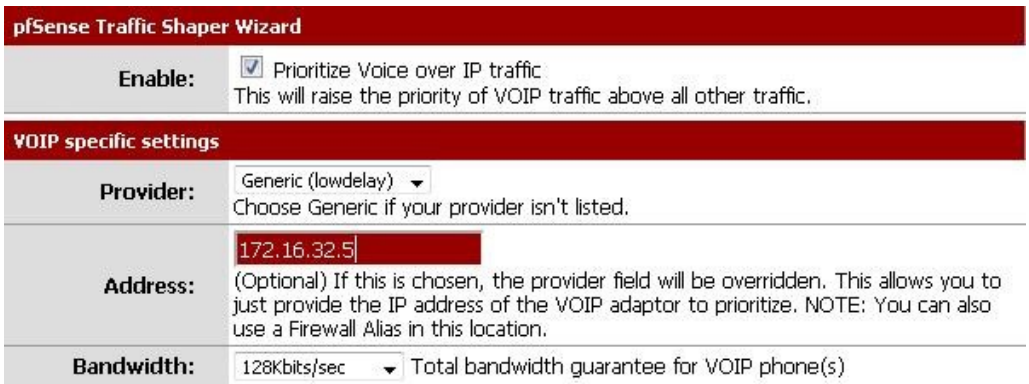


Figura 16.3. Voz sobre IP

16.5.4. Pena de Caja

La caja de la pena, se muestra en Figura 16.4, "caja de la pena", es un lugar al que se puede relegar a
mal comportamiento usuarios o dispositivos que de otra manera consumen más ancho de banda de lo deseado. Estos los usuarios se les asigna un ancho de banda de la tapa dura que no puede exceder. Verifica en el Penalizar IP o Alias para activar la función, introduzca una dirección IP o alias en el cuadro de dirección, y luego entrar en carga y límites de descarga en kilobits por segundo en sus cajas respectivas.

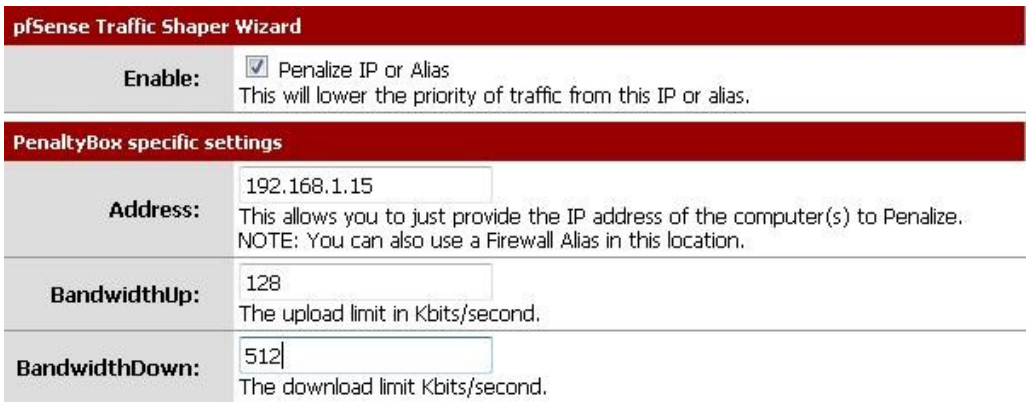


Figura 16.4. Pena de Caja

16.5.5. Redes peer-to-Peer

En la siguiente pantalla, se muestra en la Figura 16.5, "Peer-to-peer", le permitirá establecer controles sobre muchos peer-to-peer (P2P), protocolos de red. Por diseño, los protocolos P2P utilizará todos los ancho de banda disponible a menos que los límites se ponen en marcha. Si usted espera que el tráfico P2P en la red, que Es una buena práctica para garantizar que el resto del tráfico no se degrada debido a su uso. Para sancionar P2P tráfico, en primer lugar compruebe Baja prioridad del tráfico peer-to-Peer.

Muchas de las tecnologías P2P deliberadamente tratar de evitar la detección. Bittorrent es especialmente culpable de esto comportamiento. A menudo utiliza los puertos no estándar o azar, o de los puertos asociados con otros protocolos. Puede marcar la opción p2pCatchAll lo que hará que el tráfico no reconocidos que se supone como el tráfico P2P y su prioridad disminuido. Puede establecer límites estrictos de ancho de banda para este el tráfico por debajo de la regla de cajón de sastre. La carga y descarga de los límites de ancho de banda se establecen en Kilobits por segundo.

Las opciones restantes se componen de varios conocidos protocolos P2P, más de 20 en total. Compruebe cada uno que desea ser reconocido.

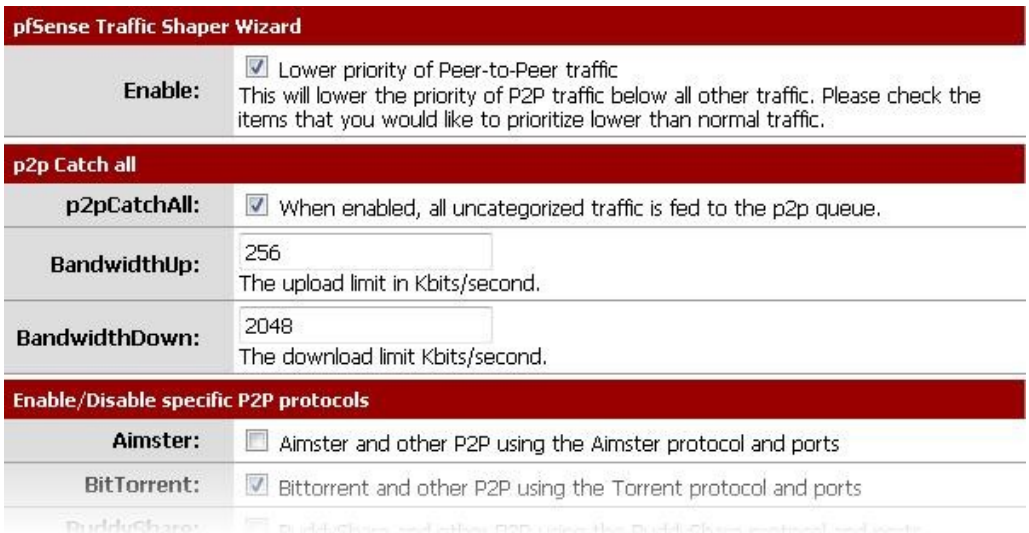


Figura 16.5. Redes peer-to-Peer

16.5.6. Red de Juegos

Muchos juegos se basan en una baja latencia para ofrecer una buena experiencia de juego online. Si alguien trata de
para descargar archivos de gran tamaño o los parches del juego durante el juego, que el tráfico puede tragar con facilidad la paquetes asociados con el juego en sí y causar retraso o desconexiones. Al marcar la opción
para priorizar el tráfico de la red de juego, como se ve en Figura 16.6, "Red de Juegos", Puede aumentar la prioridad del tráfico de juego de modo que será transferido primero y dado un trozo de garantía ancho de banda. Hay muchos juegos en la lista, marque todas las que deben ser priorizadas. Si su juego no aparece en esta lista todavía puede comprobar un juego similar, de modo que usted tendrá un norma de referencia que puede ser modificada más adelante.

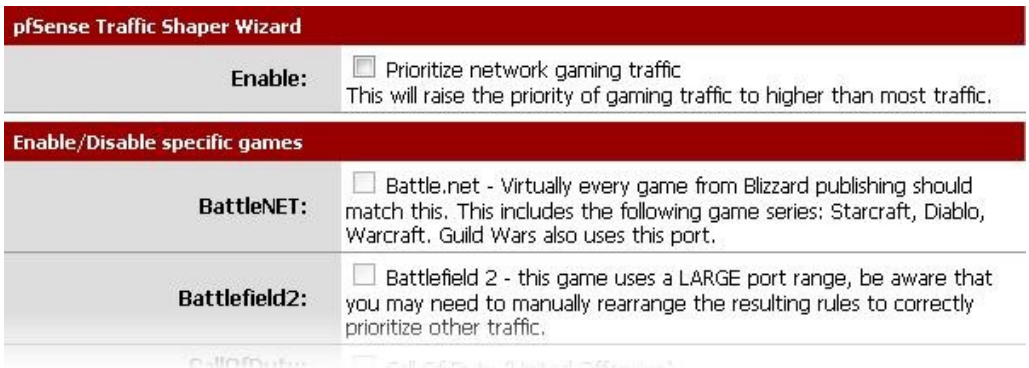


Figura 16.6. Red de Juegos

16.5.7. Subir o bajar otras aplicaciones

La pantalla de configuración última del asistente formador, visto en Figura 16.7, "Subir o Bajar Otras aplicaciones ", Las listas de muchas otras aplicaciones comúnmente disponibles y los protocolos. ¿Cómo estas protocolos se manejan dependerá del ambiente que este router pfSense se protege.
Algunos de estos puede ser deseado, y otros no. Por ejemplo, en un entorno corporativo,
es posible que desee bajar la prioridad de tráfico no interactivos como el correo, donde una desaceleración
no es observado por nadie, y elevar la prioridad de los servicios interactivos como RDP, donde los pobres
el rendimiento es un impedimento para la capacidad de las personas a trabajar. En una casa, streaming multimedia puede ser más importante, y otros servicios puede ser bajada. Habilitar la opción para la creación de redes Otros protocolos, a continuación, seleccionar y elegir de la lista.
Hay más de 25 protocolos diferentes para escoger, y cada uno se puede dar una **Superior prioridad**,**Menor prioridad**, O la izquierda en el **Prioridad por defecto**. Si ha activado p2pCatchAll, tendrá que utilizar esta pantalla para asegurarse de que estos protocolos se reconocen y se trata normalmente, en lugar de penalizado por la regla p2pCatchAll por defecto.

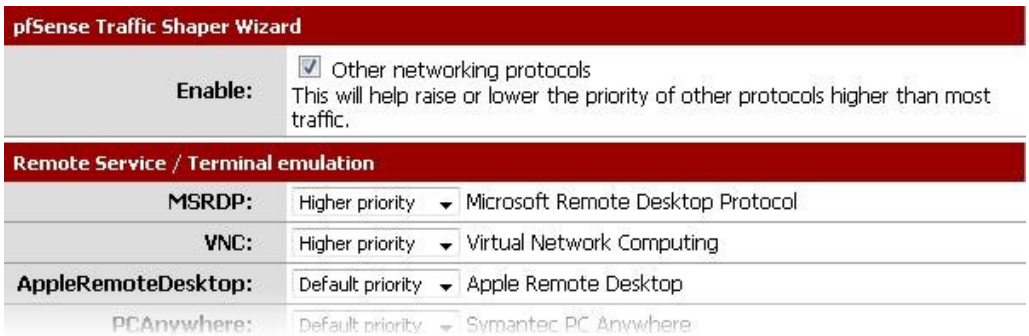


Figura 16.7. Subir o bajar otras aplicaciones

16.5.8. Fin del Asistente de

Todas las reglas y las colas de ahora será creado, pero aún no en uso. Al pulsar el botón Finalizar en la pantalla final, las normas serán cargados y activos.

Conformación ahora debe activarse para todas las conexiones nuevas. Debido a la naturaleza de estado de la talladora, sólo nuevas conexiones de tráfico se han aplicado. Para que ello está plenamente activa en todos los conexiones, debe borrar los estados. Diagnóstico Para ello, visite → Estados, haga clic en el botón de reinicio ficha Estados, visita mesa Firewall de Estado, a continuación, haga clic en Restablecer.

16.6. Monitoreo de las colas

Con el fin de estar seguros de que la modulación del tráfico está funcionando según lo previsto, puede ser monitoreado por la navegación
al Estado → Colas. Como puede verse en Figura 16.8, "Colas de WAN básica", Esta pantalla se muestran cada cola de lista por su nombre, su uso actual, y algunas estadísticas de los demás.

Figura 16.8. Las colas de base WAN

La barra gráfica muestra cómo "llena" es una cola. La tasa de datos en la cola se muestra en la dos paquetes por segundo (pps) y los bits por segundo (b / s). Toma suceder cuando un país vecino cola no está llena y la capacidad es tomado de allí cuando sea necesario. Suelta de tráfico cuando ocurren en una cola se cae a favor del tráfico de mayor prioridad. Es normal ver a gotas, y lo hace no significa que de una conexión se cae, a un paquete. Por lo general, un lado de la conexión ver que un paquete se perdió y vuelva a enviar a continuación, a menudo ralentización en el proceso para evitar futuras gotas. El contador indica suspende cuando una acción de retardo que sucede. El contador no se suspende utilizado por el programador de la configuración empleada por pfSense en 1.2.x, y probablemente debería ser cero.

16.7. Personalización avanzada

Después de usar el asistente de shaper, es posible que las normas que genera no se ajustan a sus necesidades. Si lo desea, para dar forma a un servicio que no es manejada por el asistente, un juego que utiliza una diferente puerto, o puede haber otros servicios que necesitan limitada. Una vez que las normas básicas que se han creado por el asistente, debe ser relativamente fácil de editar o copiar las reglas y crear informes personalizados por su cuenta.

16.7.1. Edición de colas Shaper

Como se menciona en el resumen, las colas son donde el ancho de banda y las prioridades son en realidad asignados. Cada cola se le asigna una prioridad, de 0-7. Cuando hay una sobrecarga de tráfico, el mayor número se prefieren las colas (por ejemplo, 7) sobre las colas de números más bajos (por ejemplo 1). Cada la cola se le asigna un límite de ancho de banda duro, o un porcentaje de la velocidad total del enlace. La colas también se pueden asignar otros atributos que controlan cómo se comportan, como ser de baja retrasar o evitar la congestión que tiene ciertos algoritmos aplicados. Las colas pueden ser modificados por va a cortafuegos → Traffic Shaper, y haciendo clic en la ficha Colas. Una lista de reglas se parecen, como que en Figura 16.9, "Shaper colas de tráfico de la lista"

colas de edición no es para los débiles de corazón. Puede ser una tarea compleja y con resultados de gran alcance,
pero sin conocimiento profundo de los valores involucrados, lo mejor es seguir con las colas
generado por el asistente y modificar su configuración, en lugar de tratar de hacer otros nuevos desde cero.

Al ver la lista de las colas, cada cola se mostrarán junto con los indicadores asociados
la cola, su prioridad, asignar ancho de banda, y el nombre. Para editar una cola, haga clic en, y para eliminar
cola, haga clic en. Usted no debe tratar de eliminar una cola si aún está siendo referenciado por una regla
Para reordenar las colas en la lista, marque la casilla al lado de la cola para ser trasladado, a continuación, haga clic en el
botón en la fila que debe estar por debajo de las colas reubicados. Al pasar el ratón
más puntero, una barra gruesa aparecerá para indicar que las normas se insertan. El orden
de las colas es estrictamente cosmética. Para añadir una nueva cola, haga clic en la parte inferior de la lista.

Figura 16.9. Traffic Shaper colas Lista

Durante la edición de una cola, cada una de las opciones deben ser consideradas cuidadosamente. Si usted está buscando
Para obtener más información sobre estos valores que se menciona aquí, visite el PF colas de paquetes
Priorización y preguntas más frecuentes [] Http://www.openbsd.org/faq/pf/queueing.html.[1] Los mejores disponibles
planificador es jerárquica Feria de Servicio curva (HFSC), y que es el único disponible en
1.2.x. pfSense

La configuración de ancho de banda debe ser una fracción del ancho de banda disponible en la cola de los padres, pero también se debe establecer con la conciencia de las colas de vecinos. Al utilizar porcentajes,
el total de todas las colas en uno de los padres dado que no puede superar el 100%. Cuando se utiliza límites absolutos,
los totales no pueden exceder el ancho de banda disponible en la cola de los padres.

La prioridad puede ser cualquier número entre 0-7. Colas con un mayor número son preferibles cuando hay una sobrecarga, por lo que situar las colas en consecuencia. Por ejemplo, el tráfico de VoIP debe ser de las más altas prioridad, por lo que se debe establecer en un 7. Peer-to-peer tráfico de la red, que se puede retrasar en favor
de otros protocolos, debe fijarse en 1.

[1] http://www.openbsd.org/faq/pf/queueing.html y también está disponible en el libro de PF de OpenBSD Packet Filter.

El nombre de una cola debe estar entre 1-15 caracteres y no puede contener espacios. La mayoría de los convención común es comenzar con el nombre de una cola con la letra "q" para que pueda ser más identificar fácilmente en el conjunto de reglas.

Hay seis diferentes opciones de Programador que se pueden establecer para una cola dada:

• Poner en cola por defecto

Selecciona esta cola por defecto, el que se encargará de todos los paquetes sin igual. Cada interfaz debe tener una y sólo una de colas por omisión.

• ACK / bajo retardo de cola (ACK)

Por lo menos una cola por cada interfaz debe tener esta serie. Normalmente, esto se reserva para - como el nombre lo indica - paquetes ACK que necesitan ser tratadas de forma especial con una prioridad alta.

• Detección Temprana al Azar (RED)

Un método para evitar la congestión en un enlace, sino que activamente intenta garantizar que la cola se no se llenan. Si el ancho de banda está por encima del máximo dado por la cola, las gotas se producirá. Además, las gotas se puede producir si el tamaño medio de la cola se acerca al máximo. Paquetes perdidos se eligen al azar, por lo que el ancho de banda más en el uso de una conexión determinada, es más probable es ver las gotas. El efecto neto es que el ancho de banda es limitado de manera justa, fomentando un equilibrio. RED sólo debe usarse con conexiones TCP ya TCP es capaz de manejar paquetes perdidos, y puede volver a enviar cuando sea necesario.

• Detección Temprana al Azar entrada y de salida (RIO)

Permite RED con entrada / salida, que se traducirá en un promedio de colas de haber sido mantenido y cotejarse con los paquetes entrantes y salientes.

• Notificación explícita de congestión (ECN)

Junto con la RED, que permite el envío de mensajes de control del acelerador que si las conexiones ambos extremos ECN apoyo. En lugar de dejar caer los paquetes como RED normalmente lo hace, se establece una bandera en el paquete que indica la congestión de la red. Si la otra parte ve y obedece a la bandera, la velocidad de la transferencia en curso se reducirá.

• Se trata de una cola de padres

Permite a esta cola para ser elegido como uno de los padres de otras colas.

La curva de Servicio (sc) es donde usted puede ajustar los requisitos de ancho de banda para esta cola.

• m1

Burstable límite de ancho de

banda

• d

Plazo para la explosión de ancho de banda, se especifica en milisegundos. (Por ejemplo, 1000 = 1 segundo)

• m2

Normal límite de ancho de banda

Por ejemplo, usted necesita m1 ancho de banda dentro d tiempo, pero un máximo normal de m2. En el tiempo inicial establecido por d, m2 no está marcada, sólo m1. Después d ha expirado, si el tráfico sigue estando por encima
m2, que se forma. Por lo general, m1 y D se dejan en blanco, por lo que sólo se comprueba m2.
Cada uno de estos valores se puede establecer para los siguientes usos:

• Límite superior

Ancho de banda máximo permitido para la cola. Va a hacer difícil la limitación de ancho de banda. El m1 parámetro aquí también se puede utilizar para limitar explosión. En el plazo d no obtendrá más
m1 de ancho de banda.

• Tiempo Real

Mínimos garantizados de ancho de banda de la cola. Esto sólo es válido para las colas de niños. El m1 parámetro siempre se cumple en plazo d, y M2 es el máximo que esta disciplina
se permita que se use.

• Compartir Enlace

La cuota de ancho de banda de una cola atrasados. A compartir ancho de banda entre las clases si el Real Tiempo garantías se han cumplido. Si establece el valor de m2 para Compartir Enlace, se reemplazar la configuración de ancho de banda de la cola. Estos dos valores son iguales, pero si ambos son
conjunto y comparte Link m2 se utiliza.

Mediante la combinación de estos factores, una cola obtendrá el ancho de banda especificado por el Real factores de tiempo,
además de los de Enlace de Acciones, hasta un máximo del límite superior. Se puede tomar un montón de prueba y error, y tal vez mucho de la aritmética, pero puede valer la pena para asegurar que su tráfico se rige
como mejor le parezca. Para obtener más información sobre m1, d, y m2 valores para diferentes escenarios, visite el pfSense Traffic Shaping foro [Http://forum.pfsense.org/index.php/board, 26.0.html].
Por último, si se trata de una cola de niños, seleccione la cola de los Padres de la lista. Haga clic en Guardar para guardar la cola
configuración y volver a la lista de la cola, a continuación, haga clic en Aplicar cambios para volver a cargar las colas y activar
los cambios.

16.7.2. Edición de Reglas Shaper

normas de tráfico configuración de control de la cantidad de tráfico se le asigna en las colas. Si un paquete coincide con un tráfico
regla de la talladora, se le asignará a la cola especificada por esa regla. se pongan en venta de paquetes se controla de manera similar a las reglas del firewall, pero con cierto control adicional de grano fino. La edición del shaper normas, ir a Firewall de → Traffic Shaper, y haga clic en la ficha Reglas. En esa pantalla, se muestra en la Figura 16.10, "Shaper Reglas tráfico de la lista", Las normas existentes se mostrarán en la interfaz de dirección, protocolo, origen, destino, colas de destino, y el nombre.

En esta pantalla también se encuentra el control maestro para dar forma. Desactive la opción Habilitar conformador de tráfico para desactivar
el formador de tráfico, a continuación, haga clic en Guardar. Para eliminar las reglas y las colas creadas por el shaper de tráfico,
y restablecer el formador a los valores predeterminados, haga clic en Quitar asistente. La próxima vez que visite firewall →
Traffic Shaper, el asistente se iniciará de nuevo.

Para editar una regla, haga clic en, y para eliminar, haga clic en regla. Las reglas se pueden mover hacia arriba o hacia abajo una fila en
haciendo clic para subir o para bajar. Para reordenar varias reglas en la lista, visita
la casilla junto a las reglas que deberán ser trasladados, a continuación, haga clic en el botón de la fila que debe estar por debajo de las normas reubicados. Las normas se moverá por encima de la fila elegida.
Usted puede hacer una nueva norma basada en otra regla existente, haga clic en junto a la fila con el regla que desea copiar. Se le presenta una pantalla de edición de reglas pre-llenado con
los detalles de la norma existente. Para agregar una nueva regla en blanco, haga clic en la parte inferior de la lista.

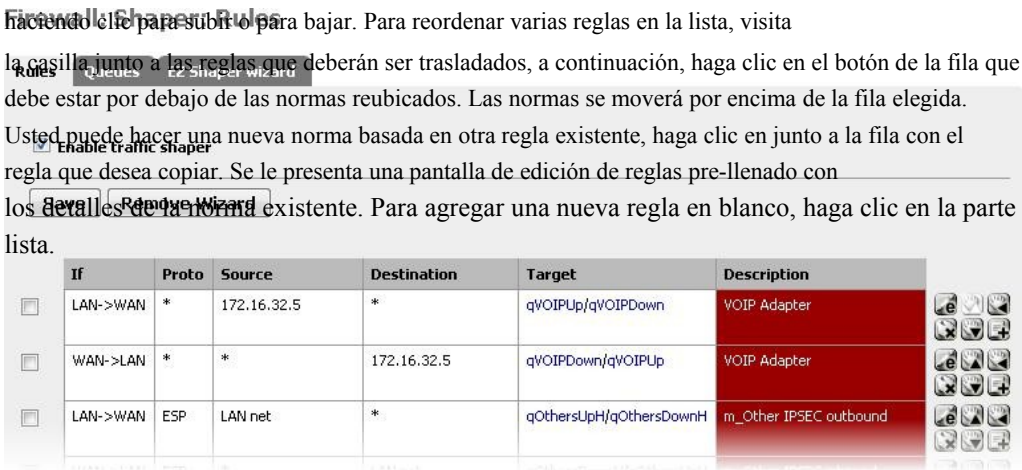


Figura 16.10. Reglas Traffic Shaper Lista

Cada regla tiene varios criterios de coincidencia que ayudará a garantizar que el tráfico adecuado se alimenta en las colas adecuadas. Antes de configurar las opciones de igualar, sin embargo, las colas de destino debe ser definido. Debe establecer tanto una cola de salida y una cola de entrada. Los paquetes que coincidan con esta norma de la dirección de salida caerá en la cola de salida, y los paquetes que coincidan con esta regla en la dirección entrante caerán en la cola de entrada. El camino del paquete se establece mediante la elección En un interfaz de la interfaz de entrada y de salida.

Ahora los criterios de coincidencia real comienza. La mayoría de estas opciones le resultará familiar a partir del servidor de seguridad

reglas. Para más información sobre cómo establecer el origen de Protocolo, y el destino, nos remitimos a Capítulo 6, Servidor de seguridad. Por ahora nos centraremos en qué se establecería estos en lugar de la forma. ¿Qué campos para establecer dependerá de la trayectoria implícita en los interfaces de entrada y salida.

Por ejemplo, si el tráfico va a ser originarios de un host de la LAN, la interfaz debe en ser LAN, y la Fuente se establecería en la dirección o subred del host LAN. Si el tráfico se va a una ubicación específica, establecer el destino en consecuencia, lo contrario, seleccione **Cualquier**. Por el tráfico se pongan en venta de servicios específicos, debe configurar el rango de puerto de destino adecuada. En este ejemplo, para que coincida con el tráfico HTTP, deje el rango de puertos de origen establecida en **Cualquier**, Y establecer el Rango de puerto de destino a HTTP. Rara vez es necesario establecer un puerto de origen, ya que suelen ser elegido al azar.

El tráfico se va emparejado dentro y fuera de forma predeterminada, pero puede utilizar la opción de dirección para limitar este comportamiento. Recuerde, sin embargo, que esto se establece desde la perspectiva del cortafuegos.

IP Tipo de Servicio (TOS) "bits de precedencia" se puede utilizar para capturar los paquetes que han sido marcadas de manejo especial. Hay tres configuraciones disponibles aquí, y cada uno de ellos puede tener uno de tres valores. Los tres campos indican una solicitud de retardo bajo, alto rendimiento o alta confiabilidad. Para cada uno de estos, sí significa que la bandera debe ser establecido. No significa que la bandera no debe ser fijado. No les importa significa que se tendrá en cuenta.

Un subconjunto de las banderas TCP que también se pueden comparar. Éstos indican diversos estados de una conexión (o la falta de ella). Pueden ser emparejado en el si o no se establece explícitamente, se aclaró, o bien (No importa).

- SYN - Sincronizar números de secuencia. Indica que un nuevo intento de conexión.
- ACK - Indica aceptación de los datos. Como se señaló anteriormente, estas son las respuestas para que el conocer los datos del remitente se recibió en Aceptar.
- FIN - Indica que no hay más datos del remitente, el cierre de una conexión.
- RST - restablecer la conexión. Este indicador se establece cuando en respuesta a una solicitud para abrir una conexión en un puerto que no tiene ningún demonio de escucha. También se puede ajustar por el software de servidor de seguridad para la espalda conexiones no deseadas.

- PSH - Indica que los datos deben ser empujados o enrojecida, incluidos los datos en este paquete, por pasar los datos a la aplicación.
- URG - Indica que el campo de urgencia es importante, y este paquete debe ser enviado antes datos que no es urgente.

El último campo, la descripción, es libre de texto y se utiliza para identificar esta regla. Tal vez le resulte útil indicará cuál es la intención de la cola es (nombre de la aplicación o protocolo), así como la dirección de la regla se establece para que coincida.

Al combinar el mayor número de estos parámetros según sea necesario, debería ser posible para que coincida con casi cualquier tráfico que tendría que hacer cola. Haga clic en Guardar para terminar y volver a la lista de reglas, a continuación, haga clic en Aplicar cambios para volver a cargar las reglas y activarlos.

16.8. Solución de problemas de Shaper

Traffic Shaping / QoS es un tema complicado, y puede resultar difícil de hacerlo bien la primera vez. Hay algunos errores comunes que la gente caiga sobre, que se tratan en esta sección.

16.8.1. ¿Por qué no el tráfico de BitTorrent va a la cola de P2P?

Bittorrent es conocido por no usar mucho en el camino de los puertos estándar. Los clientes pueden declarar que otros puertos deben utilizar para llegar a ellos, lo que significa un caos para los administradores de red intentando para rastrear el tráfico basado en el puerto solo. En 1.2.x, pfSense no tiene manera de examinar la los paquetes para contar lo que el programa de tráfico parece ser, por lo que se ve obligado a confiar en los puertos. Esta es la razón por puede ser una buena idea utilizar la regla de P2P Catchall, y / o establecer reglas para cada tipo de tráfico que quiere, y tratar su cola predeterminada por baja prioridad.

16.8.2. ¿Por qué no es el tráfico a los puertos abiertos por UPnP correctamente cola?

Tráfico permitido en el demonio UPnP va a terminar en la cola predeterminada. Esto sucede porque las reglas generadas dinámicamente por el demonio de UPnP no tiene ningún conocimiento de las colas a menos que UPnP está configurado para enviar el tráfico en una cola específica. Dependiendo de lo que han con UPnP en su entorno, esto puede ser el tráfico de baja prioridad como Bittorrent, o de alta prioridad tráfico como consolas de juegos o programas de chat de voz como Skype. La cola se puede establecer por ir a Servicios → UPnP y entrar en un nombre de la cola en el campo de Traffic Shaper cola.

16.8.3. ¿Cómo puedo calcular cuánto ancho de banda para asignar a las colas de confirmación?

Este es un tema complejo, y la mayoría de las personas pasar por alto que ya sólo adivinar un valor lo suficientemente alto.

Para una explicación más detallada con las fórmulas matemáticas, comprobar la Traffic Shaping sección de los foros pfSense [http://forum.pfsense.org/index.php/board,] 26.0.html.[2] Hay una pegajosa mensaje en ese foro que describe el proceso con gran detalle, y también hay una descarga hoja de cálculo que se puede utilizar para ayudar a facilitar el proceso.

16.8.4. ¿Por qué no <x> forma adecuada?

Al igual que con otras preguntas de esta sección, esto tiende a suceder debido a las normas consignarán bien internamente o por otros paquetes que no tienen conocimiento de las colas. Dado que no se especifica la cola una norma, termina en la cola por defecto o de la raíz, y de forma no. Puede que tenga que desactivar la WebGUI / ssh normas anti-bloqueo y tal vez incluso sustituir el valor por defecto de LAN → CUALQUIER reglas del firewall
con más opciones específicas. En el caso de paquetes, es posible que necesite ajustar la forma en su defecto cola se maneja.

2http://forum.pfsense.org/index.php/board, 26.0.html

Capítulo 17. Servidor de equilibrio de carga

Dos tipos de funcionalidad de balanceo de carga están disponibles en pfSense: Puerta de enlace y el servidor.

Gateway

balanceo de carga permite la distribución del tráfico de Internet enlazados a través de múltiples conexiones WAN. Para obtener más información sobre este tipo de balanceo de carga, consulte Capítulo 11, Múltiples conexiones WAN.

equilibrio de carga del servidor que permite distribuir el tráfico a múltiples servidores internos para la carga distribución y redundancia, y es el tema de este capítulo.

equilibrio de carga del servidor que permite distribuir el tráfico entre varios servidores internos. Es muy de uso común con los servidores web y servidores SMTP aunque puede ser utilizado para cualquier servicio que utiliza TCP.

Mientras pfSense ha sustituido de gama alta, alta balanceadores de carga de los costos comerciales incluyendo BigIP, Cisco LocalDirector, y más en entornos de producción seria, 1.2.x pfSense no es tan tan potente y flexible de estas soluciones. No es adecuado para instalaciones que requieren flexible de seguimiento y configuración de equilibrio. Para el control de TCP, simplemente comprueba que el especifica el puerto TCP está abierto. En el caso de un servidor web, el servidor no puede devolver cualquier respuestas HTTP, o los inválidos, y no hay manera de determinar esto. Para grandes o complejos despliegues, normalmente se desea una solución más potente. Sin embargo, para las necesidades básicas, el funcionalidad disponible en trajes de pfSense innumerables sitios muy bien.
Actualmente estamos revisando las opciones para un equilibrador de carga más capaz para la versión 2.0.

17.1. Explicación de las opciones de configuración

Hay dos partes de la configuración del equilibrador de carga del servidor. Virtual Server Piscinas definir la lista de servidores para ser utilizado, lo que se escucha en el puerto, y el método de monitoreo para ser utilizado. Los servidores virtuales definir el IP y el puerto para escuchar, y la piscina adecuada para dirigir la próxima tráfico a que la propiedad intelectual y el puerto.

17.1.1. Piscinas de servidor virtual

Para configurar el servidor virtual de Piscinas, vaya a Servicios → Equilibrador de carga. Haga clic para añadir una nueva
piscina. Cada una de las opciones de esta página se discute aquí.

• Nombre - Escriba un nombre para el grupo de aquí. El nombre es la forma en la piscina se hace referencia más adelante, cuando
la configuración del servidor virtual que usará este grupo.

• Descripción - Opcionalmente, escriba una descripción más larga para el grupo de aquí.

• Tipo - Esto en caso de incumplimiento de **Servidor**, Que es lo que necesitamos para esta configuración.

• Comportamiento - Seleccione **Equilibrio de carga** para equilibrar la carga entre todos los servidores en la piscina, o

Conmutación por error utilizar siempre el primer servidor de la piscina a no ser que no, entonces recurrir a posteriores servidores.

• Puerto - Este es el puerto de los servidores están escuchando en el interior. Esto puede ser diferente de la puerto externo, que se define más adelante en la configuración del servidor virtual.

• Monitor - Esto define el tipo de monitor de usar, que es como el equilibrador determina si los servidores están arriba. Selección de **TCP** hará que el equilibrador de conectar con el puerto antes se define en el puerto, y si no puede conectarse a dicho puerto, el servidor se considera abajo. Elección **ICMP** en cambio, supervisar los servidores definidos por el ping, y les marca de por si que no responden a los pings.

• Monitor IP - Este campo no es aplicable con el balanceador de carga del servidor y aparece en gris.

• Dirección IP del servidor - Aquí es donde puede rellenar la dirección IP interna de los servidores en la piscina. Introduzca uno a la vez, haga clic en Agregar a la piscina después.

• Lista - Este campo muestra la lista de servidores que se han sumado a este grupo. Puede eliminar un servidor de la piscina haciendo clic en su dirección IP y haciendo clic en Quitar de la piscina.

Después de rellenar todos los campos que desee, haga clic en Guardar. Continuar con la configuración del servidor virtual para este grupo haciendo clic en la pestaña Servidores Virtuales.

17.1.1.1. Servidores Virtuales

Servidores virtuales es donde se define el IP y el puerto para escuchar en el tráfico de envío hasta los previamente configurado piscina. Haga clic para añadir un nuevo servidor virtual. Cada una de las opciones de esta la página se discute a continuación.

• Nombre - Escriba un nombre para el servidor virtual aquí. Esto es simplemente para su referencia.

• Descripción - Opcionalmente, escriba una descripción más larga para el servidor virtual aquí. Esto también es sólo para fines de referencia.

• Dirección IP - Aquí es donde puede introducir la dirección IP que el servidor virtual escuchar. Este es por lo general su WAN IP o una dirección IP virtual en red WAN. Debe ser una dirección IP estática. Usted puede utilizar una carpa VIP aquí para una configuración de alta disponibilidad equilibrador de carga. Para obtener más información sobre el alta disponibilidad y personalidades CARP, consulte Capítulo 20, Firewall de redundancia / alta disponibilidad.

- Puerto - Este es el puerto del servidor virtual escuchar. Puede ser diferente del puerto servidores están escuchando en el interior.
- Servidor Virtual Pool - Aquí es donde puede seleccionar el grupo configurado previamente. La conexiones a la dirección IP y el puerto se define en esta pantalla será dirigido a las direcciones IP y puerto configurado en la piscina.
- Piscina de Down Server - Este es el servidor que los clientes se dirigen a si todos los servidores de la Piscina están abajo. Debe introducir algo aquí. Si usted no tiene un servidor alternativo para enviar solicitudes, usted puede poner una de las IPs de sus servidores piscina en aquí, aunque el resultado será inaccesibilidad si todos los servidores de la piscina se han reducido.

Después de rellenar los campos correctamente, haga clic en Enviar y luego en Aplicar cambios.

17.1.1.2. Reglas del firewall

El último paso es configurar reglas de firewall para permitir el tráfico a la piscina. Al igual que en un escenario de NAT, las reglas del firewall debe permitir el tráfico a la IP interna privada de los servidores, así como el puerto que se escucha en el interior. Usted debe crear un alias para los servidores en la piscina, y crear un única regla de firewall en la interfaz donde se realizará el tráfico destinado a la piscina iniciado (por lo general WAN) que permite la fuente apropiada (por lo general hay) al destino de los alias creados para la piscina. Un ejemplo concreto de ello es en Sección 17.2.4, "Configuración de las reglas del cortafuegos". Por más información sobre las reglas del cortafuegos, consulte Capítulo 6, Servidor de seguridad.

17.1.2. Pegajosa conexiones

Hay una opción de configuración adicionales para equilibrar la carga del servidor, en el marco del Sistema de → menú Avanzado. Bajo el equilibrio de carga, se encuentra utilizar conexiones pegajosa. Al marcar esta casilla se asegurará de clientes con una conexión activa a la piscina se dirigen siempre en el mismo servidor para las conexiones posteriores. Una vez que el cliente cierra todas las conexiones activas, y los tiempos de estado cerrado, la conexión se pierde pegajosa. Esto puede ser deseable para algunos equilibrio de carga web, configuraciones en las solicitudes de un cliente particular, sólo debe ir a una sola servidor, por razones de sesión o de otro tipo. Tenga en cuenta que esto no es perfecto, como si el navegador del cliente web, se cierra
todas las conexiones TCP en el servidor después de cargar una página y se sienta allí durante 10 minutos o más antes de cargar la siguiente página, la página siguiente se puede servir desde un servidor diferente. En general, esta no es un problema como la mayoría de los navegadores web no se cerrará de inmediato una conexión, y existe el estado lo suficiente como para no hacer un problema, pero si usted es estrictamente dependiente de un cliente específico no conseguir un servidor diferente en la piscina sin importar el tiempo que el navegador no se encuentra inactivo, debe buscar una solución de balanceo de carga diferentes.

17.2. Equilibrio de carga del servidor Web Ejemplo Configuración

En esta sección se muestra cómo configurar el equilibrador de carga de principio a fin para una web dos la carga del servidor medio ambiente equilibrado.

17.2.1. Ejemplo de entorno de red

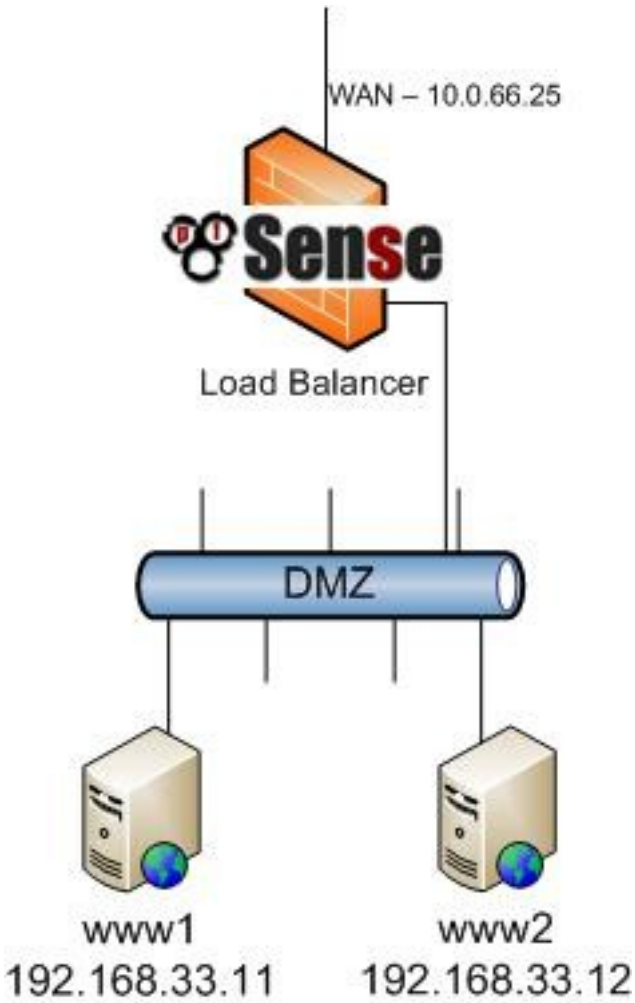


Figura 17.1. Servidor de equilibrio de carga de red de ejemplo

Figura 17.1, "Carga del servidor balanceo de ejemplo" muestra el entorno de ejemplo configurado en esta sección. Consiste en un único servidor de seguridad, utilizando su WAN IP para el grupo, con dos servidores web en un segmento de la DMZ.

17.2.2. Configuración de la piscina

Para configurar el grupo, vaya a Servicios → Equilibrador de carga y haga clic. Figura 17.2, "Pool configuración "muestra la configuración del grupo de balanceo de carga para los dos servidores web, utilizando una TCP monitor. Después de rellenar todos los campos correctamente, haga clic en Guardar.

17.2.3. Configuración del servidor virtual

De vuelta en la pantalla del equilibrador de carga Pool, haga clic en la pestaña Servidores Virtuales y haga clic para añadir una nueva
servidor virtual. Figura 17.3, "Configuración del servidor virtual" muestra la configuración del servidor virtual para escuchar en la IP WAN (10.0.66.25) en el puerto 80 y hacia adelante el tráfico en esa IP y el puerto a la servidores definidos en el **Servidores web** piscina. Para el servidor de Pool de Down, esta configuración utiliza
una de las IPs de los servidores de la **Servidores web** piscina por falta de otra opción. En este
caso, si los dos servidores de la piscina se han reducido, el servidor virtual es inaccesible. Después de rellenar la los campos de aquí, haga clic en Enviar, a continuación, en Aplicar cambios.

17.2.4. Configuración de reglas de firewall

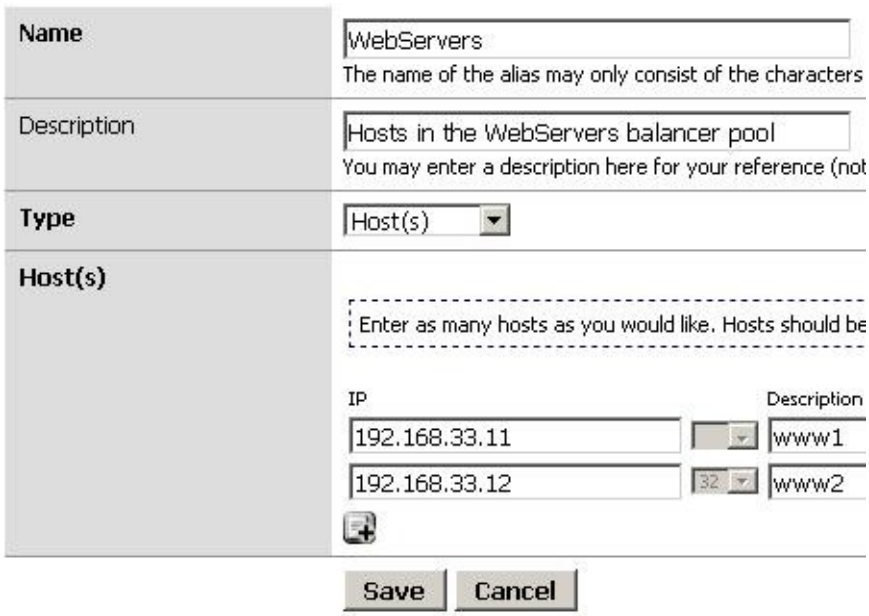


Figura 17.4. Alias de servidores web

Ahora las reglas del cortafuegos debe estar configurado para permitir el acceso a los servidores de la piscina.

Las reglas deben

permitir que el tráfico interno de la dirección IP y el puerto que se utiliza y no hay reglas son necesarias para el exterior de direcciones IP y puertos utilizados en la configuración del servidor virtual. Es preferible utilizar un alias que contiene todos los servidores en la piscina, así que el acceso se puede permitir con una sola regla de firewall. Vaya a Servidor de seguridad → Alias y haga clic para añadir un alias. Figura 17.4, "Alias de servidores web" muestra el alias utilizado para este ejemplo de configuración, que contiene los dos servidores web.

Haga clic en Guardar después de entrar en el alias, y en Aplicar cambios. A continuación vaya al servidor de seguridad → Normas y

en la ficha de la interfaz en la que se inició el tráfico de cliente (WAN, en este caso), haga clic en.

Figura 17.5, "Añadir regla de firewall para servidores web" muestra un fragmento de la regla de firewall agregó para esta configuración. Las opciones no se muestran a la izquierda en su defecto, a un lado de la descripción.

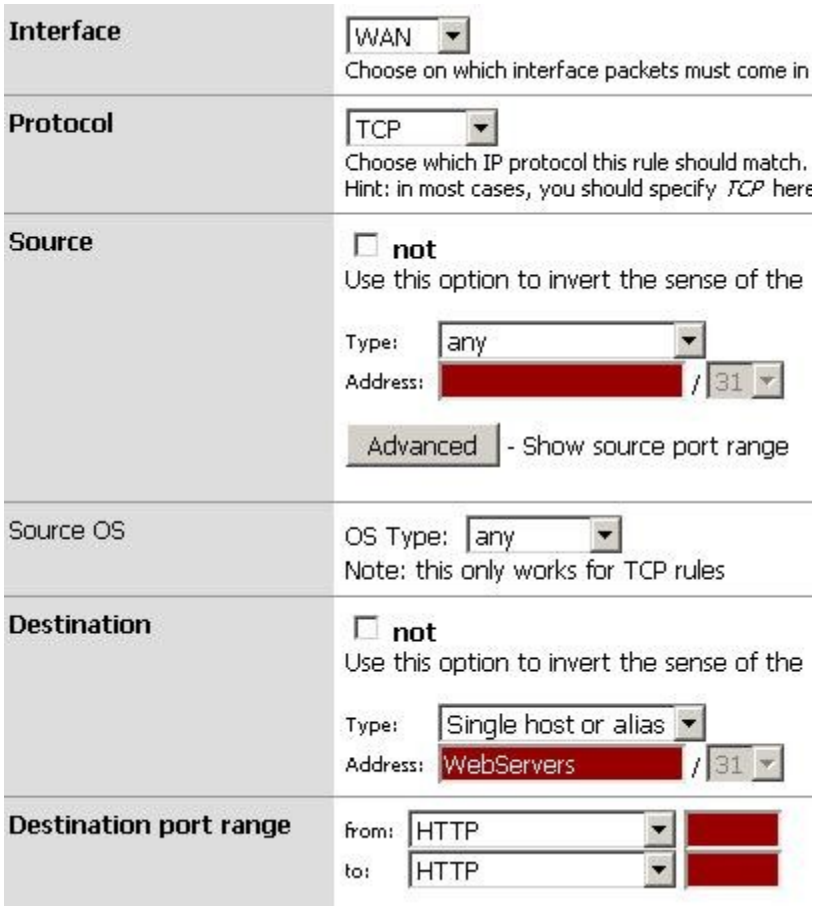


Figura 17.5. Agregar regla de firewall para servidores web,

Figura 17.6, "regla de firewall para servidores web" muestra la regla después de haber sido agregado.

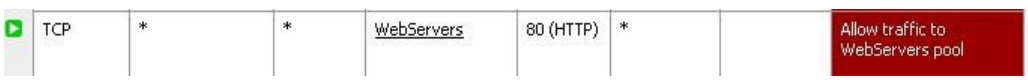


Figura 17.6. Servidor de seguridad de estado de los servidores Web

17.2.5. Ver el estado de equilibrador de carga

Ahora que el equilibrador de carga está configurado, para ver su estado, vaya al Estado → Equilibrador de carga
y haga clic en la pestaña Servidores Virtuales. Aquí podrás ver el estado de cada servidor en la piscina (como se muestra en Figura 17.7, "Estado del servidor virtual"). Si el estado ha cambiado a la línea en los últimos cinco minutos, ya que después de la primera configuración del equilibrador de carga, usted verá "en línea" se destaca en un color amarillento. Después de cinco minutos han pasado, el estado cambiará a verde.

Name	Port	Servers	Status	Description
WebVirtualServer	80	192.168.33.11 192.168.33.12	Online Last change Jul 23 2009 08:21:47 Online Last change Jul 23 2009 08:21:47	Web server pool

Figura 17.7. Virtual Server de estado

Si detiene el servicio de servidor Web en uno de los servidores o tener el servidor de la red totalmente
si se utilizan monitores de ICMP, podrás ver el estado de actualización de conexión y el servidor se eliminará de la piscina.

17.2.6. Verificación de equilibrio de carga

Para verificar el balanceo de carga, enrollamiento es la mejor opción para garantizar el caché de su navegador web y conexiones persistentes no afectan los resultados de sus exámenes. curvatura está disponible para todos los sistemas operativos
imaginables y se puede descargar desde el curl página web [http://curl.haxx.se]. Para usarlo, simplemente ejecutar curl http://***misitio*** sustitución de *misitio* con la dirección IP o nombre de host de su sitio.
Usted debe hacer esto desde fuera de la red. A continuación se ilustra un ejemplo de las pruebas con curvatura de la WAN.

#http:// rizo*10.0.66.25*

```
<html>

<head>
<title> 0.12 </ title>
</ Head>

<body>

<p> 192.168.33.12 - Server 2 </ p>

</ Body>
```

```
</ HTML>
```

Cuando se proceda a probar el equilibrio de carga, tendrá que configurar cada servidor para devolver un Página de especificar su nombre de host, dirección IP, o ambos, para que sepa qué servidor están golpeando. Si usted no tiene conexiones pegajosa habilitado, recibirá un servidor diferente cada vez que solicitud de una página con curl (con la excepción del escenario descrito en Sección 17.3.2, "desigual equilibrio ").

17.3. Solución de problemas de equilibrio de carga del servidor

Esta sección describe los problemas más comunes se encuentran los usuarios con el equilibrio de la carga del servidor, y cómo solucionarlos.

17.3.1. Las conexiones no están equilibradas

Las conexiones no están equilibradas es casi siempre un fracaso de la metodología de prueba se utiliza, y es por lo general específicos de HTTP. navegadores de Internet comúnmente mantener las conexiones a un servidor web abierta, y volver a cargar bateando apenas reutiliza la conexión existente. Una única conexión nunca será cambiar a otro servidor equilibrada. Otro problema común es la caché de su navegador web, en el navegador en realidad nunca pide a la página de nuevo. Es preferible utilizar una línea de comandos herramienta como el enrollamiento de las pruebas de esta naturaleza, porque asegura que nunca se ven afectados por el problemas inherentes a las pruebas con los navegadores web, - que no tiene caché, y abre una nueva conexión a el servidor cada vez que se ejecute. Más información sobre el rizo se puede encontrar en Sección 17.2.6, "Verificación balanceo de carga ".
Si está utilizando conexiones pegajosa, asegúrese de que está probando de IP de origen múltiple. Pruebas de una sola fuente IP siempre irá a un solo servidor a menos que los tiempos de espera largos en el medio conexiones.

17.3.2. Desigual equilibrio

Debido a la forma en que funciona el software subyacente, en entornos con poca carga, el equilibrio será desigual. El servicio de vigilancia subyacentes slbd restablece su pf ancla en cada monitor intervalo, que es cada 5 segundos. Esto significa que cada 5 segundos, la próxima conexión irá a la primer servidor en la piscina. Con los servicios de carga muy baja, donde con frecuencia tienen una conexión o menos cada 5 segundos, podrás ver el equilibrio de carga muy poco. Aún dispone de conmutación por error completo capacidades que uno de los servidores no. Este problema realmente se resuelve sin embargo, cuando su aumenta la carga hasta el punto de equilibrio de la carga es importante, será equilibrado por igual. En entornos de producción de manejar miles de paquetes por segundo, el equilibrio es igual a través de los servidores.

17.3.3. Abajo servidor no marcados como fuera de línea

Si un servidor se cae, pero no se marcan como sin conexión, es porque desde la perspectiva de la monitoreo que pfSense está haciendo, en realidad no es hacia abajo. Si se usa un monitor de TCP, que el puerto TCP está aceptando conexiones. El servicio en ese puerto se podía romper de muchas maneras y aún responder a las conexiones TCP. Para los monitores de ICMP, este problema se agrava, ya que los servidores se puede colgado sin servicios de música en todo y todavía respuesta a los pings.

17.3.4. servidor de Live no se marca como línea

Si un servidor está en línea, pero no se marca como en línea, es porque no está en línea desde la perspectiva del servidor de seguridad. El servidor debe responder en el puerto TCP utilizado o no responde a los pings proceden de el período de investigación de la interfaz de firewall más cercana a la del servidor. Por ejemplo, si el servidor está en la LAN, el servidor debe responder a las peticiones iniciadas desde IP LAN del firewall. Para verificar esta ICMP para monitores, vaya a Diagnósticos → Ping y ping a la IP del servidor mediante la interfaz donde se encuentra el servidor. Para los monitores de TCP, inicie sesión en el servidor de seguridad usando SSH, o en la consola,
y elija la opción de menú de la consola **8**. En el símbolo del sistema, intente telnet al puerto del servidor debe estar escuchando en. Por ejemplo, para probar un servidor web en el ejemplo anterior en este capítulo, tendría que ejecutar **telnet 192.168.33.11 80**.
Una conexión no se sentará allí por un tiempo tratando de conectar, mientras que una conexión exitosa se conectará de inmediato. El siguiente es un ejemplo de un error de conexión.

#telnet 192.168.33.12 80
```
Tratando de 192.168.33.12 ...
telnet: conectarse a la dirección 192.168.33.12: La operación ha agotado
el tiempo
telnet: No se puede conectar a un host remoto
```

Y aquí es un ejemplo de una conexión exitosa.

#telnet 192.168.33.12 80
```
Tratando de 192.168.33.12 ...
Conectado a 192.168.33.12.
Carácter de escape es'^]'.
```

Usted encontrará probablemente que falla la conexión, y tendrá que solucionar aún más en el servidor.

Capítulo 18. Wi-fi

pfSense incluye construido en capacidades inalámbricas que permiten a su vez su instalación en pfSense un punto de acceso inalámbrico, utilice una conexión inalámbrica 802.11 como una conexión WAN, o ambos. Este capítulo incluye también los medios sugerido de forma segura con capacidad de acceso inalámbrico externo puntos, y cómo implementar de forma segura un punto de acceso inalámbrico. la cobertura en profundidad de 802.11 se encuentra fuera de el alcance de este libro. Para aquellos que buscan información tales, recomiendo el libro 802.11 Redes inalámbricas: The Definitive Guide [http://www.amazon.com/gp/product/0596100523? es decir, = UTF8 & tag = pfSense-20 y linkCode = AS2 y campo = 1789 = 9325 y creativa y creativeASIN = 0596100523].

18.1. Recomendaciones de hardware inalámbrico

Hay una variedad de tarjetas inalámbricas compatibles con FreeBSD 7.2, y pfSense incluye soporte por cada tarjeta con el apoyo de FreeBSD. Algunos se apoyan mejor que otros. La mayoría de pfSense los desarrolladores trabajar con hardware Atheros, por lo que tiende a ser el hardware más recomendado. Muchos tienen éxito con otras tarjetas también, y Ralink es otra opción popular. Otras tarjetas puede ser apoyado, pero no admiten todas las funciones disponibles. En particular, algunas tarjetas de Intel puede se utiliza en el modo infraestructura, pero no se puede ejecutar en modo punto de acceso debido a las limitaciones de la de hardware en sí.

18.1.1. Tarjetas inalámbricas de los proveedores de renombre

Linksys, D-Link, Netgear y otros fabricantes importantes comúnmente cambiar los chipsets utilizados en sus tarjetas inalámbricas sin necesidad de cambiar el número de modelo. No hay manera de garantizar un determinado modelo de tarjeta de estos vendedores serán compatibles porque no tienes forma de saber que "Menores" revisión tarjeta que va a terminar con. Mientras que una revisión de un modelo en particular puede ser compatibles y funcionar bien, otra tarjeta del mismo modelo puede ser incompatible. Por esta razón, se recomienda evitar las cartas de los principales fabricantes. Si ya tienes una, vale la pena tratando de ver si es compatible, pero debe saber que si usted compra uno porque el "mismo" modelo trabajado para otra persona, usted puede terminar con una pieza completamente diferentes de hardware que es incompatible.

18.1.2. controladores inalámbricos incluidos en 1.2.3

~~En esta sección se enumeran los controladores inalámbricos incluidos en pfSense 1.2.3, y los ch~~ipsets que son con el apoyo de los conductores (tirando de las páginas del manual de FreeBSD para los controladores). Los conductores en FreeBSD se mencionan por su nombre de controlador, seguido por (4), como `ath (4)`. El (4) se refiere

a las interfaces del kernel, en este caso la especificación de un controlador de red. Los controladores se enumeran en orden

de la frecuencia de uso con pfSense, con base en la lista de correo y mensajes en los foros ya que el proyecto de
creación.

Para obtener más información detallada sobre tarjetas de apoyo, y la más actualizada información, consulte el wiki pfSense [http://doc.pfsense.org/index.php/Supported_Wireless_Cards].

18.1.2.1. ath (4)

Soporta tarjetas basadas en el Atheros AR5210, AR5211 y AR5212 chipsets.

18.1.2.2. ral (4)

Ralink Technology IEEE 802.11 controlador de red inalámbrica - soporta tarjetas basadas en el Ralink Tecnología RT2500, RT2501 RT2600 y chipsets.

18.1.2.3. wi (4)

Lucent Hermes, Intersil PRISM y IEEE 802.11 Spectrum24 conductor - soporta tarjetas basadas en Hermes Lucent, Intersil PRISM-II, Intersil PRISM-2.5, símbolo Intersil Prism-3, y Spectrum24 chipsets. Estas tarjetas sólo soportan 802.11b.

18.1.2.4. awi (4)

AMD PCnetMobile IEEE 802.11 PCMCIA controlador de red inalámbrica - soporta tarjetas basadas en el procesador AMD 79c930 controlador con Intersil (antes Harris) chipset PRISM de radio.

18.1.2.5. uno (4)

Comunicaciones Aironet 4500/4800 controlador inalámbrico adaptador de red - compatible con Aironet Comunicaciones 4500 y 4800 los adaptadores de red inalámbrica y variantes.

18.2. WAN inalámbrica

Usted puede asignar la tarjeta inalámbrica como su interfaz WAN o una WAN OPT en un multi-WAN implementación. Esta sección trata de asignar y configurar una interfaz inalámbrica como WAN interfaz.

18.2.1. Interface de

Si aún no lo ha asignado a su interfaz inalámbrica, ver a las interfaces → Asignar. Haga clic en Agregar para agregar una interfaz OPT para su red inalámbrica, o seleccionarlo como WAN, si se desea. Figura 18.1, "Interfaz de asignación - WAN inalámbrica" muestra una tarjeta Atheros asignado como WAN.

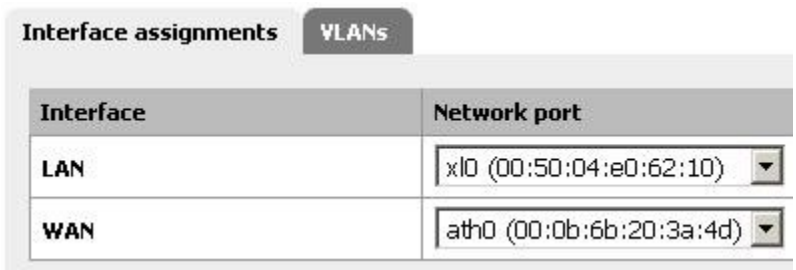


Figura 18.1. asignación de interfaz - WAN inalámbrica

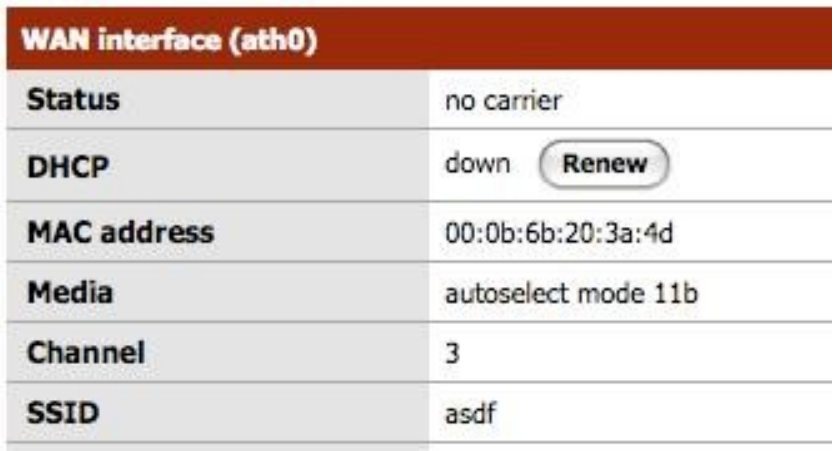
18.2.2. Configuración de su red inalámbrica

Busque el menú de interfaces para la interfaz WAN inalámbrica. En este ejemplo se utiliza WAN, por lo que se vaya a interfaces → WAN. Seleccione el tipo de configuración (DHCP, IP estática, etc), y desplácese hacia abajo en la configuración inalámbrica. Elija Infraestructura (SRS), el modo rellenar el SSID, y configurar encriptación como WEP (Wired Equivalent Privacy) o WPA (Wi-Fi Protected Access) si se utiliza. La mayoría de las redes inalámbricas no se necesita ninguna configuración adicional, pero si la suya lo hace, asegúrese de que está configurado apropiado para el punto de acceso que va a utilizar. A continuación, haga clic en Guardar.

18.2.3. Comprobar el estado inalámbrico

Vaya a Estado → Interfaces para ver el estado de la interfaz inalámbrica acaba de configurar. Usted puede decir si la interfaz se ha asociado con éxito al punto de acceso elegido por mirar en el estado de la interfaz. Estado asociado significa que está conectado con éxito, como se muestra en Figura 18.2, "WAN inalámbrica asociados".

Si aparece No hay compañía, no estaba en condiciones de asociarse. Figura 18.3, "Ninguna compañía aérea de WAN inalámbrica" muestra un ejemplo de esto, en la que configura el SSID **asdf**, Una red inalámbrica que no existe.



WAN interface (ath0)	
Status	no carrier
DHCP	down Renew
MAC address	00:0b:6b:20:3a:4d
Media	autoselect mode 11b
Channel	3
SSID	asdf

Figura 18.3. Ninguna compañía de WAN inalámbrica

18.2.4. Se muestran las redes inalámbricas disponibles y de la señal fuerza

Al navegar a Estado → Wireless, puedes ver las redes inalámbricas visible para el servidor de seguridad como se muestra en Figura 18.4, "estado de Wireless". Su interfaz inalámbrica se debe configurar antes de este elemento de menú aparecerá.

Status (wan)

SSID	BSSID	CHAN	RATE	RSSI	INT	CAPS
fw2	00:80:48:52:47:eb	1	54M	-84:-95	100	EPS
linksys	00:13:10:62:52:03	6	54M	-79:-94	100	E
cmb	00:02:6f:51:38:ee	3	54M	-66:-95	100	EPS

Figura 18.4. De estado inalámbrico

18.3. Superar e inalámbricas

Sólo las interfaces inalámbricas en el punto de acceso (hostap) el modo funcionará en una configuración de puente. Usted puede salvar una interfaz inalámbrica en hostap a cualquier otra interfaz de combinar las dos interfaces

en el mismo dominio de broadcast. Es posible que desee hacer esto si tiene dispositivos o aplicaciones que debe residir en el mismo dominio de broadcast para funcionar correctamente. Esto se discute con mayor profundidad en Sección 18.4.3.1, "Selección de puente o encaminamiento".

18.3.1. SRS y IBSS inalámbricos y puentes

Debido a las obras de forma inalámbrica en BSS (Basic Service Set) y IBSS (Independent básica Conjunto de servicios), el modo y la forma en puente funciona, no puede cerrar una interfaz inalámbrica en BSS o el modo IBSS. Cada dispositivo conectado a una tarjeta wireless en modo BSS o IBSS debe presentar la misma dirección MAC. Con el puente, la dirección MAC pasado es el actual MAC de la dispositivo conectado. Esto es normalmente deseable - es sólo cómo salvar las obras. Con la tecnología inalámbrica, la única manera que esto puede funcionar si está detrás de todos los dispositivos que la tarjeta inalámbrica presentar la misma Dirección MAC de la red inalámbrica. Esto se explica en profundidad por el conocido experto inalámbrica Jim Thompson en un puesto de la lista de correo [http://lists.freebsd.org/pipermail/freebsd-current/2005-October/056977.html].[1] Como un ejemplo, cuando VMware Player, Workstation o Server configurado para salvar a una interfaz inalámbrica, que traduce automáticamente la dirección MAC para que de la tarjeta inalámbrica. Porque no hay manera de traducir simplemente una dirección MAC en FreeBSD, y por la forma en puente en las obras de FreeBSD, es difícil ofrecer soluciones provisionales similar a lo que ofrece VMware. En algún punto de pfSense puede contribuir a ello, pero no está en la hoja de ruta para la 2.0.

18.4. El uso de un punto de acceso externo

Si usted tiene un punto de acceso inalámbrico existente, o un router inalámbrico que desea utilizar sólo como un punto de acceso ya que pfSense está actuando como el servidor de seguridad, hay varias maneras de dar cabida a inalámbrica en su red. Esta sección cubre los escenarios más comúnmente implementados.

18.4.1. En cuanto a su router inalámbrico en un punto de acceso

Al reemplazar un enrutador inalámbrico simples tales como Linksys o D-Link o dispositivo doméstico otro grado con pfSense como un servidor de seguridad perimetral, la funcionalidad inalámbrica puede mantenerse girando el router inalámbrico en un punto de acceso inalámbrico, siga los pasos descritos en esta sección. Estos son medidas genéricas que deben seguirse para cualquier dispositivo. Para encontrar información específica para su red inalámbrica enrutador, consulte la documentación.

---

[1] http://lists.freebsd.org/pipermail/freebsd-current/2005-October/0 56977.html

18.4.1.1. Desactivar el servidor DHCP

Primero tendrá que desactivar el servidor DHCP si estaba previamente en uso. Usted querrá pfSense para manejar esta función para su red, y tener dos servidores DHCP en la red causar problemas.

18.4.1.2. Cambiar la IP LAN

A continuación, tendrá que cambiar la IP de la LAN a una dirección IP no utilizada en la subred donde su punto de acceso residirá (comúnmente LAN). Es probable que con la misma IP que se asignan a la pfSense Conexión de la interfaz, por lo que requerirá una dirección diferente. Usted querrá mantener una IP funcional el punto de acceso con fines de gestión.

18.4.1.3. Conecte la interfaz LAN

La mayoría de los routers inalámbricos del puente inalámbrico en el puerto o los puertos LAN interna. Esto significa que el inalámbrico estará en el mismo dominio de broadcast y de subred IP que los puertos con cables. Para routers con un conmutador integrado, cualquiera de los puertos de conmutación por lo general va a funcionar. Usted no quiere conectar el WAN o Internet puerto en el router! Esto pondrá su red inalámbrica en una transmisión en diferentes de dominio del resto de la red, y dará lugar a NATing tráfico entre su red inalámbrica y LAN y el tráfico de doble alternando entre su red inalámbrica e Internet. Este es un feo diseño, y dará lugar a problemas en algunas circunstancias, especialmente si usted necesita para comunicarse entre los clientes inalámbricos y la LAN cableada.
Cuando se conecta la interfaz LAN dependerá de su diseño de la red elegida. La próxima secciones cubren sus opciones y sus consideraciones en los que elegir.

18.4.2. Puente inalámbrico para su LAN

Una forma común de implementar wi-fi para conectar el punto de acceso directamente a la misma interruptor como sus anfitriones LAN, donde los puentes AP los clientes inalámbricos a la red cableada. Esto funciona bien, pero ofrece un control limitado sobre la capacidad de los clientes inalámbricos para comunicarse con sus sistemas internos.

18.4.3. Puente inalámbrico a una interfaz OPT

Si desea más control sobre sus clientes inalámbricos, añadiendo una interfaz OPT para pfSense para el punto de acceso es la solución preferida. Si desea mantener sus redes inalámbricas y por cable en la misma subred IP y dominio de difusión, puede cerrar la interfaz de OPT a la LAN

interfaz. Este escenario es funcionalmente equivalente a conectar el punto de acceso directamente en su Interruptor de LAN, excepto desde pfSense está en el centro, se puede filtrar el tráfico de su red inalámbrica para proporcionar protección a los hosts de la LAN.

Usted también puede poner su red inalámbrica en una subred IP dedicada, si lo desea, al no superar la interfaz opcional en pfSense y asignar con una subred IP fuera de la subred LAN.
Esto permite el enrutamiento entre sus redes internas e inalámbricas, según lo permitido por el servidor de seguridad conjunto de reglas. Esto se hace comúnmente en las redes más grandes, en varios puntos de acceso están conectados en un interruptor que está conectado a la interfaz opcional en pfSense. También es preferible cuando que obligará a los clientes inalámbricos para conectarse a una VPN antes de permitir las conexiones a la residencia recursos de la red.

18.4.3.1. Elección de puente o encaminamiento

La elección entre el puente (utilizando la misma subred IP que la red LAN) o ruta (usando una dedicada subred IP para la conexión inalámbrica) para los clientes inalámbricos que dependen de los servicios lo los clientes inalámbricos requieren. Algunas aplicaciones y dispositivos se basan en emisiones de funcionar. AirTunes de Apple, como un ejemplo, no funcionará a través de dos dominios de broadcast, por lo que si han AirTunes en la red inalámbrica y desea utilizar en un sistema en el cable de red, debe puente de la redes cableadas e inalámbricas. Otro ejemplo son los servidores de medios utilizado por los dispositivos como Xbox 360 y Playstation 3. Estos se basan en multidifusión o difusión tráfico que sólo puede funcionar si sus redes alámbricas e inalámbricas en puente. En la casa de muchos entornos de red que tendrá aplicaciones o dispositivos que requieren su cable e inalámbricas redes para salvarse. En la mayoría de las redes corporativas, no hay aplicaciones que requieren puente. ¿Cuál elegir depende de los requisitos de las aplicaciones de red que utilice, así como su preferencia personal.
Hay algunos compromisos de la presente, un ejemplo es el paquete de Avahi. Se puede escuchar en dos diferentes dominios de difusión y retransmisión de mensajes de unos a otros con el fin de permiten DNS de multidifusión al trabajo (también conocido como Rendezvous o Bonjour) para la detección de redes y servicios.
Tener un WINS (Windows Internet Name Service) es otro ejemplo, ya que permitirá a navegar por redes de máquinas Windows / SMB habilitado incluso cuando no están en el mismo transmisión de dominio.

18.5. pfSense como punto de acceso

Con una tarjeta inalámbrica que soporta el modo hostap (`ath (4)`,`ral (4)` y `wi (4)`), PfSense puede se configura como un punto de acceso inalámbrico.

18.5.1. ¿Debo usar un AP o externa pfSense como mi acceso punto?

Históricamente, la funcionalidad de punto de acceso en FreeBSD ha sufrido de graves de compatibilidad problemas con algunos clientes inalámbricos. Con FreeBSD 7.x esto ha mejorado significativamente, sin embargo todavía puede haber algunos dispositivos incompatibles. Estas dificultades con la compatibilidad del cliente se no siempre se limita a FreeBSD, pero es posible que un grado de consumo baratos router inalámbrico punto de acceso se volvió proporciona una mayor compatibilidad de las capacidades de FreeBSD punto de acceso algunos casos. Puedo utilizar los puntos de pfSense acceso en casa sin ningún problema, con mi MacBook Pro, AirTunes Apple, Mac mini G4, iPod Touch, Palm Treo, varios ordenadores portátiles de Windows, Xbox 360, y FreeBSD clientes y funciona muy fiable en todos estos dispositivos. Existe la posibilidad de de encontrar dispositivos incompatibles con cualquier punto de acceso. FreeBSD no es una excepción y puede encontrar esto es más común en FreeBSD que otros puntos de acceso. En versiones anteriores de FreeBSD, en particular con m0n0wall en FreeBSD 4.x, no se recomienda el uso de punto de acceso de FreeBSD funcionalidad. Hoy en día funciona bien con casi todos los dispositivos y es probablemente adecuado para su red.

Esto está sujeto a cambios significativos con cada nueva versión de FreeBSD. Una al día lista de conocidos dispositivos incompatibles y la información más reciente sobre compatibilidad inalámbrica se puede encontrar en http://www.pfsense.org/apcompat.

18.5.2. pfSense Configuración como punto de acceso

El proceso de configuración de pfSense para actuar como un punto de acceso inalámbrico (AP) es relativamente fácil. Muchos de las opciones deben estar familiarizados si ha configurado otros routers inalámbricos antes, y algunos opciones pueden ser nuevos, a menos que haya usado un poco de equipo inalámbrico de calidad comercial. No hay docenas de maneras de configurar los puntos de acceso, y todos ellos dependen de su entorno. En este caso, cubrimos ajuste pfSense como una base a la AP que utiliza el cifrado WPA2 con AES. En este ejemplo, ExampleCo necesidades de acceso inalámbrico para algunos ordenadores portátiles en la sala de conferencias.

18.5.2.1. Preparación de la interfaz inalámbrica

Antes de hacer cualquier otra cosa, asegúrese de que la tarjeta inalámbrica en el router, y es la antena firmemente sujeta. Como se ha descrito anteriormente en este capítulo, la tarjeta inalámbrica debe ser asignado como interfaz de OPT y habilitado antes de la configuración restante se puede completar.

18.5.2.2. Interfaz de Descripción

Cuando está en uso como un punto de acceso, nombres de "WLAN" (Wireless LAN) o "Wireless" hará que sea fácil de identificar en la lista de interfaces. Si usted tiene un SSID único, puede encontrar más

cómodo de usar que en la descripción del lugar. PfSense Si va a manejar múltiples puntos de acceso, debe haber alguna manera de distinguir, como "WLANadmin" y "WLANsales". Vamos a llaman a esto una **ConfRoom** por ahora.

18.5.2.3. Tipo de interfaz / IP

Dado que este será un punto de acceso en una subred IP dedicada, usted tendrá que configurar el tipo de **Estática** y especificar una dirección IP y la máscara de subred. Como se trata de una subred independiente de la otras interfaces, puede ser **192.168.201.0/24**, Una subred que en otro caso no utilizados en el ExampleCo red.

18.5.2.4. Estándar inalámbrico

Dependiendo de la compatibilidad de hardware, hay varias opciones disponibles para el estándar inalámbrico configuración, incluyendo 802.11b, 802.11g, 802.11g turbo, 802.11a, y turbo 802.11a, y posiblemente otros. Para este ejemplo, vamos a elegir **802.11g**.

18.5.2.5. Modo inalámbrico

Establezca el campo Modo de **Punto de Acceso**Y pfSense utilizará hostapd para actuar como un punto de acceso.

18.5.2.6. Service Set Identifier (SSID)

Este será el "nombre" de la AP como se ve por los clientes. Es necesario configurar el SSID a algo fácilmente identificable, sin embargo, única para su configuración. Siguiendo con el ejemplo, esto puede ser llamado **ConfRoom**.

18.5.2.7. Limitar el acceso a 802.11g sólo

El 802.11g sólo controla si o no los clientes más antiguos 802.11b son capaces de asociarse con este punto de acceso. Permitir a los clientes más antiguos pueden ser necesarias en algunos ambientes si los dispositivos son siendo alrededor que lo requieran. Algunos dispositivos móviles como el Nintendo DS y la Palm Tungsten C sólo son compatibles con 802.11b y requieren una red mixta para trabajar. La otra cara de esto es que podrás ver velocidades más lentas, como resultado de permitir que dichos dispositivos en la red, como punto de acceso se verá obligado a atender el mínimo común denominador cuando un 802.11b dispositivo está presente. En nuestra sala de conferencias ejemplo, la gente sólo va a utilizar recientemente comprado portátiles propiedad de la compañía que son capaces de 802.11g, lo que se marca esta opción.

18.5.2.8. Comunicación Intra-BSS

Si marca Permitir la comunicación intra-SEV, los clientes inalámbricos se podrán ver entre sí directamente, en lugar de encaminar todo el tráfico a través de la AP. Si los clientes sólo necesitan tener acceso a la

Internet, a menudo es más seguro para desactivar esto. En nuestro escenario, la gente en la sala de conferencias puede
necesidad de compartir archivos de ida y vuelta directamente entre ordenadores portátiles, por lo que este se quedará activada.

18.5.2.9. Ocultar SSID (SSID de radiodifusión Desactivar)

Normalmente, el AP emitirá su SSID para que los clientes pueden localizar y asociar a él fácilmente.
Esto es considerado por algunos como un riesgo de seguridad, anunciando a todos los que están escuchando que tiene una red inalámbrica disponible, pero en la mayoría de los casos la comodidad es mayor que el de seguridad de riesgo. Los beneficios de deshabilitar el SSID de radiodifusión son exagerados por algunos, ya que en realidad no ocultar la red de cualquier persona capaz de usar muchas herramientas inalámbricas disponibles gratuitamente de seguridad que
fácil encontrar este tipo de redes inalámbricas. Para nuestra sala de conferencias de AP, vamos a dejar esta casilla sin marcar
para que sea más fácil para los asistentes a la reunión para encontrar y utilizar el servicio.

18.5.2.10. Selección de canales inalámbricos

Al seleccionar un canal, tendrá que ser conscientes de que ninguna de transmisores de radio cerca, en similares bandas de frecuencia. Además de los puntos de acceso inalámbrico, también hay teléfonos inalámbricos, Bluetooth, monitores de bebés, los transmisores de vídeo, microondas, y muchos otros dispositivos que utilizan el mismo 2.4 GHz que pueden causar interferencias. A menudo usted puede conseguir lejos con el uso de cualquier canal que como, siempre y cuando sus clientes de AP están cerca de la antena. La forma más segura de utilizar los canales son de 1, 6 y 11
ya que sus bandas de frecuencias no se solapen entre sí. Usted puede especificar **Auto** decirle a la tarjeta a elegir un canal adecuado, sin embargo, esta funcionalidad no funciona con algunas tarjetas de red inalámbricas.
Si usted elige **Auto** y las cosas no funcionan, elija un canal específico en su lugar. Para esta red,
ya que no hay otros a su alrededor, vamos a seleccionar el canal **1**.

18.5.2.11. De cifrado inalámbrico

Tres tipos de cifrado son compatibles con redes 802.11: WEP, WPA y WPA2. WPA2
con AES es el más seguro. Incluso si usted no está preocupado acerca del cifrado de los más de-the-air tráfico (que debería ser), que proporciona un medio adicional de control de acceso. Un WPA/WPA2
frase de paso también es más fácil trabajar con el entonces una clave WEP en la mayoría de los dispositivos, sino que actúa más como una contraseña de una cadena muy larga de caracteres hexadecimales. Al igual que con la elección entre 802.11by 802.11g, algunos dispositivos más antiguos sólo soportan WEP o WPA, pero más modernos inalámbrica tarjetas y los controladores de apoyo WPA2.
Para nuestra sala de conferencias, que utilizarán WPA2 y WEP a su vez fuera. Para ello, desactive Habilitar, WEP y WPA de verificación Habilitar. Para asegurarse de que WPA2 sólo estará en uso, sistema WPA de modo a **WPA2**. Por nuestra clave WPA Pre-Shared, usaremos **excoconf213**, Y también establecer el modo de clave WPA
Gestión de **Pre-Shared Key**.

Para utilizar WPA2 + AES, según lo deseado para la red inalámbrica sala de conferencias, sistema WPA pares

de **AES**.

Nota

Para utilizar WPA2 en un cliente inalámbrico de Windows XP, debe tener un controlador inalámbrico
que soporta WPA2. Si usted está usando wi-fi de configuración de Windows XP interfaz, con el fin de asociar a una WPA2 punto de acceso en ejecución, tendrá que actualizar el PC a Windows XP SP3 o instalar el parche de Microsoft Knowledge Base el artículo 917021 [http://support.microsoft.com/kb/917021].

18.5.2.11.1. Debilidades de cifrado inalámbrico

WEP ha tenido graves problemas de seguridad conocidos desde hace años, y nunca debe utilizarse a menos es la única opción para los dispositivos inalámbricos que debe soportar. Es posible romper el protocolo WEP en cuestión de minutos a lo sumo, y nunca se debe confiar en la seguridad. WEP no se puede confiar en para algo más que mantener alejados a los solicitantes de Internet sin conocimientos técnicos.

TKIP (Temporal Key Integrity Protocol), que forma parte de AES, se convirtió en un sustituto de WEP después de que se había roto. Se utiliza el mismo mecanismo subyacente como WEP, y por lo tanto es vulnerable a algunos ataques similares. Recientemente, estos ataques son cada vez más práctico. En el momento de escribir este artículo no es tan fácil de romper como WEP, pero nunca se debe todavía lo utilizan menos que haya dispositivos que no son compatibles con WPA o WPA2 AES usando. WPA y WPA2 en combinación con AES no están sujetos a estas fallas en TKIP.

18.5.2.12. Acabado Configuración AP

La configuración anterior debería ser suficiente para conseguir un punto de acceso inalámbrico 802.11g con correr con WPA2 + AES. Hay otras opciones que se pueden utilizar para ajustar el comportamiento de la AP, pero no son necesarias para un funcionamiento normal en la mayoría de entornos. Cuando haya terminado cambiar la configuración, haga clic en Guardar, luego en Aplicar cambios.

18.5.2.13. Configuración de DHCP

Ahora que hemos creado una red totalmente independiente, que se desea habilitar DHCP para que la asociación de los clientes inalámbricos de forma automática la posibilidad de obtener una dirección IP. Vaya a Servicios → DHCP
Server, haga clic en la ficha de la interfaz inalámbrica (ConfRoom para nuestro ejemplo de configuración). Compruebe la casilla para activar, configurar cualquier tamaño de rango que se necesita, y las opciones adicionales necesarios, a continuación, haga clic en Guardar cambios y aplicar. Para obtener más detalles sobre la configuración del servicio DHCP, consulte
Sección 21.1, "Servidor DHCP".

18.5.2.14. Adición de reglas de firewall

Desde esta interfaz inalámbrica es una interfaz territorio palestino ocupado, no tendrá las reglas del cortafuegos por defecto. En el mismo
por lo menos tendrá que tener una regla para permitir el tráfico de esta subred a cualquier destino será

sea necesario. Desde nuestros usuarios sala de conferencias tendrá acceso a Internet y acceso a otra red recursos, una regla de permiso por defecto va a estar bien en este caso. Para crear la regla, vaya al servidor de seguridad → Reglas,
y haga clic en la ficha de la interfaz inalámbrica (ConfRoom para este ejemplo). Agregar una regla para pasar el tráfico de cualquier protocolo, con una dirección de origen de la subred ConfRoom, y cualquier destino. Por más información sobre cómo crear reglas de firewall, consulte Capítulo 6, Servidor de seguridad.

18.5.2.15. La asociación de los clientes

La nueva configuración AP pfSense debe aparecer en la lista de puntos de acceso disponibles en su dispositivo móvil, suponiendo que no la radiodifusión de deshabilitar el SSID. Usted debe ser capaz a los clientes asocian con él como lo haría con cualquier otro punto de acceso. El procedimiento exacto puede variar entre los sistemas operativos, dispositivos y controladores, pero la mayoría de los fabricantes han racionalizado el proceso para que sea simple para todos.

18.5.2.16. Visualización del estado de cliente inalámbrico

Cuando usted tiene una interfaz inalámbrica configurada para el modo de punto de acceso, los clientes asociados a aparecerá sobre la situación → Wireless.

18.6. protección adicional para su red inalámbrica red

Además de una fuerte encriptación de WPA o WPA2 con AES, algunos usuarios como para emplear un capa adicional de cifrado y autenticación para permitir el acceso a recursos de red.
Las dos soluciones más comúnmente utilizados son Portal Cautivo y VPN. Estos métodos se pueden empleados si se utiliza un punto de acceso exterior en una interfaz OPT o inalámbrica interna tarjeta como punto de acceso.

18.6.1. protección adicional inalámbrica con Portal Cautivo

Al permitir Portal Cautivo en la interfaz donde reside su red inalámbrica, puede solicitar autenticación para que los usuarios pueden tener acceso a recursos de red. En las redes corporativas, esto es utilizados comúnmente con la autenticación RADIUS de Microsoft Active Directory para que los usuarios pueden utilizar sus credenciales de Active Directory para autenticar al mismo tiempo en la red inalámbrica. Cautivas configuración del Portal se trata en Capítulo 19, Portal Cautivo.

18.6.2. protección adicional con VPN

Adición de Portal Cautivo proporciona otro nivel de autenticación, pero no ofrece ninguna adicionales protección contra escuchas de su tráfico inalámbrico. Exigir VPN para permitir el acceso a la red interna e Internet añade otro nivel de autenticación, así como un adicional capa de cifrado para el tráfico inalámbrico. La configuración para el tipo elegido de VPN no será diferente a partir de una configuración de acceso remoto, pero tendrá que configurar el firewall normas relativas a la interfaz de pfSense para permitir sólo el tráfico VPN de los clientes inalámbricos.

18.6.2.1. Configuración de reglas de firewall para IPsec

Figura 18.5, "Reglas para permitir sólo IPsec desde inalámbrica" muestra las reglas mínimas necesarias para permitir sólo el acceso a IPsec en la interfaz WLAN IP. Hace ping a la interfaz WLAN IP también se puedan colaborar en la solución de problemas.

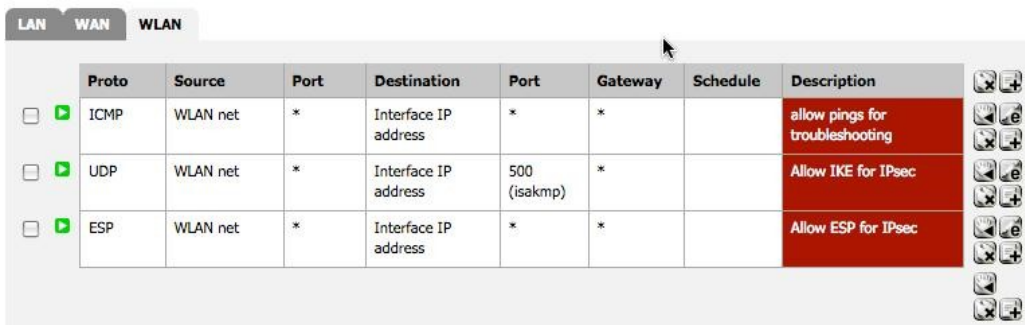


Figura 18.5. Normas para permitir que sólo IPsec desde inalámbrica

18.6.2.2. Configuración de reglas de firewall para OpenVPN

Figura 18.6, "Reglas para permitir sólo OpenVPN desde inalámbrica" muestra las reglas mínimas necesarias para permitir el acceso sólo a OpenVPN en la interfaz WLAN IP. Hace ping a la interfaz WLAN IP también pueden contribuir a la solución de problemas. Esto supone que está utilizando el puerto UDP predeterminado 1194. Si elige otro protocolo o el puerto, modifica la norma correspondiente.

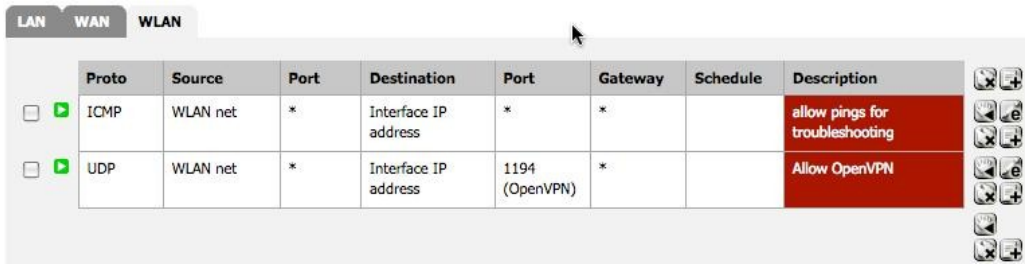


Figura 18.6. Normas para permitir que sólo OpenVPN desde inalámbrica

18.6.2.3. Configuración de reglas de firewall para PPTP

Figura 18.7, "Reglas para permitir sólo PPTP desde inalámbrica" muestra las reglas mínimas necesarias para permitir el acceso sólo a PPTP en la interfaz WLAN IP. Hace ping a la interfaz WLAN IP también se puedan colaborar en la solución de problemas.

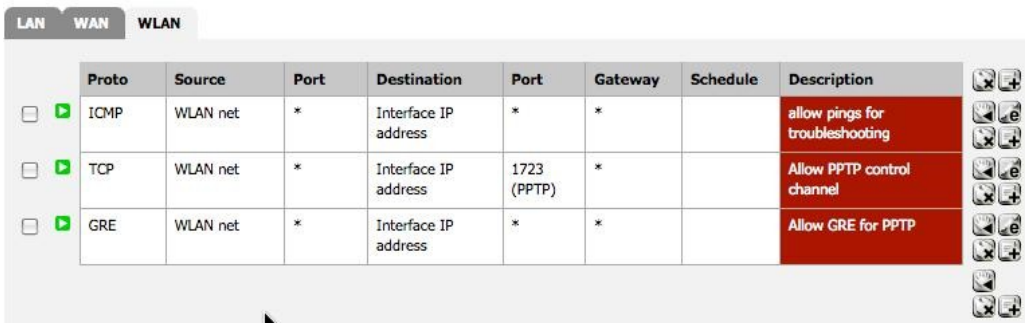


Figura 18.7. Normas para permitir que sólo PPTP desde inalámbrica

18.7. Configuración de un punto de acceso inalámbrico seguro

Su empresa u organización que desee proporcionar acceso a Internet para los clientes o huéspedes usando su conexión a Internet existente. Esto puede ser una bendición para sus clientes y negocios, pero también puede exponer a su red privada para atacar si no se realiza correctamente. Esta sección cubre el medio común de proporcionar acceso a Internet para los huéspedes y clientes, protegiendo al mismo tiempo su red interna.

18.7.1. Enfoque de múltiples cortafuegos

Para la mejor protección entre la red privada y la red pública, obtenga por lo menos dos IPs públicas de su ISP, y el uso de un segundo servidor de seguridad para la red pública. Para dar cabida a esto, se pone un interruptor entre la conexión a Internet y la WAN de los dos servidores de seguridad. Esto también tiene la ventaja de poner su red pública de una IP pública diferente de su red privada, así que si usted debe recibir un reporte de abuso, usted será capaz de distinguir fácilmente si su origen en la red pública o privada. El firewall protege su red privada verá la red pública de manera diferente que cualquier host de Internet.

18.7.2. Servidor de seguridad único enfoque

En entornos en los que el enfoque de múltiples cortafuegos es un costo prohibitivo o de otra manera indeseables, puede proteger su red interna mediante la conexión de la red pública a un OPT interfaz en pfSense. Usted debe asignar una subred IP privada dedicada a esta interfaz territorio palestino ocupado, y configurar reglas de firewall para permitir el acceso a Internet, pero no la red interna.

18.7.3. Control de acceso y filtrado de salida consideraciones

Además de no permitir el tráfico de la red de acceso público a la red privada, no son cosas adicionales que usted debe considerar en la configuración de su punto de acceso.

18.7.3.1. Restringir el acceso a la red

Si bien muchos utilizan puntos de acceso abiertos redes inalámbricas sin autenticación, debe considerar protecciones adicionales para evitar el abuso de la red. En el control sin cables, utilizando WPA o WPA2 y proporcionar la contraseña para sus invitados o clientes. Algunos tendrán la frase en un cartel en el vestíbulo o en espera, publicado en una habitación, o le facilitará al solicitud. También considerar la implementación de Portal Cautivo en pfSense (cubierto en Capítulo 19, Cautivas Portal). Esto ayuda a evitar que la gente en otras oficinas y fuera del edificio el uso de la red inalámbrica.

18.7.3.2. Deshabilitar Intra-BSS comunicación

Si su punto de acceso permite, no se debe permitir la comunicación intra-SEV. Esto evita que los clientes inalámbricos se comuniquen con otros clientes inalámbricos, que protege a sus usuarios de los ataques intencionales de otros usuarios de telefonía móvil, así como los no intencionales, como los gusanos.

18.7.3.3. El filtrado de salida

Considere qué tipo de política de salida a configurar. El más básico, permitiendo el acceso a Internet sin permitir el acceso a la red privada, es probablemente la más comúnmente implementado, pero debe tener en cuenta restricciones adicionales. Para evitar que su dirección IP pública negro lista debido a los sistemas infectados en calidad de visitante contra los robots de spam, debería considerar la posibilidad de bloqueo SMTP.

Una alternativa que aún permite a las personas utilizar sus direcciones de correo SMTP, pero limita el efecto de los robots de spam es para crear una regla para SMTP y especificar las entradas máximo por Estado de acogida en virtud de avanzada Opciones en el servidor de seguridad: Reglas: Editar página. Asegúrese de que el Estado está por encima de cualquier otra norma que coinciden con el tráfico SMTP, y especificar un límite bajo. Puesto que las conexiones no siempre puede ser adecuadamente cerrado por el cliente de correo o un servidor, no tendrá que establezca un valor demasiado bajo para evitar el bloqueo los usuarios legítimos, pero un límite de cinco conexiones deben ser razonables. Si lo desea, para especificar máximo estado de las entradas por sistema en todos sus reglas de firewall, pero tenga en cuenta que algunos protocolos se requieren decenas o cientos de conexiones para funcionar. HTTP y HTTPS puede requerir numerosas conexiones para cargar una sola página web en función del contenido de la página y la el comportamiento del navegador, así que no establezca sus límites demasiado bajos.

Usted necesidad de equilibrar los deseos de los usuarios frente a los riesgos inherentes a la concesión de Internet el acceso a los sistemas que no controlan, y definir una política que se adapte a su entorno.

18.8. Solución de problemas de conexiones inalámbricas

En lo que respecta a la tecnología inalámbrica, hay un montón de cosas que pueden salir mal. Desde defectuosa conexiones de hardware a la interferencia de radio de software incompatible / controladores o configuración sencilla desajustes, todo es posible, y puede ser un desafío para que todo funcione a la primera.

Esta sección cubrirá algunos de los problemas más comunes que han sido encontrados por usuarios y desarrolladores de pfSense.

18.8.1. Compruebe la antena

Antes de gastar cualquier momento el diagnóstico de un problema, dobles y triples, compruebe la conexión de la antena. Si se trata de un tornillo en el tipo, asegúrese de que esté completamente apretado. Para las tarjetas mini-PCI, asegúrese de que los conectores del cable flexible están conectados correctamente y que encaje en su lugar. Trenzas en las tarjetas mini-PCI son frágiles y fáciles de descanso. Después de desconectar y volver a conectar a un par de veces, puede ser necesario reemplazarlas.

18.8.2. Pruebe con varios clientes o tarjetas inalámbricas

Para eliminar una posible incompatibilidad entre las funciones inalámbricas pfSense y su red inalámbrica cliente, asegúrese de probar con varios dispositivos o tarjetas de primera. Si el mismo problema se puede repetir con

varias marcas y modelos, es más probable que sea un problema con la configuración o relacionado con el hardware que el dispositivo cliente.

18.8.3. Intensidad de la señal es baja

Si usted tiene una señal débil, incluso cuando usted está cerca de la antena del punto de acceso, consulte la antena de nuevo. Para las tarjetas mini-PCI, si sólo tiene un cable flexible en el uso y hay dos internos conectores, intente conectar con el otro conector interno en la tarjeta. También puede intentar cambiar el Canal o el ajuste de la potencia de transmisión en la configuración de la interfaz inalámbrica. Para mini-Tarjetas PCI, verifique que los extremos rotos de los conectores del cable flexible frágiles donde se conectan a la mini-Tarjeta PCI.

Capítulo 19. Portal Cautivo

La función de Portal Cautivo de pfSense te permite dirigir a los usuarios a una página web antes de que Internet el acceso está permitido. Desde esa página, puede permitir a los usuarios acceder a Internet después de hacer clic a través, o que requieren autenticación. Los usos más comunes de Portal Cautivo es de las comunicaciones inalámbricas puntos calientes, o la autenticación adicionales para permitir el acceso a las redes internas de inalámbricos clientes. También se puede utilizar con clientes de cable, si lo desea.

19.1. Limitaciones

La aplicación de portal cautivo en pfSense tiene algunas limitaciones. Esta sección cubre ellas, y las formas comunes de trabajo alrededor de ellos siempre que sea posible.

19.1.1. Sólo puede ejecutarse en una sola interfaz

Sólo se puede utilizar el portal cautivo en una interfaz de servidor de seguridad. Para las redes en múltiples subredes IP requieren la funcionalidad de portal cautivo, tendrá que utilizar un router dentro de su instalar el portal cautivo como se ilustra en la Figura 19.1, "Portal Cautivo en varias subredes".

19.1.2. No sean capaces de revertir portal

Un portal inverso, que requieren de autenticación para el tráfico que viene en su red de Internet, no es posible.

19.2. Portal de Configuración sin autenticación

Para un portal sencillo sin autenticación, todo lo que necesitas hacer es comprobar la opción Habilitar en cautividad cuadro de portal, seleccione una interfaz, y cargar una página HTML con el contenido de su portal como se describe en Sección 19.5.12, "Portal de contenidos de la página". Es posible que desee especificar una configuración adicional opciones que se detallan en Sección 19.5, "Opciones de configuración".

19.3. Portal de configuración mediante Local Autenticación

Para configurar un portal con autenticación local, marque la casilla Activar portal cautivo, seleccione una de la interfaz, elija la autenticación local, y cargar una página HTML con el contenido de su portal

como se describe en Sección 19.5.12, "Portal de contenidos de la página". Es posible que desee especificar adicionales
opciones de configuración como se detalla en Sección 19.5, "Opciones de configuración". A continuación, configure su los usuarios locales en la ficha Usuarios de los Servicios → Portal Cautivo página.

19.4. Portal de configuración mediante RADIUS Autenticación

Para configurar un portal de autenticación mediante RADIUS, primero configurar el servidor RADIUS, a continuación, siga los mismos procedimientos que la creación de un portal con autenticación local, llenando el información adecuada para su servidor RADIUS. Lea la siguiente sección para obtener información sobre opciones específicas de configuración que desee utilizar.

19.5. Opciones de configuración

En esta sección se describe cada una de las opciones de configuración de Portal Cautivo.

19.5.1. Interfaz

Aquí se selecciona la interfaz de portal cautivo se ejecutarán en. Esto no puede ser una interfaz de puente, y no puede ser cualquier red WAN o interfaz WAN OPT.

19.5.2. Máxima de conexiones simultáneas

Este campo especifica el número máximo de conexiones simultáneas por dirección IP. El valor por defecto el valor es de 4, que debería ser suficiente para la mayoría de entornos. Este límite existe para evitar que un único host de agotar todos los recursos en el servidor de seguridad, ya sea accidental o intencional. Un ejemplo cuando de otro modo sería un problema es un huésped infectado con un gusano. Los miles de conexiones emitió hará que la página de portal cautivo que se generen en varias ocasiones si el anfitrión es no autenticado ya que de otro modo generaría tanta carga que dejaría su sistema deje de responder.

19.5.3. Tiempo de inactividad

Si quiere desconectar a los usuarios inactivo, rellenar un valor aquí. Los usuarios serán capaces de volver a entrar inmediatamente.

19.5.4. Duro tiempo de espera

Para cerrar la sesión con fuerza los usuarios después de un período determinado, introduzca un valor de tiempo de espera duro. Usted debe entrar en ya sea un tiempo de espera duro, tiempo de inactividad o ambos para asegurar sesiones se eliminan si los usuarios no cierre la sesión, lo más probable es que no lo hará. Los usuarios serán capaces de volver a entrar inmediatamente después de que el tiempo de espera difícil, si sus credenciales siguen siendo válidos (para las cuentas locales, no caducado, y para la autenticación RADIUS, usuario puede seguir con éxito la autenticación en RADIUS).

19.5.5. Desconectarse ventana emergente

Marque esta casilla para activar un pop up de cierre de sesión. Por desgracia, ya que la mayoría de los navegadores tienen pop bloqueadores habilitada, esta ventana puede no funcionar para la mayoría de sus usuarios a menos que el control de la las computadoras y pueden excluir de su portal en su bloqueador de elementos emergentes.

19.5.6. Redirección de URL

Si introduce una URL aquí y previa autenticación, o hacer clic en el portal, los usuarios se redirigirá a esta URL en lugar de la que originalmente intentado acceder. Si este campo se deja en blanco, el usuario será redirigido a la dirección que el usuario inicialmente trató de acceso.

19.5.7. los inicios de sesión de usuario concurrente

Si esta casilla está marcada, sólo una entrada por cada cuenta de usuario está permitido. La entrada más reciente es permitidos y los inicios de sesión anterior en virtud de ese nombre de usuario será desconectado.

19.5.8. Filtrado de direcciones MAC

Esta opción le permite desactivar el filtrado de direcciones MAC por defecto. Esto es necesario en el caso de varias subredes detrás de un router mediante el portal, como se ilustra en la Figura 19.1, "en cautividad Portal en varias subredes ", ya que todos los usuarios detrás de un router se mostrará en el portal como el de router dirección MAC.

19.5.9. Autenticación

Esta sección le permite configurar la autenticación, si se desea. Si se deja sin autenticación seleccionado, los usuarios sólo tendrá que hacer clic a través de la pantalla de su portal de acceso. Si usted requiere autenticación, puede utilizar el gestor de usuarios locales o la autenticación RADIUS. Usuario

para el gestor de usuario local se configuran en la ficha Usuarios de los Servicios → Portal Cautivo

página. los usuarios de RADIUS se definen en el servidor RADIUS. Para aquellos con un Microsoft Active Directorio de la infraestructura de red, RADIUS se puede utilizar para autenticar usuarios del portal cautivo de Active Directory con Microsoft IAS. Esto se describe en Sección 24.1, "RADIUS Autenticación con Windows Server ". Existen numerosos servidores RADIUS otros que también pueden ser utilizado. cuentas RADIUS puede tener la posibilidad de enviar la información de uso para cada usuario de la servidor RADIUS. Consulte la documentación de su servidor RADIUS para obtener más información.

19.5.10. HTTPS entrada

Marque esta casilla para utilizar HTTPS para la página del portal. Si marca esta debe introducir un certificado y la clave privada.

19.5.11. Nombre de servidor HTTPS

Este campo es donde se especifica el nombre completo (nombre de host + dominio) que se utilizará para HTTPS. Este debe coincidir con el nombre común (CN) en el certificado para evitar que sus usuarios reciban errores de certificado en sus navegadores.

19.5.12. Portal de contenidos de la página

Aquí cargar una página HTML que contiene la página del portal que verán los usuarios cuando se trata de acceder a Internet antes de autenticar o hacer clic en el portal.

19.5.12.1. Portal de la página sin autenticación

Esto muestra el código HTML de una página del portal que se puede utilizar sin necesidad de autenticación.

```
<html>
<head>
<title> Bienvenido a nuestro portal </ title>
</ Head>
<body>
<p> Bienvenido a nuestro portal </ p>
<p> Haga clic en Continuar para acceder a Internet </ p>
<form method="post" action="$PORTAL_ACTION$">
  <input type="hidden" name="redirurl" value="$PORTAL_REDIRURL$">
  <input type="submit" name="accept" value="Continue">
</ Form>
</ Body>
```

```
</ HTML>
```

19.5.12.2. Portal de la página con la autenticación

Aquí está un ejemplo de página del portal que requieren autenticación.

```
<html>
<head>
<title> Bienvenido a nuestro portal </ title>
</ Head>
<body>
<p> Bienvenido a nuestro portal </ p>
<p> Introduzca su nombre de usuario y contraseña y pulse Entrar para
acceder a Internet </ p>
<form method="post" action="$PORTAL_ACTION$">
  <input name="auth_user" type="text">
  <input name="auth_pass" type="password">
  <input type="hidden" name="redirurl" value="$PORTAL_REDIRURL$">
  <input type="submit" name="accept" value="Login">
</ Form>
</ Body>
</ HTML>
```

19.5.13. Autenticación de contenido página de error

Aquí puede cargar una página HTML se muestren los errores de autenticación. Una de autenticación error se produce cuando un usuario introduce un nombre de usuario o contraseña, o en el caso de RADIUS autenticación, potencialmente un servidor RADIUS inalcanzable.

19.6. Solución de problemas de portal cautivo

Esta sección contiene sugerencias para la solución del problema más común con el portal cautivo.

19.6.1. Autenticación de fracasos

Los errores de autenticación son normalmente el resultado de los usuarios ingresar un nombre de usuario incorrecto o contraseña. En el caso de la autenticación RADIUS, pueden ocurrir debido a la conectividad problemas con el servidor RADIUS, o problemas en el servidor RADIUS propia. Revise su servidor RADIUS de los registros de las indicaciones de por qué se negó el acceso, y asegurar el servidor de seguridad puede comunicarse con el servidor RADIUS.

19.6.2. Portal de la página no carga (a veces) ni cualquier otro carga de la página

Se ha informado a suceder cuando se utiliza Portal Cautivo en una VLAN, pero la interfaz de los padres de la VLAN se asigna también como otra interfaz en pfSense. Por ejemplo, si `vlan0` es VLAN etiquetas 10 en `fxp1`, No se puede tener `fxp1` asignado como cualquier otra interfaz, que debe dejarse de lado.

Esta es la configuración recomendada de todas formas, y este problema es una razón más para seguir ese consejo.

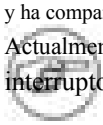
Capítulo 20. Firewall de redundancia y Alto Disponibilidad

pfSense es una de las soluciones de código abierto que ofrece muy pocas alta disponibilidad de clase empresarial
capacidades de conmutación por error de estado, lo que permite la eliminación del servidor de seguridad como un solo punto
del fracaso. Esto está previsto por la combinación de CARP, pfsync y pfSense de XML-RPC
sincronización de la configuración, cada uno de los cuales se explican en este capítulo. A menudo esto es simplemente se refiere como la carpa, aunque técnicamente CARP es sólo una parte de la solución completa.

20.1. CARP Información general

Común Dirección Redundancy Protocol (CARP) fue creado por los desarrolladores de OpenBSD como un país libre,
solución de redundancia abierto para compartir las direcciones IP entre un grupo de dispositivos de red. Similares soluciones ya existentes, principalmente el estándar del IETF para Virtual Router Redundancy Protocol (VRRP). Sin embargo Cisco reclamaciones VRRP está cubierto por su patente sobre su Hot Standby Router Protocolo (HSRP), y dijo a los desarrolladores de OpenBSD, que sería hacer valer sus patentes. Por lo tanto, el los desarrolladores de OpenBSD ha creado un nuevo protocolo libre, abierto para lograr el mismo resultado sin infringir las patentes de Cisco. CARP se dispuso en octubre de 2003 en OpenBSD,
y más tarde se añadió a FreeBSD también.

Cada firewall pfSense en un grupo CARP tiene su propia dirección IP asignada en cada interfaz,
y ha compartido la CARPA VIP asignado también. Estas IPs CARP sólo se activan si el servidor de seguridad es Actualmente el maestro. Si un fallo de cualquier interfaz de red es detectada, el firewall de última designado interruptores de dominar en todas las interfaces.



Nota

Debido a que cada miembro del grupo CARP debe tener una dirección IP en una subred, además de
la dirección IP CARP, por lo menos tres direcciones IP disponibles se requieren para cada interfaz, y más direcciones IP para los miembros del grupo adicional. Esto también se aplica a la interfaz WAN, así que asegúrese de tener al menos tres disponibles IP enrutable Las direcciones de su ISP. El bloque más pequeño enrutable que incluye 3 direcciones IP es un / 29, que tiene 8 direcciones (6 utilizable).

20.2. pfsync Información general

pfsync permite la sincronización de la tabla de estado de servidor de seguridad desde el servidor de seguridad maestro cortafuegos secundaria. Cambios en la tabla de estado de la primaria son enviados en la red para el

servidor de seguridad secundaria (s). Esto utiliza multidifusión de forma predeterminada, aunque una dirección IP se puede definir
en la interfaz de pfSense para forzar las actualizaciones de unidifusión para ambientes con sólo dos servidores de seguridad donde el tráfico multicast no funcionará correctamente (algunos interruptores de bloqueo o ruptura de multidifusión). Usted puede utilizar cualquier interfaz activa para el envío de actualizaciones pfsync, sin embargo se recomienda la utilización de
una interfaz dedicada por razones de seguridad y rendimiento. pfsync no admite ninguna tipo de autenticación, así que si usted usa otra cosa que una interfaz dedicada, es posible para cualquier usuario con acceso a la red local a los estados insertar en su servidor de seguridad secundaria. En baja entornos de rendimiento que no son de seguridad paranoica, el uso de la interfaz LAN para este fin es aceptable. Ancho de banda necesario para esta sincronización de estado pueden variar significativamente de un medio ambiente a otro, pero podría ser tan alta como 10% del rendimiento atravesar el firewall dependiendo de la velocidad de inserciones y deleciones en el estado de la red.
El beneficio de pfsync se puede conmutar por error sin perder la tabla de estado, lo que permite conmutación por error sin fisuras. En algunos entornos, no notará la diferencia entre la conmutación por error statefully y la pérdida de estado durante la conmutación por error. En otras redes, puede causar un importante pero breve corte de red.

20.2.1. pfsync y actualizaciones

Normalmente pfSense permitiría mejoras servidor de seguridad sin ningún tipo de interrupciones en la red. Por desgracia, esto no es siempre el caso con mejoras como el protocolo de pfsync ha cambiado para dar cabida a funcionalidad adicional. Es de esperar que no será el caso en el futuro, pero si usted está la actualización de pfSense 1.2 a 1.2.1 o superior, el sistema operativo subyacente pasó de FreeBSD 6.2 a 7.x, e incluye un pfsync más reciente. Siempre revise la guía de actualización en todos los vinculados liberación anuncios antes de actualizar a ver si hay alguna consideración especial para los usuarios CARP.

20.3. pfSense XML-RPC Sync Información general

pfSense sincronización de configuración le permite aprovechar al máximo los cambios de configuración en un solo el servidor de seguridad primaria, que luego se replica los cambios a lo largo de la secundaria de forma automática. Las áreas apoyadas por esto son las reglas del cortafuegos, programas de servidor de seguridad, alias, NAT, IPsec, Wake on
LAN, las rutas estáticas, equilibrador de carga, Virtual IP, conformador de tráfico, y promotor de DNS. Otros ajustes debe configurar de forma individual en el firewall secundaria, según sea necesario, aunque la sincronización cubre la mayoría si no todos, de lo que habitualmente va a cambiar. Configuración de la sincronización debe utilizar la misma interfaz que el tráfico de su pfsync.

20.4. Ejemplo de configuración redundante

En esta sección se describen los pasos en la planificación y configuración de una interfaz simple de tres CARP de configuración. Las tres interfaces LAN, WAN y pfsync. Esto es funcionalmente equivalente

a una interfaz LAN dos y el despliegue de WAN, con la interfaz de pfsync ser usado únicamente para sincronizar los estados de configuración y seguridad entre los servidores de seguridad primaria y secundaria.

20.4.1. Determinar las asignaciones de dirección IP

En primer lugar usted necesita para planificar su asignación de direcciones IP. Una buena estrategia es usar el más bajo utilizable
IP en la subred de la IP CARP, el IP de próxima posteriores como interfaz IP del servidor de seguridad primaria, y
la IP de próxima como interfaz IP del servidor de seguridad secundario. Usted puede asignar estos como se desee, lo que la elección
un esquema que tiene más sentido para usted es recomendado.

20.4.1.1. Direccionamiento WAN

Las direcciones WAN serán seleccionados de los asignados por su ISP. Para el ejemplo de la Tabla 20.1, "WAN asignaciones de dirección IP", La WAN de la pareja CARP está en una red privada, y las direcciones a través 10.0.66.10 10.0.66.12 se utilizará como las direcciones IP WAN.

Dirección IP	Uso
10.0.66.10	CARP IP compartida
10.0.66.11	Primaria firewall IP de la WAN
10.0.66.12	Secundaria firewall IP de la WAN

Tabla 20.1. WAN asignaciones de dirección IP

20.4.1.2. LAN de direccionamiento

La subred LAN es 192.168.1.0/24. Para este ejemplo, las direcciones IP LAN será asignado como se muestra en Tabla 20.2, "LAN asignaciones de dirección IP".

Dirección IP	Uso
192.168.1.1	CARP IP compartida
192.168.1.2	Primaria firewall IP de la LAN
192.168.1.3	Secundaria firewall IP de la LAN

Tabla 20.2. LAN asignaciones de dirección IP

20.4.1.3. Abordar pfsync

No habrá compartido CARP IP en esta interfaz porque no hay necesidad de uno. Estas direcciones IP son utilizarse únicamente para la comunicación entre los servidores de seguridad. Para este ejemplo, voy a utilizar 172.16.1.0/24

como la subred pfsync. Sólo dos períodos de investigación se utilizará, pero voy a usar un / 24 para ser coherentes con los
otra interfaz interna (LAN). Para el último octeto de las direcciones IP, elegí el último octeto mismo como el servidor de seguridad IP de la LAN de la coherencia.

Dirección IP	Uso
172.16.1.2	Primaria firewall IP de la LAN
172.16.1.3	Secundaria firewall IP de la LAN

Tabla 20.3. pfsync dirección IP de misiones

En la figura 20.1, "Ejemplo de diagrama de CARP red" se puede ver el diseño de este ejemplo CARP grupo. La primaria y secundaria, cada uno tiene conexiones idénticas a la WAN y LAN, y un cable de conexión entre ellos para conectar las interfaces pfsync. En este ejemplo básico, el WAN y LAN Interruptor siguen siendo posibles puntos de fallo. Conmutación de la redundancia se trata más adelante en este capítulo en Sección 20.8, "Capa 2 redundancia".

20.4.2. Configurar el servidor de seguridad primaria

En primer lugar vamos a tener todo funcionando como se desea en la primaria, la secundaria se agregó. Deja el firewall desactivado secundaria hasta llegar a ese punto.

20.4.2.1. Instalación, interfaz de asignación y configuración básica

Ir a través de la asignación de instalación y una interfaz de manera diferente que si se tratara de un solo instalar. Asigne la dirección IP previamente designado a la interfaz LAN, y entrar en la web interfaz para continuar. Ir a través del asistente de inicio, seleccionar la zona horaria, la configuración de la IP estática previamente designados para el servidor de seguridad primaria en la WAN, y el establecimiento de su administrador
contraseña. Continuar con el siguiente paso después de completar el asistente de arranque (ver de nuevo a Sección 4.2, "Asistente de configuración" si es necesario).

20.4.2.2. Configuración de las IPs virtuales CARP

Vaya a Servidor de seguridad → IP virtual y haga clic para añadir su primera CARPA VIP. La edición virtual IP Se mostrará la pantalla, como se ve en Figura 20.2, "IP WAN CARP"

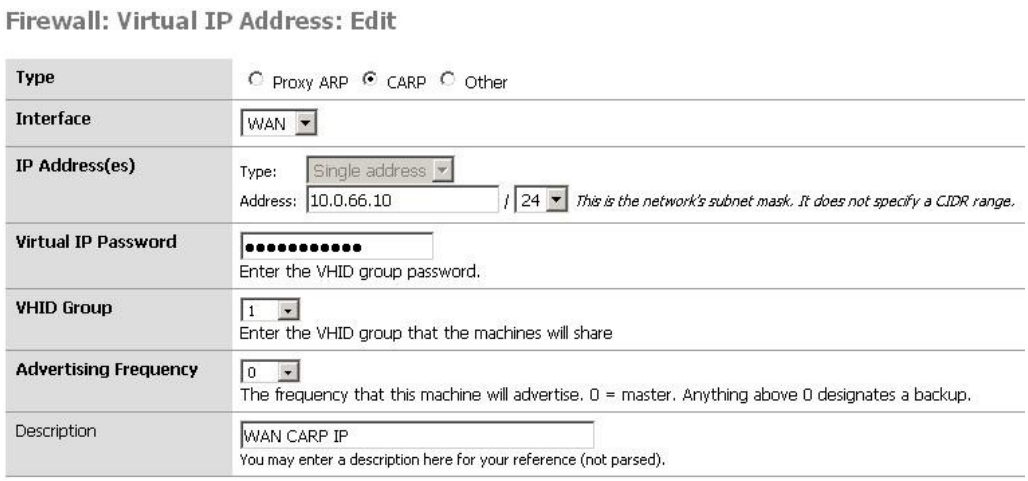


Figura 20.2. WAN IP CARP

Para el tipo, seleccione **CARP**. La interfaz se debe establecer en **WAN**. Para obtener la dirección IP, introduzca en el compartir, dirección IP WAN elegido antes. En este ejemplo, es **10.0.66.10**. El Virtual IP contraseña puede ser cualquier cosa que te gusta, y siempre y cuando todos sus sistemas de uso de pfSense con su sincronización de la configuración, no lo que necesitas saber esta contraseña, ya que automáticamente sincronizarse con el servidor de seguridad secundaria. Puede generar una contraseña al azar usando una contraseña herramienta de generación, o golpear al azar en el teclado para crear una. Cada IP CARP en un par de cortafuegos debe utilizar un único grupo VHID (Virtual Host ID), y también debe ser diferente de cualquier VHIDs en uso en cualquier interfaz de red conectada directamente si CARP o VRRP es también presente en otros routers o cortafuegos en su red. Si usted no tiene ninguna otra carpa o VRRP tráfico presente en su red, usted puede comenzar a **1**. De lo contrario, se establece en el VHID disponible siguiente en la red. La frecuencia de publicidad debe establecerse de acuerdo a la función de esta máquina en del grupo. Ya que éste será el maestro, que debe establecerse en **0**. En el sistema de copia de seguridad, esto debe se **1** o superior. Por la descripción, escriba algo relevante como **WAN IP CARP**. Haga clic en Guardar cuando haya terminado.

Ahora haga clic para añadir otra IP virtual para la LAN (Figura 20.3, "LAN CARP IP"). Esta vez, Tipo conjunto de **CARP**, Interfaz de **LAN**, Y la dirección IP a la IP LAN compartidas, **192.168.1.1**. Este IP virtual contraseña es para otro grupo de investigación, por lo que no tiene que coincidir con el de la WAN, y otra vez que nunca se necesita saber la contraseña. El VHID debe ser diferente de la de la WAN IP CARP, por lo general se establece un número mayor, en este caso **2**. Una vez más, ya que este sistema es dueño de la frecuencia de publicidad debe ser **0**. Por la descripción, escriba **IP LAN CARP** o algo similar descriptivo. Haga clic en Guardar cuando haya terminado.

Después de guardar la LAN IP CARP, podrás ver ambas personalidades en la lista, como en la Figura 20.4, "Virtual IP
lista ". Haga clic en Aplicar cambios y luego ambos IPs CARP se activa.

20.4.2.3. Configurar salida NAT para la carpa

El siguiente paso será configurar NAT para que los clientes de la LAN utilizará la WAN para compartir la propiedad intelectual como la dirección. Vaya a Servidor de seguridad → NAT, y haga clic en la ficha de salida. Seleccione la opción de habilitar
Manual de salida NAT (NAT avanzada de salida), a continuación, haga clic en Guardar.

Una regla que parece que se NAT el tráfico de LAN a la WAN IP. Puede ajustar esta norma a
trabajar con la dirección IP en lugar del CARP. Haga clic en el a la derecha de la regla. En la traducción sección, seleccione la WAN CARP dirección IP de la Dirección desplegable. Cambiar la descripción
mencionar que esta regla NAT LAN a la WAN CARP. Como referencia, se puede comparar
su configuración de salida regla de NAT para los de la Figura 20.5, "Entrada de salida NAT"

Después de hacer clic en Guardar en la regla de NAT, y haga clic en Aplicar cambios, las nuevas conexiones dejando la WAN ahora se traducirá a la IP CARP. Puede confirmar esto con un sitio web que
muestra la dirección IP desde la que está siendo visitada, como http://www.pfsense.org/ip.php .

También debe ver la salida de esta ajustada regla NAT en la lista, como en la figura 20.6, "Configuración avanzada NAT de salida".

20.4.2.4. Configurar pfsync

La siguiente tarea consiste en configurar la interfaz pfsync que será la línea de comunicación entre el servidor de seguridad primaria y de copia de seguridad. Vaya a las interfaces → OPT1 para configurar esta opción. Si usted no tiene
una interfaz OPT1 sin embargo, usted tendrá que asignar en Interfaces → (Asignar) (véase Sección 4.3.1, "Asignar interfaces").

Sólo unas pocas opciones es necesario establecer, como se muestra en Figura 20.7, "pfsync Interfaz de configuración".
La interfaz tiene que estar habilitado y que ayudaría a utilizar **pfsync** por su nombre. Hay que establecido para una dirección IP estática, y teniendo en cuenta la dirección decidida anteriormente para el lado primario de pfsync,
172.16.1.2/24.

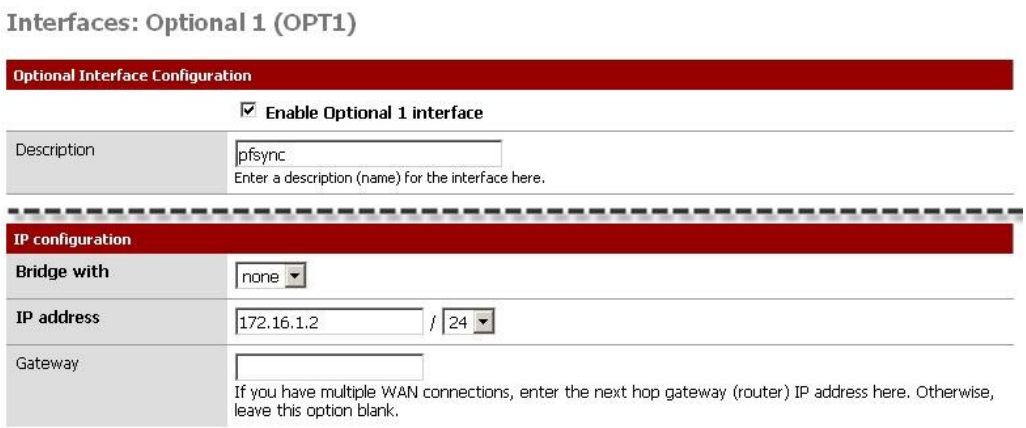


Figura 20.7. pfsync interfaz de configuración

Cuando haya terminado de introducir la información para la interfaz pfsync, haga clic en Guardar.

La interfaz pfsync también necesitará una regla de firewall para permitir el tráfico de la copia de seguridad. Ir al cortafuegos → Reglas, y haga clic en la ficha pfsync. Añadir una nueva regla de firewall que se permita el tráfico de cualquier protocolo de cualquier fuente a cualquier destino. Dado que esto sólo será una conexión directa privada con un cable de conexión, se puede permitir todo el tráfico desde el punto pfsync.

20.4.2.5. Modificar el servidor DHCP

Si pfSense está actuando como un servidor DHCP, es necesario instruir a asignar una IP CARP como puerta de entrada IP. De lo contrario pfSense hará uso de su comportamiento por defecto de asignar la IP configurada en la interfaz como puerta de entrada. Que la propiedad intelectual es específico para el servidor de seguridad primaria, por lo que necesita para cambiar a una IP CARP de conmutación por error a trabajar para sus sistemas de cliente DHCP.

Vaya a Servicios → Servidor DHCP. Cambie el campo Puerta de enlace de **192.168.1.1**, La compartida CARP LAN IP. Ajuste el punto de conmutación por error IP a la actual dirección IP del sistema de copia de seguridad, **192.168.1.3**. Esto permitirá que el servicio DHCP en ambos sistemas para mantener un conjunto común de los arrendamientos.

Guardar y, a continuación, en Aplicar cambios.

20.4.3. Configuración del servidor de seguridad secundaria

A continuación las interfaces, direcciones IP, y las reglas del firewall en la necesidad de secundaria a ser configurado.

20.4.3.1. Interfaz de misiones y de direccionamiento IP

Antes de conectar las interfaces WAN, LAN, o pfsync, el poder en el sistema y pasar por la asignación de instalación y una interfaz que lo hizo para el servidor de seguridad primaria. Establezca la IP de la LAN desde la consola a la copia de seguridad previamente designado IP LAN del **192.168.1.3**, Establezca el DHCP configuración de la misma que la primaria, y luego debe ser seguro para conectar las conexiones de red.

A continuación, debe acceder a la interfaz web y pasar por el asistente de configuración, tal como se hizo en el primario. Configurar la IP WAN, y establecer la contraseña de administrador para el mismo valor que el en el primario.

También tendrá que configurar la interfaz de sincronización como en Sección 20.4.2.4, "pfsync Configurar", Pero con la dirección IP elegida para el sistema de copia de seguridad

20.4.3.2. Reglas del firewall

Usted necesitará una regla de firewall temporal para permitir la configuración inicial de sincronización a suceder. Ir para Firewall → Reglas, y haga clic en la ficha pfsync. Añadir una nueva regla de firewall que se permita el tráfico de cualquier protocolo de cualquier fuente a cualquier destino. Ponga "temporal" en la descripción para que pueda estar seguro de que ha sido sustituido más tarde. La regla debe ser similar a Figura 20.8, "Servidor de seguridad de pronunciarse sobre interfaz pfsync "

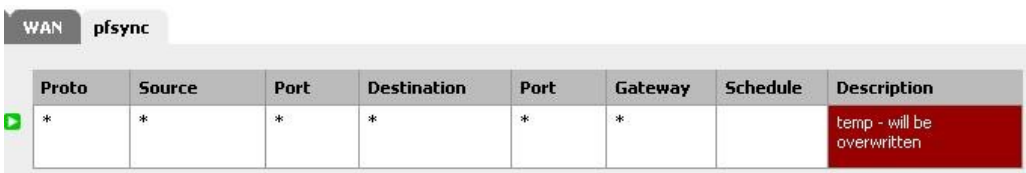


Figura 20.8. Servidor de seguridad de Estado en la interfaz pfsync

20.4.4. Configurar sincronización de la configuración

El último paso es configurar la sincronización de la configuración entre la primaria y de copia de seguridad.

En el servidor de seguridad único maestro, vaya a Servidor de seguridad de → Virtual IP, y haga clic en la ficha Configuración de CARP.

Compruebe Sincronizar habilitado, y recoger **pfsync** como sincronizar la interfaz. Para el pfsync sincronización entre pares IP, escriba la dirección IP para la interfaz de pfsync el sistema de copia de seguridad, **172.16.1.3**. Revise todas las casillas restantes en la pantalla, e introduzca el período de investigación del sistema de copia de seguridad de pfsync de nuevo en

Sincronizar con la propiedad intelectual. Por último, introduzca la contraseña WebGUI admin en la contraseña de sistemas remotos
caja. Haga clic en Guardar cuando haya terminado.

Cuando la configuración de sincronización se guardan en la primaria, automáticamente copiará los configuración de la primaria a la copia de seguridad para cada opción seleccionada en la página de Configuración de CARP. Este
incluye la configuración adecuada de salida NAT para la carpa, las reglas del cortafuegos para la interfaz pfsync, e incluso las personalidades CARP. Dentro de los 30 segundos, la sincronización de la configuración inicial debería haber terminado.

La configuración del servidor DHCP no están sincronizados, lo que los cambios en el sistema de copia de seguridad se necesario establecer el período de investigación CARP como puerta de entrada, y utilizar las primarias de la dirección IP LAN como la
DHCP pares de conmutación por error, como en Sección 20.4.2.5, "Modificación del servidor DHCP".

Si la configuración de sincronización de la primaria a la copia de seguridad, entonces usted sabe que la interfaz de sincronización
está conectado y funcionando correctamente. Si no, puedes ir a diagnósticos → Ping, escoger el pfsync interfaz, e intentar hacer ping a la pfsync dirección IP del sistema de oposición. Si eso no funciona, compruebe que está utilizando un cable de conexión y / o tener una luz de enlace en la interfaz pfsync de ambos sistemas.

La pareja CARP ahora se activa, pero todavía tendrá que comprobar el estado y la prueba de que la conmutación por error está funcionando correctamente. Salte a Sección 20.6, "la funcionalidad de conmutación por error de Verificación" para el resto.

Nota

Usted no debe configurar la sincronización desde el servidor de seguridad de copia de seguridad para el maestro
cortafuegos. Existen protecciones que se deben evitar este lazo de la sincronización de causar daño, pero se desordenan los registros con mensajes de error y nunca debe ser configurado de esta manera.

20.5. Multi-WAN con CARP

También puede implementar CARP para la redundancia de servidor de seguridad en una configuración multi-WAN, siempre
como todas las interfaces WAN tener al menos 3 direcciones IP estáticas cada uno. Esta sección se detallan los VIP y configuración de NAT necesarios para un despliegue de doble WAN CARP. Esta sección sólo se tratan temas específica a la carpa y multi-WAN.

20.5.1. Determinar las asignaciones de dirección IP

Para este ejemplo, cuatro direcciones IP se utilizan en cada WAN. Cada uno necesita un servidor de seguridad IP, además

de una carpa

IP de salida NAT, más uno para un NAT 1:1 que se utiliza para un servidor de correo interno
el segmento de la DMZ.

20.5.1.1. WAN y WAN2 direccionamiento IP

Tabla 20.4, "Direccionamiento IP WAN" y Tabla 20.5, "WAN2 direccionamiento IP" mostrar la IP abordar tanto para redes WAN. En la mayoría de estos entornos se IPs públicas.

Dirección IP	Uso
10.0.66.10	IP compartidas CARP para NAT Saliente
10.0.66.11	Primaria firewall IP de la WAN
10.0.66.12	Secundaria firewall IP de la WAN
10.0.66.13	IP compartidas CARP para NAT 01:01

Tabla 20.4. Direccionamiento IP WAN

Dirección IP	Uso
10.0.64.90	IP compartidas CARP para NAT Saliente
10.0.64.91	Primaria cortafuegos WAN2 IP
10.0.64.92	Secundaria cortafuegos WAN2 IP
10.0.64.93	IP compartidas CARP para NAT 01:01

Tabla 20.5. Direccionamiento IP WAN2

20.5.1.2. LAN de direccionamiento

La subred LAN es 192.168.1.0/24. Para este ejemplo, las direcciones IP LAN se asignará de la siguiente manera.

Dirección IP	Uso
192.168.1.1	CARP IP compartida
192.168.1.2	Primaria firewall IP de la LAN
192.168.1.3	Secundaria firewall IP de la LAN

Tabla 20.6. LAN asignaciones de dirección IP

20.5.1.3. DMZ de direccionamiento

La subred DMZ es 192.168.2.0/24. Para este ejemplo, las direcciones IP LAN se asignan de la siguiente en Tabla 20.7, "zona de distensión asignaciones de direcciones IP".

Dirección IP	Uso
192.168.2.1	CARP IP compartida
192.168.2.2	Primaria cortafuegos IP DMZ
192.168.2.3	Secundaria cortafuegos IP DMZ

Tabla 20.7. DMZ asignaciones de dirección IP

20.5.1.4. Abordar pfsync

No habrá compartido CARP IP en esta interfaz porque no hay necesidad de uno. Estas direcciones IP sólo se utilizan para la comunicación entre los servidores de seguridad. Para este ejemplo, 172.16.1.0/24 se ser utilizado como la subred pfsync. Sólo dos períodos de investigación se utilizará, pero a / 24 se utiliza para ser coherente con las interfaces internas. Para el último octeto de las direcciones IP, el octeto misma como la última cortafuegos IP LAN es elegida para la coherencia.

Dirección IP	Uso
172.16.1.2	Primaria firewall IP de la LAN
172.16.1.3	Secundaria firewall IP de la LAN

Tabla 20.8. pfsync dirección IP de misiones

20.5.2. Configuración de NAT

La configuración de NAT utilizando las carpas es la misma que sin ella, aunque es necesario utilizar sólo CARPA VIP, o IPs públicas en una subred dirigida a uno de sus asociados en la ejecución CARP para garantizar que estas direcciones siempre son accesibles. Ver Capítulo 7, Network Address Translation Para obtener más información sobre configuración de NAT.

20.5.3. Configuración del Firewall

Con Multi-WAN necesita una política para la red local a la ruta a la puerta de enlace predeterminada de otra manera cuando intenta enviar el tráfico a la dirección de CARP en su lugar saldrá una secundaria Conexión WAN.

Es necesario añadir una regla en la parte superior de las reglas del firewall para todas las interfaces internas que dirigirá tráfico para todas las redes locales a la puerta de enlace predeterminada. La parte importante es la puerta de entrada tiene que ser

predeterminado para esta regla y no una de las conexiones de conmutación por error o equilibrio de carga. El destino de
esta regla debe ser la red local LAN, o un alias que contiene todas las redes a nivel local accesible.

20.5.4. Multi-WAN CARP con DMZ Diagrama

Debido a la WAN y los elementos adicionales zona de despeje, un diagrama de este diseño es mucho más compleja como puede verse en la Figura 20.9, "Diagrama de Multi-WAN CARP con zona de distensión".

20.6. Comprobación de la funcionalidad de conmutación por error

Desde que uso CARP es sobre la alta disponibilidad, debe ser probado a fondo antes de ser colocada en la producción. La parte más importante de que la prueba es asegurarse de que los pares se CARP gracia de conmutación por error durante interrupciones del sistema.

Si ninguna de las acciones en esta sección no funcionan como se espera, consulte Sección 20.10, "CARP Solución de problemas ".

20.6.1. Compruebe el estado CARP

En ambos sistemas, vaya a Estado → CARP (failover). El principal debería mostrar MASTER para el estado de todas las personalidades CARP. El sistema de copia de seguridad deben mostrar copia de seguridad como el estado. Si el
sistema de respaldo en lugar muestra MINUSVALIDOS, haga clic en el botón Activar CARP, a continuación, volver a cargar y la
Condición Jurídica y Social → CARP (failover) página. Ahora debe aparecer correctamente.

20.6.2. Compruebe configuración de la replicación

Vaya a lugares clave en el router de copia de seguridad, como cortafuegos → Reglas y Firewall → NAT y garantizar que las normas creadas sólo en el sistema primario se replica en las copias de seguridad.

Si ha seguido el ejemplo anterior en este capítulo, usted debe ver que su "temperatura" reglas del firewall en la interfaz pfsync ha sido sustituido por el imperio de la primaria.

20.6.3. Comprobar el estado de conmutación por error de DHCP

Si ha configurado la conmutación por error de DHCP, su estado se puede comprobar yendo al Estado → DHCP Arrendamientos. Una nueva sección aparecerá en la parte superior de la página que contiene el estado del DHCP Piscina de conmutación por error, como en Figura 20.10, "Condición Jurídica y Social de conmutación por

error DHCP Pool".

Failover Group	My State	Since	Peer State	Since
"dhcp0"	normal	2009/07/21 16:33:03	normal	2009/07/21 12:24:34

Figura 20.10. Conmutación por error de DHCP Pool Estado

20.6.4. Prueba de conmutación por error CARP

Ahora para la prueba de conmutación por error real. Antes de empezar, asegúrese de que se puede navegar desde un cliente detrás de
el par CARP tanto con pfSense cortafuegos en línea y funcionando. Una vez que se confirma al trabajo, sería un momento excelente para hacer una copia de seguridad.

Para la prueba real, desenchufe el principal de la red o bien apagarlo. Usted debe ser capaz de mantener a navegar por Internet a través del enrutador de copia de seguridad. Comprobar estado → CARP (failover) de nuevo en
la copia de seguridad y ahora debe informar que es MASTER para la LAN y la WAN CARPA VIP.

Ahora que el sistema primario de nuevo en línea y debe recuperar su papel como maestro, y el sistema de reserva debería degradar a BACKUP una vez más, y debe conectividad a Internet todavía funcionan correctamente.

Debe probar el par CARP en situaciones de error tanto como sea posible. Otro individuo Las pruebas pueden incluir:

- Desconecte el cable de LAN o WAN
- Saque el enchufe de alimentación de la primaria
- Desactivar CARP en la primaria
- Pruebe con cada sistema individual (apagar copia de seguridad, de alimentación y apague el el primario)
- Descargar un archivo o tratar de streaming de audio / vídeo durante la conmutación por error
- Pruebe con un ping continuo a un host de Internet durante la conmutación por error

20.7. Proporcionar redundancia Sin NAT

Como se mencionó anteriormente, sólo CARPA VIP proporcionar redundancia y sólo pueden ser utilizados en junto con NAT. También puede proporcionar redundancia para enrutar subredes IP pública con la carpa.
En esta sección se describe este tipo de configuración, que es común en grandes redes, ISP y redes inalámbricas de ISP, y entornos de co-localización.

20.7.1. Asignación de IP pública

Usted necesitará por lo menos un / 29 públicos bloque de IP de la WAN de pfSense, que proporciona seis direcciones IP en uso. Sólo tres son necesarios para una implementación de firewall de dos, pero este es el más pequeño Subred IP que se acomoda a tres direcciones IP. Cada servidor de seguridad requiere un período de investigación, y la necesidad de que
por lo menos una CARPA VIP en el lado WAN.

La segunda subred IP pública se dirigirá a una de sus personalidades CARP por su proveedor de Internet, coubicación proveedor, o el router aguas arriba si el control de esa parte de la red. Debido a esta subred
se encamina a un VIP CARP, el enrutamiento no se depende de un único servidor de seguridad. Para el representado configuración de ejemplo en este capítulo, un / 23 de subred IP pública será utilizado y lo estar en dos subredes / 24 redes.

20.7.2. Red de Información general

La red de ejemplo se muestra aquí es un entorno de co-ubicación que consta de dos pfSense
se instala con cuatro interfaces de cada uno - WAN, LAN, DBDMZ y pfsync. Esta red contiene un número de servidores web y bases de datos. No se basa en ninguna red real, pero hay un sinnúmero de producción similar a este despliegue.

20.7.2.1. De redes WAN

La WAN es donde la red se conecta a la red de aguas arriba, ya sea su proveedor de Internet, co-proveedor de la ubicación o el router aguas arriba.

20.7.2.2. Conexión de redes

LAN en pfSense es un nombre de interfaz fija, y es una interfaz requerida en el punto 1.2. LAN no se un nombre descriptivo apropiado para este segmento en esta implementación. El segmento de LAN en esta red contiene servidores web, y sería más apropiado descrito como una zona de despeje o segmento de los servidores Web, pero se LAN aquí a causa de esta restricción. Es posible que desee añadir una interfaz de quinto a los servidores de seguridad en esta circunstancia, y dejar la interfaz asignada como LAN desenchufada para que sus interfaces con nombres más descriptivos. pfSense 2.0 permite cambiar el nombre de la Conexión de la interfaz, por lo que este no será un examen en el futuro. Con frecuencia se utilizan en las VLAN este tipo de despliegues, en cuyo caso se puede asignar una VLAN no utilizada a la LAN, y el uso de una el apropiado nombre de interfaz de optar por esta red interna, en lugar de LAN.

20.7.2.3. DBDMZ Red

Este segmento es una interfaz OPT y contiene los servidores de base de datos. Es común para segregar los servidores web y bases de datos en dos redes en entornos de alojamiento. Los servidores de base de datos

no deberían nunca requerir acceso directo desde Internet, y por lo tanto están menos sujetos a compromiso que los servidores web.

20.7.2.4. pfsync Red

La red pfsync en este diagrama se utiliza para replicar los cambios de configuración a través de XML pfSense RPC y para pfsync para replicar cambios de estado de la tabla entre los dos servidores de seguridad. Como se describe anteriormente en este capítulo, una interfaz dedicada para este propósito se recomienda.

20.7.2.5. Diseño de redes

Figura 20.11, "Diagrama del CARP con enrutado IP" ilustra este diseño de red, incluyendo todos los enrutable direcciones IP, LAN, y la zona de distensión de base de datos.

Nota

Segmentos que contienen los servidores de bases de datos normalmente no tienen que ser público acceso, y por lo tanto sería más común el uso privado subredes IP, pero la ejemplo ilustrado aquí se pueden utilizar independientemente de la función de las dos internas subredes.

20.8. La redundancia de capa 2

Los diagramas anteriormente en este capítulo no describió la capa 2 (interruptor) de redundancia, para evitar lanzando muchos conceptos a los lectores al mismo tiempo. Ahora que tiene una comprensión de redundancia de hardware con pfSense, esta sección cubre la capa de dos elementos de diseño que deben considerar al planear una red redundante. En este capítulo se asume una implementación del sistema dos, aunque las escalas de las instalaciones hasta que usted requiere.

Si ambos sistemas redundantes pfSense están conectados en el mismo interruptor en cualquier interfaz, que interruptor se convierte en un punto único de fallo. Para evitar este punto único de fallo, la mejor opción es de desplegar dos interruptores para cada interfaz (que no sea la interfaz pfsync dedicado).

El diagrama de enrutado IP está centrada en la red, no se incluye la infraestructura de conmutación. La Figura 20.12, "Diagrama del CARP redundante con switches" ilustra la forma en que el medio ambiente mira con una infraestructura de conmutación redundante.

20.8.1. Interruptor de configuración

Cuando utilice varios modificadores, debe interconexión. Mientras usted tiene una sola conexión entre los dos interruptores, y no el puente en cualquiera de los servidores de seguridad, esto es seguro

con cualquier tipo de interruptor. En caso de superar el uso, o cuando existen múltiples interconexiones entre los interruptores, se debe tener cuidado para evitar la capa 2 bucles. Usted necesitará un switch administrado que se capaz de utilizar Spanning Tree Protocol (STP) para detectar y bloquear los puertos que de otra manera interruptor de crear bucles. Cuando se usa STP, si un vínculo activo muere, por ejemplo, Fallo del interruptor, a continuación, una copia de seguridad
vínculo automático puede ser educado en su lugar.

En pfSense 2.0, también se prestará apoyo añadido para el `lagg (4)` agregación de enlaces y conmutación por error de enlace
interfaz que también le permite tener varias interfaces de red conectado a uno o más
interruptores para tolerancia a fallos más.

20.8.2. Anfitrión de redundancia

Es más difícil obtener redundancia de acogida para sus sistemas críticos dentro del firewall. Cada sistema puede tener dos tarjetas de red y una conexión a cada grupo de interruptores utilizando Link Agregación de Control Protocol (LACP) o una funcionalidad similar específica del proveedor. Los servidores podrían También tienen múltiples conexiones de red, y dependiendo del sistema operativo que puede ser capaz de ejecutar CARP en un conjunto de servidores de modo que sería redundante así. Proporcionar redundancia de acogida es más específica a las capacidades de los interruptores y el sistema operativo del servidor, que está fuera el alcance de este libro.

20.8.3. Otros puntos únicos de fallo

Cuando se trata de diseñar una red totalmente redundante, hay muchos puntos de fallo que a veces se perdió. Dependiendo del nivel de tiempo de actividad que se espera alcanzar, hay más y más cosas a considerar que una falla simple interruptor. Éstos son algunos ejemplos más de la redundancia en una escala más amplia:

- Cada segmento redundante debería tener el poder aislado.
  - Los sistemas redundantes debe estar en interruptores separados.
  - Uso de múltiples bancos de UPS y generadores.
  - Utilice los proveedores de potencia, entrando en los lados opuestos del edificio cuando sea posible.
- Incluso una configuración multi-WAN no es garantía de disponibilidad de Internet.
  - El uso de múltiples tecnologías de conexión a Internet (DSL, Cable, T1, fibra, wi-fi).
  - Si cualquiera de las dos compañías utilizan el mismo polo / túnel / ruta, ambos podrían ser eliminados en la al mismo tiempo.

• Tener copias de seguridad de refrigeración, enfriadores redundante o una portátil / acondicionador de aire de emergencia.

• Considere la posibilidad de colocar el segundo grupo de equipos redundantes en otra habitación, otro piso, o otro edificio.

• Tener un duplicado de instalación en otra parte de la ciudad o en otra ciudad. ¿Por qué comprar uno cuando se puede comprar dos por el doble del precio?

• He oído de alojamiento es barato en Marte, pero la latencia es asesino.

20.9. CARP con puente

CARP no es compatible con el puente en una capacidad nativa. Se requiere una gran cantidad de manuales intervención. Los detalles del proceso se pueden encontrar en Sección 9.5.2, "CARP".

20.10. CARP Solución de problemas

CARPA es una tecnología muy compleja, y con tantas maneras diferentes para configurar una conmutación por error clúster, puede ser difícil para que todo funcione correctamente. En esta sección, algunos comunes (y no tan común) los problemas se discuten y se espera resolver la mayoría de los casos. Si todavía tiene problemas después de leer esta sección, hay una dedicada CARP / VIP bordo en el pfSense Foro [http://forum.pfsense.org/index.php/board,] 36.0.html.

Antes de ir mucho más lejos, tómese el tiempo para revisar todos los miembros de la agrupación CARP para garantizar que que tienen configuraciones compatibles. A menudo, ayuda a caminar a través de la configuración de ejemplo, haga doble comprobar todos los ajustes correctos. Repita el proceso a los miembros copia de seguridad, y el reloj para los lugares donde la configuración deben ser diferentes en las copias de seguridad. Asegúrese de revisar la CARP estado (Sección 20.6.1, "Comprobar el estado CARP") Y garantizar la CARP está habilitado en todos los clúster miembros.

Los errores relativos a la carpa se registrará en estado → Registros del sistema, en la pestaña Sistema. Compruebe los registros en cada sistema implicados para ver si hay algún mensaje en relación con sincronización XMLRPC, CARP transiciones de estado, u otros errores.

20.10.1. Comunes errores de configuración

Hay tres errores de configuración muy común que suceda que impiden que la carpa de trabajo correctamente.

20.10.1.1. Use un VHID diferente en cada VIP CARP

Un VHID diferentes se debe utilizar en cada CARPA VIP que usted cree. Por desgracia, no siempre es así de simple. CARPA es una tecnología multicast, y como cualquier cosa con tal CARP en la misma segmento de red debe utilizar un VHID único. VRRP también utiliza un protocolo similar como la carpa, por lo que También debe asegurarse de que no entra en conflicto con VRRP VHIDs, como si su proveedor u otro enrutador de la red utiliza VRRP.

La mejor forma de evitar esto es utilizar un conjunto único de VHIDs. Si usted está en una conocida caja de seguridad red, inicie la numeración en 1. Si usted está en una red donde VRRP o CARP son contradictorios, puede que tenga que consultar con el administrador de esa red para encontrar un bloque libre de VHIDs.

20.10.1.2. Incorrecta Tiempos

Compruebe que todos los sistemas involucrados estén debidamente sincronizar sus relojes y tienen tiempo válido zonas, especialmente si se ejecuta en una máquina virtual. Si los relojes están muy alejadas, algunos tareas de sincronización, como conmutación por error de DHCP no funcionará correctamente.

20.10.1.3. Máscara de subred incorrecta

Debe utilizar la máscara de subred real de una CARPA VIP, no / 32. Debe coincidir con la máscara de subred para la dirección IP de la interfaz a la que el período de investigación CARP se le asigna.

20.10.1.4. Dirección IP para la interfaz CARP

La interfaz en la que el período de investigación CARP reside ya debe tener otra IP definida directamente en la interfaz (VLAN, LAN, WAN, TPO) antes de que pueda ser utilizado.

20.10.2. Incorrecta Hash Error

Hay algunas razones por qué este error puede aparecer en los registros del sistema, un poco más preocupante que otros.

Si CARP no funciona correctamente cuando se ve este error, podría deberse a una configuración falta de coincidencia. Asegúrese de que para un VIP, que la máscara de subred VHID, la contraseña y la dirección IP / todo el partido.

Si la configuración parece ser correcta y CARP sigue sin funcionar, mientras que la generación de este error mensaje, entonces puede haber varias instancias de CARP en el mismo dominio de broadcast. Es posible que necesidad de desactivar CARP y supervisar la red con tcpdump (Capítulo 25, Captura de paquetes) para comprobar si hay otras carpas o tráfico CARP-como, y ajustar su VHIDs adecuadamente.

Si CARP está funcionando correctamente, y aparece este mensaje cuando el sistema arranca, puede ser en cuenta. Es normal que este mensaje sea visto en el arranque, siempre y cuando CARP continúa para funcionar correctamente (MASTER muestra primaria, copia de seguridad muestra BACKUP para el estado).

20.10.3. Ambos sistemas aparecen como MASTER

Esto ocurrirá si la copia de seguridad no puede ver los anuncios CARP del maestro. Compruebe que reglas de firewall, problemas de conectividad, configuraciones de conmutación. También puedes ver los registros del sistema para cualquier errores relevantes que podrían conducir a una solución. Si usted está viendo esto en una máquina virtual (VM) Producto, tales como ESX, consulte Sección 20.10.5, "Problemas en el interior de máquinas virtuales (ESX)".

20.10.4. Sistema Maestro, pegado como RESERVA

En algunos casos, esto se puede suceder normalmente durante unos 5 minutos después de que un sistema vuelve a vida. Sin embargo, ciertas fallas de hardware o de otras condiciones de error puede hacer que un servidor en silencio asumir un advskew alta de 240 para señalar que todavía tiene un problema y no debe convertirse en maestro. Usted puede comprobar desde el shell o de diagnóstico → Comando.

#ifconfig carp0

```
carp0: banderas = 49 mtu <UP,LOOPBACK,RUNNING> 1500
 inet 10.0.66.10 máscara de red 0xffffff80
 carpas: BACKUP vhid un advbase un advskew 240
```

En ese caso, usted debe aislar ese servidor de seguridad y realizar pruebas de hardware adicional.

20.10.5. Problemas en el interior de máquinas virtuales (ESX)

Cuando se utiliza CARP interior de una máquina virtual, especialmente de VMware ESX, algunos especiales configuraciones son necesarias:

1. Activar el modo promiscuo en el conmutador virtual.

2. Habilitar "Los cambios de dirección MAC".

3. Habilitar "transmite forjado".

Además, hay un error en la funcionalidad de conmutador virtual de VMware, donde el tráfico de multidifusión se colocado de nuevo al sistema de envío en múltiples tarjetas de red físicos están conectados a un conmutador virtual. CARP no pasa por alto tráfico, ya que en una red que funciona normalmente que nunca suceder, y lo ve como otro host que afirma ser el maestro. Por lo tanto ambos servidores de seguridad siempre estar atascado en el modo de copia de seguridad. Hay algunos parches están probados para proporcionar una solución alternativa para

CARP en esta situación, y VMware ha sido notificado del fallo del conmutador virtual, por lo que no puede ser un
problema en el futuro.

20.10.6. Problemas de configuración de sincronización

Verifique los siguientes puntos cuando los problemas con la sincronización de la configuración se frente:

- El nombre de usuario debe ser el mismo en todos los nodos.
- La contraseña de la sincronización de la configuración en el maestro debe coincidir con la contraseña en la copia de seguridad.
- El WebGUI debe estar en el mismo puerto en todos los nodos.
- El WebGUI debe utilizar el mismo protocolo (HTTP o HTTPS) en todos los nodos.
- Usted debe permitir el tráfico al puerto WebGUI en la interfaz que está sincronizando con.
- La interfaz pfsync debe estar activado y configurado en todos los nodos.
- Eliminar todos los caracteres especiales de todo tipo que se están sincronizando: las reglas NAT, Las reglas de firewall, direcciones IP virtuales, etc ya no debería suponer un problema, pero si tiene dificultades, es una buena cosa para probar.
- Asegúrese de que sólo el nodo de sincronización principal tiene las opciones de sincronización habilitada.
- Asegúrese de que no hay una dirección IP se especifica en el Sincronizar a la propiedad intelectual en el nodo de copia de seguridad.

20.10.7. CARP y Solución de Problemas Multi-WAN

Si tiene problemas para llegar a la carpa de personalidades cuando se trata de Multi-WAN, doble control que tiene una norma como la que se menciona en Sección 20.5.3, "Configuración del Firewall"

20.10.8. Extracción de una CARPA VIP

Si una dirección IP CARP debe ser eliminado por cualquier motivo, el sistema de acogida debe ser reiniciado. Eliminación de una dirección IP CARP de un sistema vivo puede resultar en un kernel panic o la inestabilidad del sistema. versiones más recientes de pfSense advertirá de este hecho, y pedir confirmación de un reinicio cuando un CARP eliminación de VIP se intenta.

Capítulo 21. Servicios

La instalación base de pfSense viene junto con un conjunto de servicios que se suman algunos fundamentales funcionalidad y flexibilidad al sistema de firewall. Como su nombre lo indica, las opciones que se encuentran dentro de los servicios de control que el router proporcionará a los clientes, o en el caso de los servicios de enrutamiento, otros routers también. Estos servicios incluyen la prestación de direccionamiento DHCP, DNS y la resolución DNS dinámico, SNMP, UPnP y mucho más. Este capítulo comprende los servicios disponibles en el base del sistema. Hay muchos más servicios que se pueden agregar con los paquetes, que se más adelante en el libro.

21.1. Servidor DHCP

El servidor DHCP asigna direcciones IP y opciones de configuración relacionados a los PC cliente en su red. Es activado por defecto en la interfaz LAN, y con el defecto de la LAN IP 192.168.1.1, el rango de alcance predeterminado sería a través de 192.168.1.199 192.168.1.10. En su defecto configuración, pfSense asigna su IP LAN como la puerta de enlace y servidor DNS si el reenviador DNS está habilitado. Hay muchas opciones disponibles para ajustar en la WebGUI.

21.1.1. Configuración

Para modificar el comportamiento del servidor DHCP, vaya a Servicios → Servidor DHCP. Desde allí se puede alterar el comportamiento del servidor DHCP, junto con las asignaciones estáticas de IP y algunas opciones relacionadas como ARP estático.

21.1.1.1. La elección de una interfaz

En la página de configuración DHCP existe una ficha para cada interfaz no WAN. Cada interfaz tiene su propia configuración del servidor DHCP independiente, y pueden ser activadas o desactivadas de manera independiente el uno del otro. Antes de hacer cualquier cambio, asegúrese de que usted está buscando en la ficha de la derecha interfaz.

21.1.1.2. Opciones de servicio

El primer ajuste en cada ficha pfSense dice si o no para manejar peticiones DHCP en ese interfaz. Para habilitar el DHCP en la interfaz, visita el servidor DHCP en Active [nombre] interfaz caja. Para desactivar el servicio, desactive la caja misma.

Normalmente, el servidor DHCP responderá a las peticiones de cualquier cliente que solicite un contrato de arrendamiento. En mayoría de los entornos de este comportamiento es normal y aceptable, pero en más restringido o seguro

entornos de este comportamiento no es deseable. Con la opción Denegar clientes desconocidos conjunto, sólo clientes con asignaciones estáticas definidas recibirán contratos de arrendamiento, que es una práctica más segura, pero es mucho menos conveniente.

Nota

Esto protegerá contra los usuarios de bajo conocimiento y las personas que casualmente enchufe dispositivos. Tenga en cuenta, sin embargo, que un usuario con conocimientos de su red podría codificar una dirección IP, máscara de subred puerta de enlace, y DNS que aún les dará acceso. También podría alterar / parodia de su dirección MAC para que coincida con un cliente válido y aún obtener una concesión. Cuando sea posible pareja, con esta configuración de las entradas ARP estáticas, de control de acceso en un interruptor que limitará las direcciones MAC de los puertos de conmutación determinadas
para aumentar la seguridad y apagar o deshabilitar puertos interruptor que usted debe saber no estar en uso.

La dirección IP de la interfaz que se está configurando también se muestra, junto con su máscara de subred. Por debajo de esa línea de la gama disponible de direcciones IP para que la máscara de subred se imprime, que puede ayudar a determinar qué direcciones de inicio y finalización de usar para el rango de conjunto DHCP.

21.1.1.3. Rango de direcciones (DHCP Pool)

Las dos cajas de gama pfSense decirle lo que será la dirección y el apellido para su uso como un servidor DHCP piscina. La gama se debe introducir con el menor número primero, seguido por el número más alto. Por ejemplo, el valor por defecto de LAN rango DHCP se basa en la subred de la IP por defecto de LAN dirección. Sería **192.168.1.10** a **192.168.1.199**. Este rango puede ser tan grande o tan pequeño como sus necesidades de red, pero debe ser totalmente en el interior de la subred para la interfaz se está configurando.

21.1.1.4. Los servidores WINS

Dos servidores WINS (Windows Internet Name Service) se puede definir que se transmitirá a los clientes. Si usted tiene uno o varios servidores WINS disponible, introduzca las direcciones IP. La servidores reales no tienen que estar en esta subred, pero asegúrese de que el buen encaminamiento y cortafuegos las normas existen para hacerles llegar en los equipos cliente. Si esto se deja en blanco, no hay servidores WINS se envía al cliente.

21.1.1.5. Servidores DNS

Los servidores DNS pueden o no deben rellenarse, dependiendo de su configuración. Si está utilizando el Reenviador DNS integrado en pfSense para manejar DNS, deje estos campos en blanco y pfSense se automáticamente se asigna como el servidor DNS para los equipos cliente. Si el promotor de DNS está desactivado

y estos campos se dejan en blanco, pfSense pasará lo que los servidores DNS están asignados a en virtud del sistema → Configuración general. Si desea utilizar servidores DNS personalizado en lugar de la automática opciones, llene las direcciones IP de hasta dos servidores DNS aquí. (Véase Sección 24.2, "Contenido gratuito Filtrar con OpenDNS " para un ejemplo.) En las redes con servidores Windows, especialmente las empleo de Active Directory, se recomienda utilizar los servidores de DNS del cliente. Cuando se utiliza el reenviador DNS en combinación con la carpa, especifique el período de investigación CARP en esta interfaz aquí.

21.1.1.6. Gateway

La opción de puerta de enlace también se puede dejar en blanco si pfSense es la puerta de enlace para la red. En caso de que no sea el caso, escriba la dirección IP de la puerta de entrada a ser utilizado por clientes en esta interfaz. Cuando se utiliza CARP, complete el período de investigación CARP en esta interfaz aquí.

21.1.1.7. Tiempos de arrendamiento DHCP

El tiempo de permiso por defecto y el control de tiempo de concesión máximo el tiempo que un contrato de arrendamiento tendrá una duración de DHCP. La el tiempo de activación de arrendamiento se utiliza cuando un cliente no solicita un tiempo de expiración específica. Si el cliente se especifica el tiempo que quiere un contrato de arrendamiento a la última, el ajuste de tiempo de concesión máximo permiten limitar que a una cantidad razonable de tiempo. Estos valores se especifican en segundos, y los valores por defecto son 7200 segundos (2 horas) para el tiempo predeterminado, y 86.400 segundos (1 día) para el máximo tiempo.

21.1.1.8. Conmutación por error

Si este sistema es parte de una configuración de conmutación por error como un grupo CARP, entrar en el punto de conmutación por error de dirección IP siguiente. Esta debe ser la verdadera dirección IP del otro sistema en esta subred, no una compartida CARP dirección.

21.1.1.9. ARP estático

La casilla de verificación Habilitar la estática de las entradas ARP funciona de manera similar a negar desconocidos direcciones MAC desde la obtención de contratos de arrendamiento, pero da un paso más en la que también limitará los desconocidos máquina se comunique con el router pfSense. Esto dejaría a los posibles abusadores de codificar una dirección no utilizada en esta subred, eludir restricciones de DHCP.

Nota

Cuando se utiliza ARP estático, tenga cuidado para garantizar que todos los sistemas que necesitan

comunicarse con el router se enumeran en la lista de asignaciones estáticas antes de activar esta opción, sobre todo el sistema que se utiliza para conectarse a la pfSense WebGUI.

21.1.1.10. DNS dinámico

Para la configuración de DNS dinámico, haga clic en el botón Opciones avanzadas a la derecha de ese campo. Para habilitar esta
función, marque la casilla y luego rellenar un nombre de dominio para los nombres de host DHCP. Si está utilizando promotor de pfSense de DNS, puede en lugar de dejar esta opción en blanco y configurar el ajuste
dentro de la configuración de reenviador DNS.

21.1.1.11. Servidores NTP

Para especificar los servidores NTP (Network Time Server Protocol), haga clic en el botón Opciones avanzadas de la derecha
de ese campo, y escriba las direcciones IP de hasta dos servidores NTP.

21.1.1.12. Inicio en la red

Para ver la configuración de red Habilitar el arranque, haga clic en el botón Opciones avanzadas a la derecha de ese campo. A continuación, puede marcar la casilla para activar la función y, a continuación, escriba una dirección IP desde la que arrancar
imágenes están disponibles, y un nombre de archivo para la imagen de arranque. Ambos de estos campos debe estar configurado
para arranque en red para funcionar correctamente.

21.1.1.13. Guardar configuración

Después de realizar estos cambios, asegúrese de hacer clic en Guardar antes de intentar crear asignaciones estáticas.
Los ajustes se perderán si se navega fuera de esta página sin guardar primero.

21.1.1.14. Asignaciones estáticas

Estática asignaciones DHCP le permiten expresar su preferencia por que ser la dirección IP asignada
a un PC determinado, en función de su dirección MAC. En la red donde los clientes desconocidos se les niega, este también sirve como una lista de "conocidos" los clientes que están autorizados a recibir contratos de arrendamiento o estática ARP
las entradas. asignaciones estáticas se pueden añadir en una de dos maneras. En primer lugar, desde esta pantalla, haga clic y
se le presentará un formulario para agregar una asignación estática. El otro método consiste en agregar
desde el punto de vista de arrendamiento DHCP, que se expone más adelante en este capítulo.

De los cuatro campos de esta pantalla, sólo la dirección MAC es necesario. Al entrar sólo el MAC
dirección, se agregó a la lista de clientes conocidos para su uso cuando la opción Denegar clientes desconocidos se establece. Hay un enlace al lado del campo de la dirección MAC que se copia la dirección MAC de la PC
se utiliza para acceder a la WebGUI. Esto se proporciona para su conveniencia, en comparación con la obtención de la MAC
dirección en otra, más complicada, las formas.

Nota

La dirección MAC se puede obtener de un símbolo del sistema en la mayoría de las plataformas. En Basados en UNIX o UNIX-por igual trabajo, sistemas operativos, incluyendo Mac OS X, escribiendo "**ifconfig-a**"Mostrará la dirección MAC de cada interfaz. En Windows- las plataformas basadas en "**ipconfig / all**"Mostrará la dirección MAC. El MAC dirección también puede a veces encontrarse en una pegatina en la tarjeta de red, o cerca de la tarjeta de red para los adaptadores integrados. Para los hosts en la misma subred, el MAC se puede determinar haciendo ping a la dirección IP de la máquina y luego ejecutar **"Arp -A "**.

El campo de dirección IP es necesaria si esta será una asignación de IP estática en lugar de sólo informar a la servidor DHCP que el cliente es válido. Esta dirección IP es realmente una preferencia, y no una reserva. Asignación de una dirección IP aquí no evitará que otra persona utilizando la misma dirección IP. Si esta dirección IP está en uso cuando este cliente solicita un contrato de arrendamiento, en lugar recibirá una de la piscina en general. Por esta razón, el pfSense WebGUI no le permite asignar direcciones IP estáticas asignaciones en el interior de su piscina DHCP.

Un nombre de host también se puede establecer, y no tiene que coincidir con el nombre real establecido en el cliente. El nombre de host configurado aquí se utilizarán durante el registro de direcciones de DHCP en el promotor de DNS.

La descripción es cosmético, y su disposición para ayudar a rastrear toda la información adicional acerca de esta entrada. Podría ser el nombre de la persona que utiliza el PC, su función, la razón necesitaba una dirección estática, o el administrador que ha agregado la entrada. También puede dejarse en blanco.

Haga clic en Guardar para terminar de editar la asignación estática y volver a la página de configuración del servidor DHCP.

21.1.2. Condición Jurídica y Social

Se encuentra el estado del servicio de servidor DHCP en Estado → Servicios. Si está habilitada, su estado se debe tal como se ejecuta, como en Figura 21.1, "demonio DHCP Estado del servicio". La botones en el lado derecho le permiten reiniciar o detener el servicio de servidor DHCP. El reinicio debe no será necesario que pfSense se reiniciará automáticamente el servicio cuando los cambios de configuración se realizan que requieren un reinicio. Detener el servicio también es probable que nunca sea necesario, como el servicio se detiene cuando se desactiva todas las instancias del servidor DHCP.

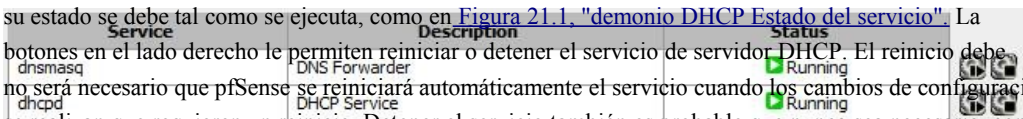


Figura 21.1. Demonio del servicio DHCP Estado

21.1.3. Arrendamientos

Puede ver los actuales contratos asignados a Diagnóstico → DHCP concede. Esta pantalla muestra la dirección IP asignada, la dirección MAC se asigna a, el nombre de host (si los hay) que el cliente enviado como parte de la solicitud de DHCP, el inicio y el final del contrato de arrendamiento, si la máquina está actualmente en línea, y si el contrato está activo, ha caducado, o un registro estático.

21.1.3.1. Ver inactivos arrendamientos

De forma predeterminada, sólo concesiones activas y estáticas se muestran, pero usted puede ver todo, incluyendo el contrato de arrendamiento expire, haciendo clic en el botón Mostrar todos los contratos de arrendamiento configurado. Para reducir la vista de nuevo a
normales, haga clic en el Salón de concesiones activas y estáticas sólo botón.

21.1.3.2. Wake on LAN Integración

Si hace clic en la dirección MAC, o el Wake on LAN botón a la derecha del contrato de arrendamiento, pfSense enviará un Wake on LAN paquete a ese host. Para obtener más detalles acerca de Wake on LAN, consulte
Sección 21.8, "Wake on LAN".

21.1.3.3. Agregar asignación estática

Para hacer un contrato de arrendamiento dinámico en una asignación estática, haga clic en el de la derecha del contrato de arrendamiento. Esto
antes de llenar la dirección MAC de esa máquina en el "Editar asignación estática" de pantalla. Usted tendrá que añadir la deseada dirección IP, nombre de host y la descripción y haga clic en **Guardar**. Cualquier contratos en vigor de este dirección MAC se borrará de los contratos de arrendamiento de archivo al guardar la nueva entrada.

21.1.3.4. Eliminar un contrato de arrendamiento

Al tiempo que visualiza los contratos de arrendamiento, es posible eliminar inactivos o contrato de arrendamiento expiró manualmente haciendo clic en el
botón en la parte final de una línea. Esta opción no está disponible para las concesiones activas o estático, sólo para
fuera de línea o contrato de arrendamiento expire.

21.1.4. Servicio DHCP Registros

El demonio DHCP registro de su actividad al Estado → Registros del sistema, en la pestaña DHCP. Cada DHCP solicitud y la respuesta se mostrará, junto con cualquier otra condición social y mensajes de error.

21.2. De retransmisión DHCP

peticiones DHCP tráfico de difusión. El tráfico de difusión se limita al dominio de difusión donde se se inicia. Si es necesario proporcionar el servicio DHCP en un segmento de red sin un servidor DHCP, utiliza DHCP Relay para reenviar las solicitudes a un servidor definido en otro segmento. No es posible ejecutar tanto un servidor DHCP y un relé de DHCP en el mismo tiempo. Para habilitar el DHCP relé primero debe desactivar el servidor DHCP en cada interfaz.

Una vez que el servidor DHCP está desactivado, visite Servicios → Relé DHCP. Al igual que con el servidor DHCP, hay una ficha para cada interfaz. Haga clic en la interfaz en la que desea ejecutar el repetidor de DHCP, a continuación, marque la casilla junto a Activar DHCP en la interfaz de relé [nombre], que también le permitirá establecer las otras opciones disponibles.

Si marca ID Anexar circuito y la identificación del agente a las solicitudes, el relé de DHCP se anexará el circuito ID (número de interfaz pfSense) y la identificación del agente a la solicitud de DHCP. Esto puede ser necesario por el servidor DHCP en el otro lado, o puede ayudar a distinguir cuando las solicitudes se originó.

La opción de proxy peticiones al servidor DHCP en WAN subred se limita a lo que dice. Si se activa, pasará las peticiones de los clientes DHCP en esta interfaz con el servidor DHCP que asigna el Dirección IP a la interfaz WAN. Alternativamente, usted puede llenar en la dirección IP del servidor DHCP a los que las solicitudes deben ser proxy.

21.3. DNS Forwarder

El reenviador DNS en pfSense es una resolución de caché DNS. Es activado por defecto, y utiliza los servidores DNS configurados en el sistema → Configuración general, o los que se obtienen de su ISP para configurar dinámicamente interfaces WAN (DHCP, PPPoE y PPTP). Para estática IP WAN conexiones, debe entrar en los servidores DNS en el sistema → General de instalación o durante la instalación asistente para el redireccionador de DNS para la función. También puede utilizar los servidores DNS configurados estáticamente
con configurado dinámicamente interfaces WAN, desmarcando la opción "Permitir la lista del servidor DNS que se se reemplaza por DHCP / PPP WAN "caja en el Sistema → Página general de la instalación.

En versiones anteriores, pfSense inicialmente trató el primer servidor DNS configurado cuando se trata de resolver un nombre DNS, y se trasladó posteriormente a configurar los servidores DNS si el fracaso de la primera de resolver. Esto podría causar grandes retrasos si uno o más de los disponibles los servidores DNS inalcanzable. En pfSense 1.2.3 y finales de este comportamiento se ha cambiado para consultar todos los servidores DNS a la vez, y el único de la primera respuesta recibida se utiliza y se almacena en caché. Esto da lugar a mucho más rápido servicio de DNS, y puede ayudar a suavizar los problemas que se derivan de los servidores DNS que están intermitente lenta o alta latencia.

21.3.1. Configuración de DNS Forwarder

La configuración de reenviador DNS se encuentra en Servicios → Reenviador DNS.

21.3.1.1. Habilitar DNS Forwarder

Al marcar esta casilla se convierte en el promotor de DNS o desactivar si se desea desactivar esta funcionalidad.

21.3.1.2. Registro de contratos de arrendamiento DHCP en DNS reenviador

Si quieres que tu nombres internos de la máquina para los clientes DHCP para resolver en absoluto, marque esta casilla. Esto sólo funciona para las máquinas que especifican un nombre de host en sus peticiones DHCP.

21.3.1.3. Registro de las asignaciones DHCP estática en DNS reenviador

Esto funciona igual que los contratos de arrendamiento DHCP en la opción Crear forwarder DNS, salvo que registros de las direcciones DHCP de asignación estática.

21.3.1.4. Anfitrión Invalida

La primera sección en la parte inferior de la pantalla reenviador DNS es donde puede especificar anula para la resolución de nombres DNS de acogida. Aquí usted puede configurar un nombre de host específicos para resolver de manera diferente
que de otra manera sería a través de los servidores DNS utilizados por el promotor de DNS. Esto es útil para dividir Configuraciones de DNS (ver Sección 7.5.2, "Split DNS"), y como un medio semi-efectiva de bloqueo el acceso a determinados sitios web específicos.

Figura 21.2, "DNS Reemplazar Ejemplo" ilustra un DNS aumento al presupuesto para una red interna servidor (example.com y www.example.com), así como un ejemplo de bloquear el acceso a myspace.com y www.myspace.com.

Host	Domain	IP	Description
	example.com	192.168.1.100	www override
	myspace.com	127.0.0.1	hack block
www	myspace.com	127.0.0.1	hack block
www	example.com	192.168.1.100	www override

Figura 21.2. DNS Ejemplo Reemplazar

Nota

No se recomienda para uso estrictamente reemplazar la funcionalidad de DNS como un medio de bloquear el acceso a determinados sitios. Hay innumerables maneras de evitar esto. Es será evitar que los usuarios no técnicos, pero es muy fácil de recorrer para los que tienen más aptitud técnica.

21.3.1.5. Reemplaza dominio

anulaciones de dominio se encuentran en la parte inferior de la pantalla DNS reenviador. Esto le permite especificar un servidor DNS diferente a utilizar para resolver un dominio específico.

Un ejemplo de esto es donde comúnmente se desplegó en las redes de pequeñas empresas con un solo servidor interno con Active Directory, por lo general de Microsoft Small Business Server. El DNS las solicitudes de nombres de dominio de Active Directory debe ser resuelto por el interior de Windows Server para Active Directory para funcionar correctamente. Adición de un reemplazo para el dominio de Active Directory apuntando a la dirección IP del servidor interno de Windows asegura que estos registros se resuelven adecuadamente si los clientes están utilizando pfSense como un servidor DNS o el servidor de Windows en sí.
En un entorno de Active Directory, los sistemas siempre deben utilizar su servidor DNS de Windows como su servidor DNS principal para las funciones dinámicas de registro de nombres correctamente. En los entornos con un solo servidor DNS de Windows, usted debe permitir que el promotor de DNS con un reemplazo para su dominio de Active Directory y pfSense utilizar como servidor DNS secundario para el interior máquinas. Esto asegura la resolución de DNS (a excepción de Active Directory) no tiene una sola punto de falla, y la pérdida del único servidor no significará una interrupción completa de Internet. La pérdida de un solo servidor en un entorno por lo general tienen consecuencias importantes, pero los usuarios será más probable que te deje en paz para solucionar el problema si es que aún puede consultar su lolcats, MySpace, Facebook, y otros en la media hora.
Otro uso común de anulaciones DNS para resolver los dominios DNS interno en sitios remotos utilizando un servidor DNS en el sitio principal de acceso a través de VPN. En tales ambientes normalmente se desea para resolver todas las consultas DNS en el sitio central para el control centralizado sobre DNS, sin embargo, algunos organizaciones prefieren dejar DNS de Internet se resuelven con pfSense en cada sitio, y el reenvío sólo consultas para los dominios internos de la central de servidor DNS. Tenga en cuenta que necesitará una ruta estática para esta función a través de IPsec. Ver Sección 13.4.4, "pfSense-inició tráfico e IPsec" para más de la información.

21.4. DNS dinámico

El cliente de DNS dinámico en pfSense le permite registrar la dirección IP de su interfaz WAN con una variedad de proveedores de servicios de DNS dinámico. Esto es útil cuando se desea de forma remota

conexiones de acceso IP dinámica, más comúnmente utilizado para conectarse a una VPN, servidor web, o por correo
servidor.

Nota

Esto sólo funciona en su interfaz WAN primario. Las interfaces no pueden OPT
utilizar el construido en el cliente DNS dinámico. También puede registrarse sólo una dinámica
De nombres DNS. pfSense 2.0 admite como diferentes servicios de DNS dinámico a medida que
deseo, permite el registro del territorio palestino ocupado WAN IP, y permite el registro de su
IP real del público en ambientes donde pfSense recibe una IP privada de la WAN y
NAT es ascendente.

21.4.1. Uso de DNS dinámico

pfSense permite el registro con nueve diferentes proveedores de DNS dinámico de la versión 1.2.3. Usted
puede ver los proveedores disponibles haciendo clic en el desplegable Tipo de servicio desplegable. Usted puede encontrar
Más información sobre los proveedores mediante la búsqueda de su nombre para encontrar su sitio web. La mayoría ofrece una base
nivel de servicio sin costo alguno, y algunos ofrecen servicios adicionales de alta calidad a un coste.
Una vez que usted decida sobre un proveedor, visite su sitio web, inscribirse para una cuenta y configurar un nombre de host.
Los procedimientos de este varían para cada proveedor, pero no tienen instrucciones de sus sitios web. Después de
configurar el nombre de host con el proveedor, a continuación, configurar pfSense con los ajustes.

21.4.1.1. Tipo de Servicio

Seleccione su proveedor de DNS dinámico aquí.

21.4.1.2. Nombre de la máquina

Introduzca el nombre que ha creado con su proveedor de DNS dinámico.

21.4.1.3. MX

Un registro MX (Mail Exchanger) registro es el número de servidores de correo de Internet para saber dónde entregar el correo para
su dominio. Algunos proveedores de DNS dinámico le permitirá configurar el DNS dinámico a través de su
cliente. Si el suyo no, escriba el nombre de host del servidor de correo que reciben correo electrónico de Internet para
su dominio DNS dinámico.

21.4.1.4. Los comodines

Habilitación de DNS comodín en el nombre de DNS dinámico significa que todos los nombre de host consultas
se resolverá a la dirección IP de su nombre de host DNS dinámico. Por ejemplo, si

el nombre de host es example.dyndns.org, lo que permite comodín hará *. example.dyndns.org (A.example.dyndns.org, b.example.dyndns.org, etc) resolver el mismo example.dyndns.org.

21.4.1.5. Nombre de Usuario y Contraseña

Aquí es donde puede entrar el nombre de usuario y la contraseña de su proveedor de DNS dinámico.

21.4.2. RFC 2136 DNS dinámico actualizaciones

El RFC 2136 DNS dinámico funcionalidad de actualizaciones que permite registrar un nombre de host en cualquier Servidor DNS apoyo RFC 2136 actualizaciones. Esto se puede utilizar para actualizar los nombres de host en BIND y Windows Server servidores DNS, entre otros.

Esto puede funcionar simultáneamente con uno de los discutidos previamente servicio de DNS dinámico proveedores, sin embargo también está limitado a una configuración única y sólo se registrará la IP WAN, no los de las interfaces WAN OPT.

21.5. SNMP

La Red de Protocolo simple de administración [Http://en.wikipedia.org/wiki/Snmp] (SNMP) demonio le permitirá controlar de forma remota algunos parámetros del sistema pfSense. En función de la opciones elegidas, se puede monitorear el tráfico de red, los flujos de la red, las colas de PF, y el sistema general información, tales como CPU, memoria y uso del disco. La implementación de SNMP utilizada por pfSense es bsnmpd, que por defecto sólo tiene las bases de gestión más básicos de la información (MIB) disponibles, y se extiende por los módulos cargables.[1] Además de que el demonio SNMP, también puede enviar capturas a un servidor SNMP para ciertos eventos. Estos varían en función de los módulos cargados. Por ejemplo, la red de cambios de estado de vínculos generará una trampa si tiene el módulo MIB II cargado.
El servicio SNMP se puede configurar por la navegación a los servicios → SNMP.
La forma más fácil de ver lo que se dispone de datos sería ejecutar snmpwalk contra el pfSense sistema desde otro host con Net-SNMP o un equivalente instalado. El contenido íntegro de la MIB disponibles están fuera del alcance de este libro, pero hay un montón de recursos impresos y en línea para SNMP, y algunos de los árboles MIB están cubiertos en el RFC. Por ejemplo, el anfitrión de Recursos MIB se define en el RFC 2790.

21.5.1. SNMP demonio

Estas opciones determinan si, y cómo, el demonio SNMP se ejecutará. Para activar el demonio SNMP, de verificación Habilitar. Una vez Habilitar se ha comprobado, a continuación, las otras opciones se pueden cambiar.

[1] http://people.freebsd.org/ ~ harti / bsnmp /

21.5.1.1. Puerto de votación

conexiones SNMP son UDP, SNMP y por defecto a los clientes a través del puerto UDP 161. Este ajuste hará que el demonio para que escuche en un puerto diferente, y debe su cliente o el agente SNMP de votación cambiarse para adaptarse.

21.5.1.2. Sistema de localización

Este campo de texto especifica qué cadena se devuelve cuando la ubicación del sistema se consulta a través de SNMP. Usted puede seguir cualquier convención es necesaria para su organización. Para algunos dispositivos una ciudad o estado puede estar lo suficientemente cerca, mientras que otros pueden necesitar los detalles más específicos, como la que rack y posición en la que reside el sistema.

21.5.1.3. Sistema de contacto

El contacto del sistema es también un campo de texto que se pueden establecer sin embargo, requieren sus necesidades.

Podría ser un nombre, una dirección de correo electrónico, un número de teléfono, o lo que sea necesario.

21.5.1.4. Leer cadena de la Comunidad

Con SNMP, la cadena de comunidad actúa como una especie de nombre de usuario y contraseña en una. SNMP los clientes tendrán que utilizar esta cadena de comunidad cuando el sondeo. El valor predeterminado de "público" es común, por lo que debería pensar en cambiar a otra cosa, además de restringir el acceso con el servicio SNMP con las reglas del cortafuegos.

21.5.2. SNMP Traps

Encomendar al demonio SNMP para enviar capturas SNMP, marque Activar. Una vez que ha sido Habilitar marcada, las otras opciones a continuación, se puede cambiar.

21.5.2.1. Trampa de servidor

El servidor trampa es el nombre de host o dirección IP para que las trampas SNMP debe ser reenviado.

21.5.2.2. Trampa de puerto del servidor

De forma predeterminada, las trampas SNMP se establecen en el puerto UDP 162. Si el receptor de captura SNMP se establece un trato diferente puerto, modifica este ajuste para equiparar.

21.5.2.3. SNMP cadena trampa

Esta cadena se enviará junto con cualquier trampa SNMP que se genera.

21.5.3. Módulos

Los módulos cargables disponible aquí permitir que el demonio SNMP para entender y responder a las consultas de información del sistema más. Cada módulo de carga se consumen más recursos. Por lo tanto, garantizar que sólo los módulos que se utilizarán realmente se cargan.

21.5.3.1. MIBII

Este módulo proporciona información especificada en la norma árbol MIB II, que abarca redes de información e interfaces. Después de haber cargado este módulo será, entre otras cosas, le permite consultar información de interfaz de red incluyendo el estado, el hardware y las direcciones IP, el cantidad de datos transmitidos y recibidos, y mucho más.

21.5.3.2. Netgraph

El módulo NetGraph proporciona información NetGraph-relacionados, tales como nombres de nodo NetGraph y los estados, los compañeros de gancho, y los errores.

21.5.3.3. PF

El módulo de FP da acceso a una gran cantidad de información sobre fondos de pensiones. El árbol MIB cubre los aspectos de la
el conjunto de reglas, los estados, las interfaces, tablas y altq colas.

21.5.3.4. Recursos de acogida

Este módulo cubre la información sobre el propio anfitrión, incluida la carga promedio el tiempo de actividad, y procesos, tipos de almacenamiento y uso, los dispositivos conectados del sistema, e incluso instalar software.

21.5.4. Se unen a la interfaz LAN sólo

Esta opción hará que el demonio SNMP escuchar en la interfaz LAN solamente. Esto facilita la comunicaciones a través de túneles VPN IPsec, ya que elimina la necesidad de la ya mencionada ruta estática, sino que también ayuda a proporcionar una seguridad adicional al reducir la exposición del servicio de otras interfaces.

21.6. UPnP

Universal Plug and Play [http://en.wikipedia.org/wiki/Upnp] (UPnP) es un servicio de red que permite que el software y los dispositivos a configurar uno al otro al conectar a una red. Esto incluye

la creación de sus delanteros propios puertos NAT y las normas de firewall. El servicio de UPnP en pfSense, que se encuentra en Servicios → UPnP, permitirá a los equipos cliente y otros dispositivos tales como un juego consolas para permitir de forma automática el tráfico necesarios para llegar a ellos. Hay muchos programas populares y los sistemas que soportan UPnP, como Skype, uTorrent, mIRC, clientes de mensajería instantánea, PlayStation 3, y Xbox 360.

UPnP utiliza el Simple Service Discovery Protocol (SSDP) para la detección de redes, que utiliza el puerto UDP 1900. El demonio UPnP utilizado por pfSense, miniupnpd, también utiliza el puerto TCP 2189. Puede que tenga que permitir el acceso a estos servicios con las reglas del cortafuegos, especialmente si usted tiene eliminado de la LAN por defecto a cualquier norma, o en configuraciones de puente.

21.6.1. Las preocupaciones de seguridad

El servicio de UPnP es un ejemplo clásico de la "Seguridad vs Conveniencia" trade-off. UPnP, por su propia naturaleza, es inseguro. Cualquier programa en la red podría permitir en adelante y todo el tráfico - una pesadilla para la seguridad. Por otro lado, puede ser una tarea que introducir y mantener puertos NAT hacia delante y sus normas correspondientes, especialmente cuando se trata de consolas de juegos. Hay una gran cantidad de conjeturas y de investigación involucrados para encontrar el adecuado y la configuración de puertos, pero sólo funciona con UPnP y requiere poco esfuerzo administrativo. adelante Manual de puerto para dar cabida a estas situaciones tienden ser demasiado permisiva, lo que podría exponer a los servicios que no deben estar abiertos a través de Internet. Los delanteros del puerto son también siempre, en UPnP puede ser temporal. Hay controles de acceso en la configuración del servicio UPnP, lo que ayudará a bloquear quién y qué se le permite hacer modificaciones. Más allá de los controles integrados de acceso, además puede controlar el acceso con reglas de firewall. Cuando está bien controlada, UPnP también puede ser un poco más de seguridad al permitir que los programas para recoger y escuchar en los puertos al azar, en lugar de siempre tener el mismo puerto abierto y reenviado.

21.6.2. Configuración

El servicio UPnP se configura por la navegación a los servicios → UPnP. Habilitar el servicio marcando la casilla Enable UPnP. Cuando haya terminado de realizar los cambios necesarios, que son se describe en el resto de esta sección, haga clic en Guardar. El servicio UPnP continuación, se iniciará automáticamente.

21.6.2.1. Interfaces

Esta configuración le permite elegir las interfaces en los que UPnP es permitido escuchar. Más de una interfaz puede ser elegido presionando Ctrl mientras haces clic en las interfaces adicionales. Anulación de la selección de una interfaz funciona del mismo modo, mantenga pulsado Ctrl mientras haces clic en para eliminar la selección.

Si una interfaz se tiende un puente a otro, UPnP sólo debe ser seleccionado en el "padre" de interfaz, no el que se tiende un puente. Por ejemplo, si usted tiene OPT1 puente de LAN, sólo habilitar UPnP de la LAN.

21.6.2.2. Velocidad máxima

Desde la versión 1.2.3 pfSense, ahora puede establecer la descarga y velocidades de carga máxima para los puertos abiertos por UPnP. Estas velocidades se establecen en Kilobits por segundo, por lo que para limitar la descarga a 1,5 Mbit / s, que se introduzca **1536** en el campo de velocidad máxima de descarga.

21.6.2.3. Reemplazar dirección WAN

De forma predeterminada, el servicio UPnP se puede configurar mas adelante el puerto y las reglas del cortafuegos a la dirección de la WAN.

Esta configuración le permite ingresar una dirección IP alternativa, como una dirección secundaria WAN o una compartir la dirección del CARP.

21.6.2.4. Traffic Shaping cola

De forma predeterminada, las reglas creadas por UPnP no asignará el tráfico en una cola de formador. Al participar en el nombre de una cola en este campo, el tráfico que pasa por una regla creada con UPnP entrarán en esta cola. Seleccione la cola de prudencia, ya que cualquier dispositivo con UPnP habilitado o programa utilizará esta cola. Es podría ser Bittorrent, o podría ser una consola de juegos, así que elige una cola que tiene una prioridad que se ajuste a con el mejor el tráfico que espera a ser más común.

21.6.2.5. Registro de paquetes

Cuando esta casilla está marcada, los delanteros puerto generados por UPnP se establecerá en registro, de modo que cada conexión realizada tendrá una entrada en los registros del cortafuegos, que se encuentra en estado de → Registros del sistema, en en la pestaña Firewall.

21.6.2.6. Utilice el tiempo de actividad del sistema

De forma predeterminada, el demonio UPnP los informes del servicio de tiempo de actividad cuando se les pregunta en lugar del sistema el tiempo de actividad. Al activar esta opción hará que el informe del tiempo de funcionamiento real del sistema en su lugar.

21.6.2.7. Denegar por defecto

Si el incumplimiento por negar el acceso a la opción UPnP está activado, UPnP sólo permitirá el acceso a clientes que coincidan con las reglas de acceso. Este es un método más seguro de controlar el servicio, pero como se mencionó anteriormente, también es menos conveniente.

21.6.2.8. UPnP permisos de usuario

Hay cuatro campos para especificar las reglas de acceso definidas por el usuario. Si el defecto es negar la opción elegido, debe establecer reglas para permitir el acceso. Las reglas son formuladas con el siguiente formato:

port|port <allow|deny> <external range)> IP|IP/CIDR> <internal range)> <internal port|port

21.6.2.8.1. El permiso de usuario UPnP Ejemplo 1

Negar el acceso al puerto 80 de reenvío de todo en la LAN, 192.168.1.1, con un / 24 de subred.

negar 192.168.1.1/24 80 80

21.6.2.8.2. El permiso de usuario UPnP Ejemplo 2

Permitir 192.168.1.10 que transmita cualquier puerto sin privilegios.

permiten 1024-65535 192.168.1.10 1024 hasta 65.535

21.6.3. Condición Jurídica y Social

El estado del servicio UPnP sí mismo puede ser visto en estado de → Servicios. Esto mostrará si el servicio se está ejecutando o se detiene, y le permiten detener, iniciar o reiniciar el servicio. Esto debería ser todos los de manera automática, pero se puede controlar manualmente si es necesario. Una lista de la actualidad enviado puertos y clientes como la de Figura 21.3, "la pantalla que muestra el estado UPnP PC cliente con remitió los puertos " se puede ver en Estado → UPnP.

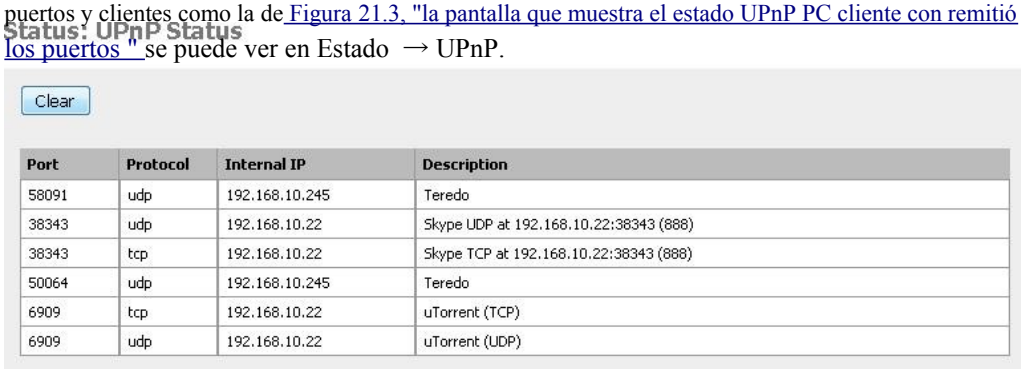


Figura 21.3. UPnP pantalla de estado que muestra los equipos cliente con los puertos remitió

Cuando el servicio se está ejecutando también debe aparecer al explorar la red con un UPnP conscientes del sistema operativo como Windows 7 o Windows Vista, como lo demuestra Figura 21.4, "pfSense sistema como se ve por Windows 7 cuando se navega por "Network. Puede hacer clic en los router icono y haga clic en Ver página web del dispositivo para abrir la WebGUI en su navegador por defecto. Si hace clic derecho en el router y haga clic en Propiedades, también mostrará la versión de pfSense y la propiedad intelectual la dirección del router.

Figura 21.4. sistema de pfSense como se ve por Windows 7 en su navegación por la Red

21.6.4. Solución de problemas

La mayoría de los problemas con UPnP tienden a involucrar puente. En este caso, es importante que usted tenga

específicas

las reglas del firewall para permitir UPnP en el puerto UDP 1900. Puesto que es el tráfico de multidifusión, el destino debe ser la dirección de broadcast de la subred, o en algunos casos haciendo **cualquier** será necesario. Consulte a su servidor de seguridad en los registros de estado → Registros del sistema, en la ficha servidor de seguridad, para ver si el tráfico está siendo
bloqueado. Preste especial atención a la dirección de destino, ya que puede ser diferente de lo esperado.

Más problemas con las consolas de juegos también pueden ser aliviados por la conmutación de salida manual NAT y permitir puerto estático. Ver Sección 7.6.2, "puerto estático" para más detalles.

21.7. OpenNTPD

La OpenNTPD [http://www.openntpd.org/servicio] es un Protocolo de red Tiempo [http://en.wikipedia.org / wiki / Network_Time_Protocol] (NTP) demonio que escuchará las peticiones de los clientes y les permitirá sincronizar su reloj con el del sistema de pfSense. Por ejecutando un servidor local de NTP y usarlo para sus clientes, reduce la carga en la parte inferior del estrato servidores y puede asegurar que sus sistemas siempre se puede llegar a un servidor de hora. Antes de delegar esta tarea a su sistema de pfSense, es una buena práctica para asegurarse de que tiene un reloj preciso y mantiene la hora razonable.

No hay mucho para configurar el servidor OpenNTPD, disponible en Servicios → OpenNTPD. Marque la casilla Permitir, selección de interfaces que se debe escuchar a, y haga clic en Guardar. Más de una interfaz puede ser elegido presionando Ctrl mientras haces clic en las interfaces adicionales. Anulación de la selección de una interfaz funciona del mismo modo, mantenga pulsado Ctrl mientras haces clic en para eliminar la selección.
El servicio se iniciará de inmediato, sin embargo, habrá un retraso de varios minutos antes de que dará servicio a las peticiones NTP, ya que el servicio se asegura de su tiempo es correcta antes de responder a las solicitudes.

OpenNTPD registros se mantienen en estado de → Registros del sistema, en la ficha OpenNTPD. OpenNTPD ha muy poco de registro, a menos que haya un problema del servicio no generará ninguna de las entradas de registro.

21.8. Wake on LAN

La Wake on LAN [Http://en.wikipedia.org/wiki/Wake_on_lan] (WOL) en la página de Servicios → Wake on LAN se puede utilizar para despertar los ordenadores de un estado de apagado mediante el envío de especial "Los paquetes Magia". La NIC en el equipo que se va a despertar debe ser compatible con WOL y tiene que estar configurado correctamente. Normalmente hay una configuración del BIOS para permitir WOL, y no adaptadores integrados probable es que necesitan un cable WOL conectado entre el NIC y un encabezado de WOL en la placa base.

WOL tiene muchos usos potenciales. Por lo general, estaciones de trabajo y los servidores se mantienen funcionando a causa de
servicios que prestan, los archivos o impresoras que comparten, o por conveniencia. Uso de WOL permitiría estos a permanecer apagado, y ahorrar energía. Si un servicio se requiere, el sistema puede ser despertado cuando sea necesario. Otro ejemplo sería si alguien tiene acceso remoto a un sistema, pero el usuario la apague. Uso de WOL la máquina puede ser despertado, y puede ser a continuación, acceder una vez que ha arrancado.

WOL no ofrece seguridad inherente. Cualquier sistema en la misma capa 2 de la red puede transmitir un WOL paquete, y el paquete será aceptado y obedecido. Lo mejor es configurar sólo WOL en el BIOS para las máquinas que lo necesitan, y desactivarlo en todos los demás. Hay un par de proveedores específicos WOL extensiones que proporcionan una cierta seguridad extra, pero no universalmente compatibles.

21.8.1. Despierta una sola máquina

Para despertar una sola máquina, seleccione la interfaz a través del cual se puede llegar, y entrar en el sistema de dirección MAC en el formato de *xx: xx: xx: xx: xx: xx*. Al hacer clic en Enviar, pfSense transmitirá un Magic Packet WOL a la interfaz elegida, y si todo ha ido como previsto, el sistema debe despertar. Tenga en cuenta que los sistemas tomará algún tiempo para arrancar. Es puede ser de varios minutos antes de que el sistema de destino está disponible.

21.8.2. Almacenamiento de direcciones MAC

Para almacenar una dirección MAC para la conveniencia después, haga clic en el en la lista de almacenar las direcciones MAC,
y podrás ver una pantalla de edición en blanco. Escoja la interfaz a través del cual se puede llegar, y
introducir la dirección del sistema MAC en el formato de *xx: xx: xx: xx: xx: xx*. Una descripción puede
También se consignará para su posterior consulta, por ejemplo, "Pat PC" o "Sue servidor". Haga clic en Guardar cuando
terminado y que será devuelto a la página principal de WOL y la nueva entrada debe ser visible
en la lista en la parte inferior de la página.

El mantenimiento de las entradas es similar a otras tareas en pfSense: Haga clic para editar una entrada existente,
y haga clic para quitar una entrada.

21.8.3. Despierta una sola máquina almacenados

Para enviar un Magic Packet WOL a un sistema que ha sido previamente almacenados, haga clic en su dirección MAC
en la lista de los sistemas de almacenado. La dirección MAC se destacó como un enlace. Usted será llevado
volver a la página WOL, con el interfaz del sistema y la dirección MAC precargada en el formulario. Haga clic en
Enviar y el Magic Packet será enviado.

21.8.4. Despierta Todos los equipos almacenados

En la página WOL, hay un botón que se puede utilizar para enviar un Magic Packet WOL a todos
sistemas de almacenado. Haga clic en el botón y las solicitudes se enviarán, sin otra intervención necesaria.

21.8.5. Reactivación desde DHCP Arrendamientos Ver

Para enviar un WOL Magic Packet desde el punto de vista DHCP Arrendamientos en diagnósticos → DHCP arrendamientos,
haga clic en su dirección MAC en la lista de contratos de arrendamiento, que debe ser destacado como un enlace. El vínculo WOL
sólo estará activa para los sistemas cuyo estado se muestra como "en línea". Usted será llevado de nuevo a
la página de activación por LAN, con el interfaz del sistema y la dirección MAC precargada en el formulario. Haga clic en Enviar
y el Paquete Magia será enviado.

21.8.6. Guardar en DHCP Arrendamientos Ver

Usted puede copiar una dirección MAC a una entrada de asignación de nuevas WOL mientras ve los contratos de
arrendamiento DHCP en

21.9. Servidor PPPoE

pfSense puede actuar como un servidor PPPoE y aceptar / autenticar las conexiones de los clientes PPPoE en un interfaz local, actuando como un concentrador de acceso. Esto puede ser usado para forzar a los usuarios autenticarse antes de obtener acceso a la red, o para controlar su comportamiento de inicio de sesión. Esta se encuentra bajo Servicios → Servidor PPPoE. Usted encontrará que esta configuración es muy similar a la VPN PPTP servidor (Capítulo 14, PPTP VPN).

Para activar esta función, primero debe seleccionar Habilitar servidor PPPoE. A continuación, seleccione la interfaz que en que para ofrecer este servicio. Ajuste la máscara de subred que debe asignarse a los clientes PPPoE y el número de usuarios PPPoE permitir. A continuación, introduzca la dirección del servidor que es la dirección IP que el sistema de pfSense enviará a los clientes PPPoE para usar como puerta de entrada. Introduzca una dirección IP dirección en el cuadro Dirección remota área de distribución y que se utilizará junto con la máscara de subred definido en su momento para definir la red utilizada por los clientes PPPoE.

Las opciones restantes son para la autenticación mediante RADIUS. Si desea pasar la autenticación peticiones a un servidor RADIUS, complete la información en la mitad inferior de la pantalla. Si en cambio prefiere usar autenticación local, a continuación, Guardar la configuración y haga clic en la ficha de usuario agregar usuarios locales. Haga clic para añadir un usuario y luego rellenar el nombre de usuario, contraseña, y una opcional dirección IP.

Ver Sección 24.1, "de autenticación RADIUS con Windows Server" para obtener información sobre la configuración hasta RADIUS en un servidor Windows, pero puede utilizar cualquier servidor RADIUS que desees.

Capítulo 22. Sistema de seguimiento

Tan importante como los servicios prestados por pfSense son los datos y la información que le permite pfSense ver. A veces parece que los routers comerciales salen de su manera de ocultar toda la información posible de usuarios, pero pfSense puede proporcionar casi toda la información que cualquier persona podría quiero volver (y algo más).

22.1. Sistema de Registros

pfSense registros de un poco de datos por defecto, pero lo hace de una manera que no se desbordará la de almacenamiento en el router. Los registros se encuentran en Estado → Sistema de Registros en el WebGUI, y bajo `/ Var / log /` en el sistema de archivos. Algunos componentes como DHCP e IPsec, entre otros, generar suficientes registros que tienen sus propias fichas de registro para reducir el desorden en las principales de registro del sistema y la facilidad de solución de problemas para estos servicios individuales. Para ver estos otros registros, haga clic en
en la ficha para el subsistema que desea ver.

pfSense registros están contenidos en un registro binario circular o formato de obstrucción. Estos archivos tienen un

tamaño fijo,
y nunca crecen. Como consecuencia de esto, el registro sólo se llevará a cabo una cierta cantidad de entradas y las entradas viejas son continuamente expulsados del registro como los nuevos se agregan. Si esto es un problema para usted o su organización, usted puede ajustar la configuración de registro para copiar estas entradas a otro servidor con syslog donde pueden ser retenidos de forma permanente o en rotación con menor frecuencia. Ver Sección 22.1.3, "Registro remoto con Syslog" más adelante en esta sección para obtener información acerca de syslog.

22.1.1. Viendo los archivos de registro

El sistema de registros puede ser encontrado en estado de → Registros del sistema, en la pestaña Sistema. Esto incluirá
las entradas de registro generados por el propio anfitrión, además de los creados por algunos de los servicios y paquetes que no tienen sus registros de redirigir a otras fichas y archivos de registro.

Como se puede ver por ejemplo en las entradas Figura 22.1, "Ejemplo de entradas del registro del sistema", hay son las entradas de registro del demonio SSH, el paquete avahi, y el cliente de DNS dinámico. Muchos otros subsistemas registrará aquí, pero la mayoría no se sobrecarga de los registros a la vez. Normalmente, si un servicio tiene muchas entradas de registro que se trasladó a su propia pestaña / archivo de registro. También tenga en cuenta en este ejemplo
que los registros están configurados para aparecer en el orden inverso, y las entradas más recientes aparecen en la parte superior
de la lista. Consulte la sección siguiente para saber cómo configurar los registros para el orden inverso.

Aug 5 18:15:57	avahi-daemon[38307]: Found user 'avahi' (UID 1003) and group 'avahi' (GID 1003).
Aug 5 18:15:41	avahi-daemon[44110]: Leaving mDNS multicast group on interface em0.IPv4 with address 192.168.10.1.
Aug 5 18:15:41	avahi-daemon[44110]: Leaving mDNS multicast group on interface tun0.IPv4 with address 192.168.100.2.
Aug 5 18:15:41	avahi-daemon[44110]: Got SIGTERM, quitting.
Aug 5 18:15:32	sshd[38258]: Accepted password for admin from 192.168.10.10 port 64864 ssh2
Aug 5 01:01:02	php: : phpDynDNS: No Change In My IP Address and/or 25 Days Has Not Past. Not Updating Dynamic DNS Entry.
Aug 5 01:01:02	php: : DynDns: Cached IP: 72.69.194.6
Aug 5 01:01:02	php: : DynDns: Current WAN IP: 72.69.194.6
Aug 5 01:01:02	php: : DynDns: _detectChange() starting.
Aug 5 01:01:02	php: : DynDns: updatedns() starting
Aug 5 01:01:02	php: : DynDns: Running updatedns()

Figura 22.1. Ejemplo de las entradas del registro del sistema

22.1.2. Cambiar la configuración de registro

configuración de registro pueden ser ajustados por ir a Estado → Registros del sistema y el uso de la ficha Configuración. Aquí
usted encontrará varias opciones para elegir que controlan cómo se muestran los registros.

La primera opción, las entradas de registro Mostrar en orden inverso, controla el orden en que los registros se muestran
en las distintas fichas de registro. Con esta opción, la más nueva de las entradas será en la parte superior de la registro de salida. Cuando esta opción está desactivada, la más antigua de las entradas será en la parte superior. Algunas personas
encontrar estos dos métodos útiles y fáciles de seguir, así que usted puede elegir cualquier configuración que usted prefieren.

El ajuste que viene, Número de entradas de registro para mostrar el resultado, sólo controla la cantidad de líneas de registro se muestran
en cada ficha. La actual registros puede contener más datos, por lo que este puede ser ajustado hacia arriba o hacia abajo un poco
si es necesario.

Normalmente, todos los paquetes bloqueados por defecto del firewall regla de rechazo se registra. Si no deseas para ver estas entradas de registro, desactive los paquetes de registro bloqueados por la opción de la regla por defecto.

El filtro Mostrar troncos opción controla la salida de la ficha Servidor de seguridad de registros. Cuando se activa, la salida no será interpretado por el analizador de registro, y en su lugar se mostrará en su prima
formato. A veces esto puede ayudar en la solución de problemas, o si necesita ayuda en el registro de primas dará información de un técnico más de lo que normalmente se ve en el registro de salida por defecto del firewall. La prima los registros son más difíciles de leer e interpretar que la analiza los registros, por lo que este es típicamente no se controla la mayoría de
de la época.

Haga clic en Guardar cuando haya terminado de hacer cambios. Las opciones restantes en esta pantalla son discutido en la siguiente sección.

22.1.3. Registro remoto con Syslog

Las otras opciones en Estado → Registros del sistema en la ficha Configuración son para el uso de syslog para copiar
registro de las entradas a un servidor remoto. Debido a que los registros mantenidos por pfSense en el router en sí son de tamaño finito, copiar estas entradas a un servidor syslog puede ayudar a solucionar problemas y largo plazo seguimiento. Los registros en el router se borran al reiniciar el sistema, así que tener una copia remota también puede ayudar a diagnosticar los eventos que ocurren justo antes de reiniciar el router.

Algunas políticas de la empresa o legislativos dictan cuánto tiempo deben mantenerse los registros de firewalls y similares dispositivos. Si su organización requiere la retención de registros a largo plazo, tendrá que configurar un syslog servidor para recibir y mantener estos registros.

Para iniciar el registro de forma remota, de verificación Habilitar syslog'ing al servidor syslog remoto, y rellenar una dirección IP
dirección de su servidor syslog junto al servidor remoto Syslog. Si usted también desea desactivar registro local, se puede comprobar Deshabilitar escritura de archivos de registro en el disco ram local, pero esto no es general
recomienda.

El servidor syslog es típicamente un servidor que es directamente accesible desde su sistema de pfSense una interfaz local. Inicio de sesión también pueden ser enviados a un servidor a través de una VPN, pero necesitan algo extra
configuración (véase Sección 13.4.4, "pfSense-inició tráfico e IPsec") Usted no debe enviar syslog datos directamente a través de su conexión WAN, como lo es de texto plano y podría contener sensibles de la información.

Marque las casillas para las entradas del registro que desea copiar al servidor syslog. Usted puede elegir para iniciar sesión de forma remota los eventos del sistema, eventos cortafuegos, los eventos del servicio DHCP, autoridades Portal, eventos VPN
y todo lo demás.

Asegúrese de hacer clic en Guardar cuando haya terminado de hacer cambios.

Si usted no tiene un servidor syslog, es bastante fácil de configurar una. Ver Sección 24.3, "Servidor Syslog en Windows con Kiwi Syslog " para obtener información sobre la configuración de Kiwi Syslog en Windows. Casi cualquier sistema UNIX o UNIX que puede ser utilizado como un servidor syslog. FreeBSD se describe en el siguiente sección, pero otros pueden ser similares.

22.1.3.1. Configurar un servidor de Syslog en FreeBSD

Configuración de un servidor syslog en FreeBSD sólo requiere un par de pasos. En estos ejemplos, reemplace *192.168.1.1* con la dirección IP de su servidor de seguridad, vuelva a colocar *Consejo Ejecutivo-RTR* con el nombre de host
de su servidor de seguridad, y reemplazar *Consejo Ejecutivo-rtr.example.com* con el nombre de host de DNS y dominio
de su servidor de seguridad. Yo uso *192.168.1.1* en estos ejemplos, ya que se recomienda hacer esto

con la dirección interna del router, no un tipo de interfaz WAN.

En primer lugar, es probable que necesite una entrada en `/ Etc / hosts` que contiene la dirección y el nombre de su
cortafuegos, así:

192.168.1.1 *Consejo Ejecutivo-RTR* *Consejo Ejecutivo-rtr.example.com*

Luego hay que ajustar los indicadores de inicio de syslogd para que acepte mensajes de syslog desde el servidor de seguridad. Editar
`/ Etc / rc.conf` y añadir esta línea si no existe, o añadir esta opción a la línea ya existente para el ajuste:

`syslogd_flags = "-un` *192.168.1.1* `"`

Por último, tendrás que añadir algunas líneas a `/ Etc / syslog.conf` que las capturas de las entradas de registro de
esta máquina. Debajo de las entradas existentes, añada las siguientes líneas:

```
! *
+ *
+Consejo Ejecutivo-RTR
*.* / Var / log /Consejo Ejecutivo-RTR. Log
```

Esas líneas se restablecerán los filtros del programa de acogida y, a continuación, establecer una serie de filtro para el servidor de seguridad
(Utilizar su nombre corto como entró en `/ Etc / hosts`). Si está familiarizado con syslog, usted puede buscar
en `/ Etc / syslog.conf` en el router pfSense y también el filtro de registros de diversos servicios en archivos separados de registro en el servidor syslog.

Después de estos cambios será necesario reiniciar syslogd. En FreeBSD esto es sólo un simple comando:

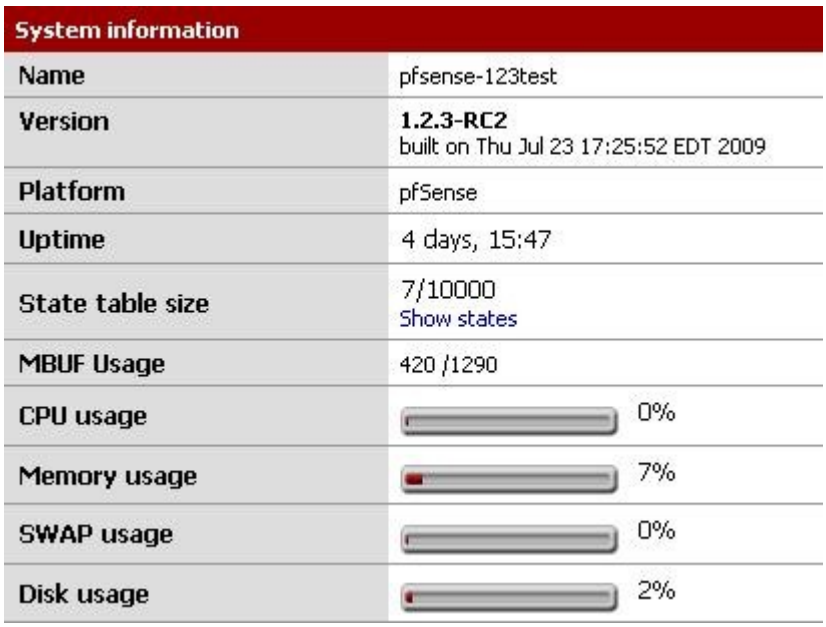
#/ Etc / rc.d / syslogd reiniciar

Ahora debería ser capaz de mirar en el archivo de registro en el servidor de syslog y ver que rellenar con entradas del registro de la actividad que ocurre en el servidor de seguridad.

22.2. Estado del sistema

La página principal de un sistema de pfSense es también la página de estado del sistema (Estado → Sistema, se muestra
en Figura 22.2, "Estado del sistema"). Contiene información básica del sistema, tales como el nombre del router, la versión de pfSense que se está ejecutando, la plataforma (Sección 1.6, "Plataformas"), el tiempo de actividad, indicando el tamaño de tabla (Sección 4.5.9.6, "Firewall de Estados máximo"), MBUF uso, uso de CPU,

el uso de memoria, uso de espacio de intercambio y el uso del disco. Los contadores de la página de actualización cada pocos
segundos de forma automática, por lo que actualizar la página no es necesario.



System information	
Name	pfsense-123test
Version	**1.2.3-RC2** built on Thu Jul 23 17:25:52 EDT 2009
Platform	pfSense
Uptime	4 days, 15:47
State table size	7/10000 Show states
MBUF Usage	420 /1290
CPU usage	0%
Memory usage	7%
SWAP usage	0%
Disk usage	2%

Figura 22.2. Estado del sistema

22.3. Estado de la interfaz

El estado de las interfaces de red puede ser visto en estado de → Interfaces. En la primera parte de Figura 22.3, "estado de la interfaz", una conexión PPPoE WAN se ha hecho y la IP, DNS, etc se ha obtenido. También puede ver la dirección de la interfaz de red MAC, tipo de medios de comunicación, en / paquetes a cabo, los errores y colisiones. tipos de conexión dinámica como PPPoE y PPTP tiene un Botón Desconectar cuando está conectado y un botón de conexión cuando está desconectado. Interfaces de la obtención de un IP de DHCP tiene un botón de lanzamiento cuando hay un contrato de arrendamiento activo, y un botón Renovar cuando no la hay.

En la parte inferior de la imagen, se puede ver la conexión LAN. Dado que se trata de un interfaz normal con una dirección IP estática, sólo con el juego habitual de los elementos se muestran.

Si el estado de una interfaz dice que "ninguna compañía", entonces por lo general significa que el cable no está conectado o el dispositivo en el otro extremo está funcionando mal de alguna manera. Si los errores se muestran, son normalmente de naturaleza física: el cableado o errores en el puerto. El sospechoso más común es el cable, y son fáciles y baratos de reemplazar.

22.4. Estado de los servicios

Muchos sistemas y servicios de paquete de mostrar el estado de sus demonios en el Estado → Servicios. Cada servicio se muestra con un nombre, una descripción, y la condición, como se ve en Figura 22.4, "Servicios de Condición Jurídica y Social ". La situación es por lo general aparece como marcha o parado. Desde este punto de vista, un corredor de servicios
pueden ser renovadas por clic o detenida por clic. Un servicio detenido puede ser iniciado haciendo clic en. Normalmente, no es necesario para controlar los servicios de esta manera, pero de vez en cuando puede haber razones de mantenimiento o reparación para hacerlo.

Service	Description	Status
avahi	Not available.	Running
dnsmasq	DNS Forwarder	Running
ntpd	NTP clock sync	Running
dhcpd	DHCP Service	Running
bsnmpd	SNMP Service	Running
miniupnpd	UPnP Service	Running
racoon	IPsec VPN	Running

Figura 22.4. Servicios de estado

22.5. RRD Gráficos

Gráficos RRD son otro útil conjunto de datos proporcionados por pfSense. Mientras que el router está ejecutando realiza un seguimiento de varios bits de datos acerca de cómo el sistema realiza, a continuación, almacena estos datos en la base de datos Round-Robin (DRR) archivos. Los gráficos de estos datos están disponibles en estado → RRD Gráficos. En esa pantalla hay seis tabletas, cada uno de los cuales son cubiertos en esta sección: Sistema, Tráfico, paquetes, calidad, colas, y Ajustes.

Cada gráfico está disponible en tramos varias veces, y cada uno de ellos es como promedio durante un diferente período de tiempo basado en cuánto tiempo se está cubriendo en un grafo dado. También en cada gráfico será una leyenda y un resumen de los datos que se muestran (mínimos, promedios, máximos, valores actuales, etc.) Los gráficos están disponibles en una gama de 4 horas con un promedio de 1 minuto, una hora 16 gama, con un promedio de 1 minuto, una serie de 2 días con un promedio de 5 minutos, una serie de 1 mes con un media hora, una serie de 6 meses con un promedio de 12 horas, y una serie de 1 año con un promedio de 12 horas.

Muchos gráficos se pueden ver en el estilo inversa o el estilo absoluto. Con estilo inversa, el gráfico se divide por la mitad horizontalmente y el tráfico de entrada se muestra va desde el centro,

y el tráfico de salida se muestra bajando desde el centro. Con un estilo absoluto, los valores se superpuestos.

En Figura 22.5, "Gráfico del tráfico WAN", Se puede ver que es un gráfico 16 horas inversa de tráfico en de la WAN, que ha tenido un uso máximo de 1.74Mbit / s promedio durante un período de 1 minuto.

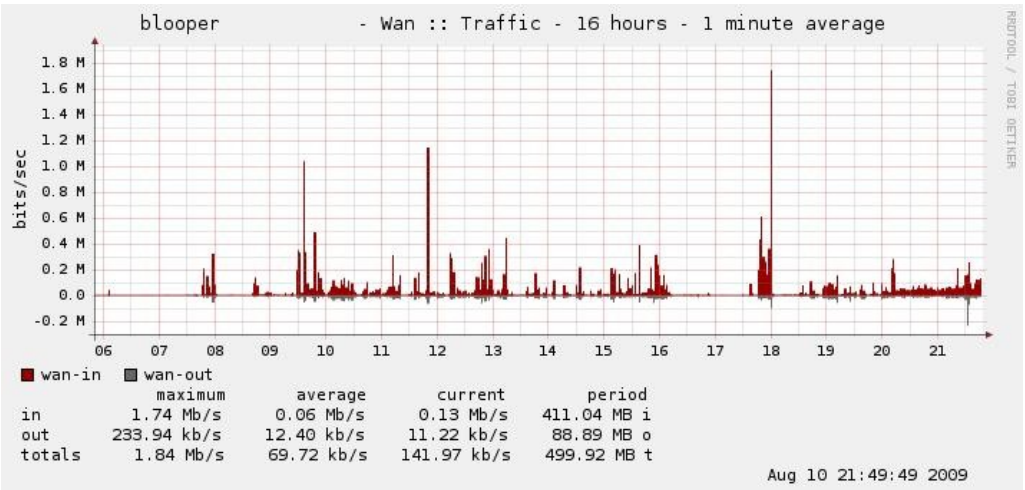


Figura 22.5. Gráfico del tráfico WAN

22.5.1. Sistema de Gráficos

Los gráficos en la ficha Sistema de mostrar un panorama general de la utilización del sistema, incluyendo uso de la CPU, el rendimiento total, y los estados de firewall.

22.5.1.1. Procesador Gráfico

El procesador gráfico muestra el uso de la CPU para los procesos de usuario y el sistema, las interrupciones, y el número de los procesos en ejecución.

22.5.1.2. El rendimiento gráfico

El gráfico muestra el rendimiento del tráfico entrante y saliente sumaron para todas las interfaces.

22.5.1.3. Estados Gráfico

El gráfico de estados es un poco más complejo. Se muestra el número de estados del sistema, pero también se rompe
por el valor de varias maneras. Se muestra los estados del filtro de reglas de firewall, NAT estados de reglas NAT, la cuenta de la fuente única de activos y las direcciones IP de destino, y el número de cambios de estado por segundo.

22.5.2. Tráfico Gráficos

gráficos de tráfico se muestran la cantidad de ancho de banda utilizado en cada interfaz disponible en bits por segunda notación, y también hay una opción Allgraphs que mostrará todos los gráficos de tráfico en una sola página.

22.5.3. Paquete de Gráficos

Los gráficos de paquetes de trabajo al igual que los gráficos de tráfico, pero en lugar de información basado en la ancho de banda utilizado, informa el número de paquetes por segundo (pps) pasado.

22.5.4. Calidad de los gráficos

El gráfico de calidad seguimiento de la calidad de la WAN o interfaz WAN, como (las que tienen una puerta de enlace especificado, o mediante DHCP). Se muestran en estas gráficas son el tiempo de respuesta de la puerta de entrada en milisegundos, así como un porcentaje de paquetes perdidos. Cualquier pérdida en el gráfico indica la conectividad cuestiones o los tiempos de uso de ancho de banda excesivo.

22.5.5. Cola de gráficos

Los gráficos de colas son un compuesto de cada cola conformador de tráfico. Cada cola individuales se muestra, representada por un color único. Usted puede ver bien el gráfico de todas las colas, o un gráfico de la que representan las gotas de todas las colas.

22.5.6. Configuración

Las gráficas RRD puede ser personalizado para adaptarse mejor a sus preferencias. Usted puede incluso desactivar si usted prefiere utilizar alguna solución gráfica externa en su lugar. Haga clic en Guardar cuando termine de hacer los cambios.

22.5.6.1. Habilitar gráfica

Marque la casilla para activar la gráfica, o quite la marca gráfica de desactivar.

22.5.6.2. Categoría por defecto

La toma por defecto Categoría opción de la ficha que aparecerá en primer lugar cuando se hace clic sobre la situación → RRD gráficos.

22.5.6.3. Estilo predeterminado

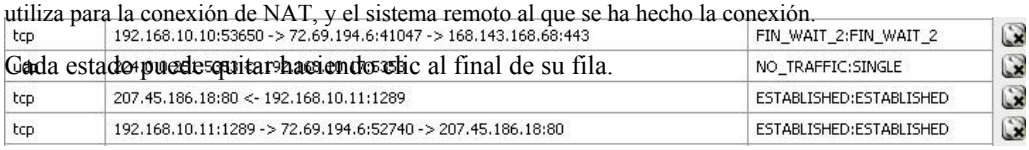
La opción por defecto de estilo que recoge el estilo de gráficos para el uso por defecto, inversa o el Absoluto.

22.6. Servidor de seguridad de los Estados

Como se discutió en Sección 6.1.2, "filtrado con estado", PfSense es un firewall y usa un estado para realizar un seguimiento de cada conexión desde y hacia el sistema. Estos estados pueden ser vistos en varios maneras, ya sea en la WebGUI o desde la consola.

22.6.1. Viendo en la WebGUI

Visualización de los estados de la WebGUI se puede hacer visitando el Diagnóstico → Estados (Figura 22.6, "Los Estados Ejemplo"). Aquí podrás ver el protocolo para cada sentido, en su origen, router, y Destino, y su estado de conexión. Cuando se trata de entradas NAT, las tres entradas de la columna central representan el sistema que hizo la conexión, la dirección IP y puerto de pfSense utiliza para la conexión de NAT, y el sistema remoto al que se ha hecho la conexión.



Cada estado puede quitar haciendo clic al final de su fila.

Figura 22.6. Estados Ejemplo

22.6.2. Viendo con pftop

pftop está disponible en el sistema de menú de la consola, y ofrece una vista en vivo de la tabla de estado a lo largo de con la cantidad total de ancho de banda consumido por cada estado. Hay varias maneras de alterar la vista al ver pftop. Pulse h para ver una pantalla de ayuda que explica las opciones disponibles.

Los usos más comunes son el uso del 0 al 8 para seleccionar diferentes puntos de vista, el espacio para una inmediata
actualización, y q para salir.

22.7. Tráfico Gráficos

Gráficos de tráfico en tiempo real dibujados con SVG (Scalable Vector Graphics) que están en constante actualización. Usted puede encontrarlos en Estado → Los gráficos de tráfico, y un ejemplo de la gráfica se puede que se encuentran en la Figura 22.7, "Ejemplo de WAN Gráfico". Estos le permitirán ver el tráfico que pasa, y dar una visión mucho más clara de lo que está sucediendo "ahora" de confiar en los datos de un promedio de las gráficas RRD.

Sólo una interfaz es visible en un momento, y usted puede elegir cuál ver en el
Interfaz de lista desplegable. Una vez que la interfaz es elegido, la página se actualizará automáticamente y empezar a mostrar el nuevo gráfico. La característica Dashboard en pfSense 2.0 (también disponible en una versión beta paquete en el punto 1.2) permite la visualización simultánea de múltiples gráficos de tráfico en una sola página.

Capítulo 23. Paquetes

El sistema de paquetes pfSense ofrece la posibilidad de ampliar pfSense sin añadir hinchazón y posibles vulnerabilidades de seguridad a la distribución base. Los paquetes sólo se admiten en plena no se instala, el CD en vivo y más plataformas embebidas. Las versiones más recientes que están incrustados sobre la base de NanoBSD ahora tienen la capacidad de ejecución de algunos paquetes. Algunos paquetes pueden También se construirá en el sistema base, como el paquete SIP Proxy. Para ver los paquetes disponibles, vaya a Sistema → Paquetes.

23.1. Introducción a los paquetes

Muchos de los paquetes han sido elaborados por la comunidad pfSense y no por el pfSense desarrollo de equipos. Los paquetes disponibles varían ampliamente, y algunos son más maduros y en buen estado que otras. Hay paquetes que instalan y proporcionan una interfaz GUI para software de terceros, tales como calamares, y otros que extienden la funcionalidad de pfSense sí mismo, como el conjunto de paneles que backports algunas funciones de pfSense 2.0.

Nota

Estos paquetes de pfSense son diferentes a los paquetes de FreeBSD puertos que están cubiertos en Sección 24.4, "Utilización de Software de Sistema de ports de FreeBSD (Paquetes) " en el capítulo de software de terceros.

Con mucho, el paquete más populares disponibles para pfSense es para el servidor proxy Squid. Se instala más de dos veces más que el siguiente paquete más popular: squidGuard, que es un filtro de contenidos que trabaja con Squid para controlar el acceso a los recursos web por los usuarios. Como era de esperar, la tercera paquete más popular es Lightsquid, que es un registro de Squid paquete de análisis que le permite ver los sitios web que han sido visitadas por los usuarios detrás del proxy.

Algunos otros ejemplos de paquetes disponibles (que no son Squid relacionados) son los siguientes:

- Ancho de banda de los monitores que muestran el tráfico por dirección IP, tales como frecuencia, BandwidthD, NTOP, y Darkstat.
- Servicios adicionales como un servidor DNS, servidor TFTP, FreeRADIUS y FreeSwitch (a VoIP PBX).
- La representación de otros servicios como SIP, IGMP y IMSpector.

• Sistema de utilidades como NUT para el seguimiento de un UPS, lcdproc para el uso de una pantalla LCD, y phpsysinfo.

• Popular de terceros utilidades como nmap, iperf y arping.

• Enrutamiento BGP, edición de Cron, Nagios y los agentes de Zabbix, y muchos, muchos otros.

Al escribir estas líneas hay más de 50 diferentes paquetes disponibles, demasiados para cubrirlos todos en este libro! Si desea ver la lista completa, que estará disponible dentro de su pfSense sistema de navegación del sistema → Paquetes.

Usted puede notar que la pantalla de los paquetes pueden tardar un poco más en cargar que otras páginas de la interfaz web. Esto se debe a que obtiene la información del paquete XML desde nuestros servidores antes de se procesa la página para proporcionar la información más actualizada del paquete. Si el servidor de seguridad se no tienen una conexión funcional a Internet como la resolución de DNS, esto no y le notificará, como en Figura 23.1, "no del paquete de recuperación de información". Si anteriormente con éxito recuperar la información del paquete, se mostrará desde la memoria caché, pero puede que no tenga el más la información más reciente. Esto es generalmente causado por una configuración de servidor DNS incorrecta o faltante. Para conexiones estáticas de IP, compruebe que trabajan los servidores DNS se registran en el sistema → General Configuración de la página. Para aquellos con conexiones asignada dinámicamente, asegurar los servidores asignados por su ISP están funcionando. Es posible que desee anular estos servidores asignados dinámicamente con OpenDNS [Http://www.opendns.com] u otro servidor DNS.

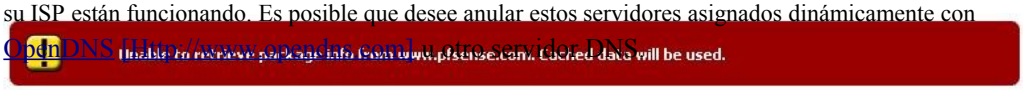


Figura 23.1. Paquete de recuperación de información no

Un número creciente de paquetes tienen un enlace Información del paquete en la lista de paquetes, que apunta a un sitio con más información sobre ese paquete en particular. Usted debe leer la información en el paquete Información de enlace antes de instalar un paquete. Después de la instalación, usted puede encontrar el más reciente paquete Información de enlace de cada paquete instalado en la pestaña de paquetes instalados.

23.2. Instalación de paquetes

Los paquetes se instalan desde Sistema → Paquetes. Los listados que se manifiestan en Figura 23.2, "El paquete de venta", Se mostrará el nombre de un paquete, la categoría, la versión y el estado, un paquete vincular la información, y una breve descripción. Prestar mucha atención al estado de antes de instalar paquetes, algunos paquetes son experimentales y no se debe instalar en la producción crítica

sistemas. Usted también debe mantener los paquetes instalados a lo estrictamente necesario para su implementación.

Figura 23.2. El paquete de venta

Los paquetes están instalados, haga clic en el botón a la derecha de su entrada. Al hacer clic, usted será llevado a la pantalla de instalación de paquetes donde el progreso de la instalación se mostrará (Figura 23.3, "después de la instalación del paquete de pantalla").

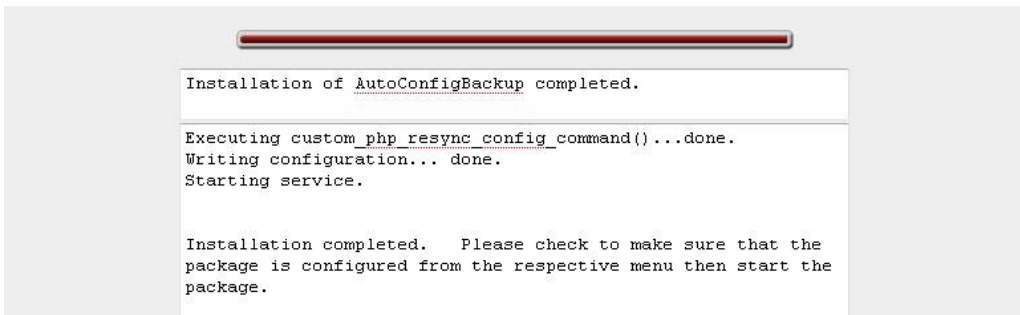


Figura 23.3. Posterior a la instalación de la pantalla del paquete

23.3. Reinstalación y actualización de paquetes

Los paquetes se vuelven a instalar y actualizar la misma manera. Para empezar, vamos a Sistema → Paquetes y clic en la ficha paquetes instalados. Las listas no debe verse como Figura 23.4, "Instalación Lista de paquetes ". Encuentra el paquete que desea volver a instalar o actualizar en la lista. Si hay una nueva Disponible en versión de lo que usted ha instalado, la columna del paquete, versión serán resaltados en rojo indicando las versiones antiguas y nuevas. Haga clic para actualizar o reinstalar el paquete.

Otra opción sería volver a instalar para volver a instalar sólo el código XML componentes GUI de un paquete, que se puede hacer haciendo clic en junto a la entrada de paquetes. A menos que se le indique por un desarrollador, no debe usar esta opción, ya que puede perder las actualizaciones de los binarios que la última interfaz gráfica de usuario
componentes que necesite.

Package Name	Category	Package Info	Package Version	Description
AutoConfigBackup	Services	Package Info	1.15	Automatically backs up your pfSense configuration. All contents are encrypted on the server. Requires pfSense Premium Support Portal Subscription from https://portal.pfsense.org

Figura 23.4. Lista de paquetes instalados

23.4. Desinstalación de paquetes

Para desinstalar un paquete, vaya a Sistema → Paquetes y haga clic en la pestaña paquetes instalados. Buscar el paquete en la lista y haga clic en el botón. El paquete de continuación, se eliminará de el sistema.

Algunos paquetes experimentales sobrescribir los archivos distribuidos con el sistema base. Estos paquetes no se puede desinstalar, ya que al hacerlo se rompería el sistema base restante. La entrada de paquetes aún puede mostrar el icono de desinstalación, pero todavía estará presente después de su intento de extracción. Paquetes con esta peculiaridad se etiquetará como tal en su campo de descripción. Si se actualiza el sistema, que se sobreponen a los cambios realizados por estos paquetes, por lo que este es un medio posible de desinstalación. Tenga mucho cuidado con cualquier paquete que no se puede desinstalar, por lo general destinados a la experimentación con sistemas no críticos.

23.5. Paquetes de desarrollo

Los paquetes son relativamente fáciles de desarrollar, y usted puede encontrar que usted o su organización pueden beneficiarse de la elaboración de un paquete que no existe. Para aquellos interesados en la creación de sus propios paquetes, los recursos están disponibles en el pfSense Wiki de documentación [http://doc.pfsense.org / index.php / Developing_Packages]. Si crea un paquete y piensan que puede ser de uso a los demás, en contacto con nosotros y su trabajo puede ser evaluado para su inclusión en el sistema de paquetes para que todos puedan ver.

Capítulo 24. Software de terceros y pfSense

Aunque este libro se centra en pfSense, hay una serie de paquetes de software de tercero que puede ser configurado para funcionar con pfSense o aumentar su funcionalidad. En este contexto, en tercer lugar software de consulta de software disponibles de otros proveedores o fuentes que se pueden utilizar junto con pfSense, pero no se considera parte del "sistema de pfSense". Estos son diferentes de los paquetes de pfSense, que son software adicional que se ejecuta en el sistema de pfSense y se integra en la interfaz gráfica de usuario del sistema.

24.1. RADIUS de autenticación de Windows Servidor

Windows 2000 Server y Windows Server 2003 puede ser configurado como un servidor RADIUS mediante Servicio de Microsoft de autenticación de Internet (IAS). Esto le permite autenticar el pfSense servidor PPTP, Portal Cautivo, o el servidor PPPoE en sus cuentas de usuario local de Windows Server o Active Directory.

24.1.1. La elección de un servidor para IAS

NIC requiere una cantidad mínima de recursos y es adecuado para su adición a la existencia de Windows Servidor en la mayoría de entornos. Microsoft recomienda instalarlo en un dominio de Active Directory controlador para mejorar el rendimiento en entornos en los que la NIC está autenticando en Active Directorio. También es posible instalarlo en un servidor miembro, que puede ser deseable en algunos entornos para reducir la huella de ataque de los controladores de dominio - cada red servicio de acceso proporciona otra vía potencial de comprometer el servidor. NIC no tienen un historial de seguridad sólida, especialmente en comparación con otras cosas que se debe ejecutar en su los controladores de dominio de Active Directory para funcionar, así que esto no es mucho de una preocupación más en entornos de red. La mayoría de entornos de instalar IAS en uno de sus controladores de dominio.

24.1.2. Instalación de la NIC

En el servidor de Windows, vaya a Panel de control, Agregar o quitar programas, y seleccione Agregar o quitar Componentes de Windows. Desplácese hacia abajo y haga clic en Servicios de red, haga clic en Detalles. Compruebe Servicio de autenticación Internet en la lista Servicios de red y haga clic en Aceptar. A continuación, haga clic en Siguiente

y la NIC se instalará. Es posible que tenga que proporcionar el CD del servidor para la instalación de completa. Cuando la instalación haya finalizado, haga clic en Finalizar.

24.1.3. Configuración de la NIC

Para configurar la NIC, que aparezca la NIC MMC en Herramientas administrativas, Internet Servicio de autenticación. En primer lugar un cliente RADIUS será añadido para pfSense, a continuación, el acceso remoto políticas se configurará.

24.1.3.1. Adición de un cliente RADIUS

Haga clic en Clientes RADIUS y haga clic en Nuevo cliente RADIUS, como se muestra en Figura 24.1, "Añadir cliente RADIUS nuevo ".

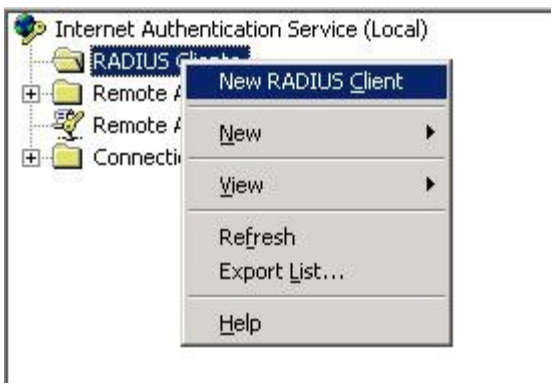


Figura 24.1. Agregar nuevo cliente RADIUS

Escriba un "nombre" para el servidor de seguridad, como se muestra en la Figura 24.2, "Añadir nuevo cliente RADIUS - Nombre y dirección del cliente ", que puede ser su nombre de host o FQDN. El campo de dirección de cliente debe ser la dirección IP que pfSense iniciará sus solicitudes de RADIUS, o un nombre de dominio completo que se determinación de esa dirección IP. Esta será la dirección IP de la interfaz más cercana a la del radio servidor. Si el servidor RADIUS es accesible a través de su interfaz LAN, esta será la IP de la LAN. En despliegues en pfSense no es su servidor de seguridad perimetral, y su interfaz WAN se encuentra en la red interna donde reside el servidor RADIUS, la dirección IP WAN es lo que debe entre aquí. Escriba el nombre de amistad ya la dirección de pfSense, a continuación, haga clic en Siguiente. Deja cliente-proveedor establecido en **RADIUS estándar**, Y rellenar un secreto compartido, como se muestra en Figura 24.3, "Añadir nuevo cliente RADIUS - Secreto compartido". Este secreto compartido es lo que entrar en pfSense más tarde. Haga clic en Finalizar.

Ya ha finalizado la configuración del NIC. Usted puede ver el cliente RADIUS que acaba de agregó que en Figura 24.4, "de venta del cliente de RADIUS".

Friendly Name	Address	Protocol	Client-Vendor
fw0	10.0.66.22	RADIUS	RADIUS Standard

Figura 24.4. Listado del cliente RADIUS

Ahora ya está listo para configurar pfSense con la información RADIUS configurado aquí, utilizando la dirección IP del servidor IAS y el secreto compartido configurado previamente. Consulte el parte de este libro que describe el servicio que desea utilizar con RADIUS para mayor orientación. RADIUS se puede utilizar para Portal Cautivo (Sección 19.4, "Configuración del Portal Usar RADIUS Autenticación "), el servidor PPTP (Sección 14.5.2, "autenticación"), Y el servidor PPPoE (Sección 21.9, "Servidor PPPoE"), Y también en algunos paquetes.

24.1.3.2. Configuración de usuarios y Política de acceso remoto

Si un usuario puede autenticar a través de RADIUS se controla con permiso de acceso remoto en cada usuario de la cuenta en la ficha Marcado de las propiedades de cuenta de usuarios y Equipos. No se puede especificar para permitir o denegar el acceso, o acceso de control remoto a través de Directiva de acceso. Usted tiene la opción de especificar el acceso aquí para cada usuario mediante la especificación de permitir o negar. Para entornos de pequeño con los requisitos básicos, esto puede ser preferible. Acceso remoto políticas escala mejor para entornos con más usuarios, usted puede colocar simplemente un usuario en un determinado Grupo de Active Directory para permitir el acceso VPN, y también ofrecen capacidades más avanzadas, como tiempo de las restricciones al día.
Más información sobre las políticas de acceso remoto se puede encontrar en la documentación de Microsoft en http://technet.microsoft.com/en-us/library/cc785236% 29.aspx 28WS.10%.

Después de configurar los usuarios y las políticas de acceso remoto si lo desea, usted está listo para probar el servicio que está utilizando con RADIUS en pfSense.

24.1.3.3. Solución de problemas de la NIC

En caso de fallar la autenticación, esta sección se describen los problemas más comunes se encuentran los usuarios con las NIC.

24.1.3.3.1. Compruebe el puerto

En primer lugar garantizar el puerto por defecto 1812 se está utilizando. Si el servidor IAS se ha instalado anteriormente, puede haber sido configurado con los puertos no estándar. En la consola MMC de la NIC, haga clic en

Servicio de autenticación Internet (local) en la parte superior izquierda de la consola MMC y haga clic en Propiedades.

A continuación, haga clic en la ficha Puertos. Puede especificar varios puertos separándolos con comas (Como se muestra en Figura 24.5, "NIC Puertos"). El puerto 1812 debe ser uno de los puertos configurados para Autenticación. Si está utilizando la funcionalidad de administración de cuentas RADIUS, así, el puerto 1813 debe ser uno de los puertos especificados en Contabilidad.

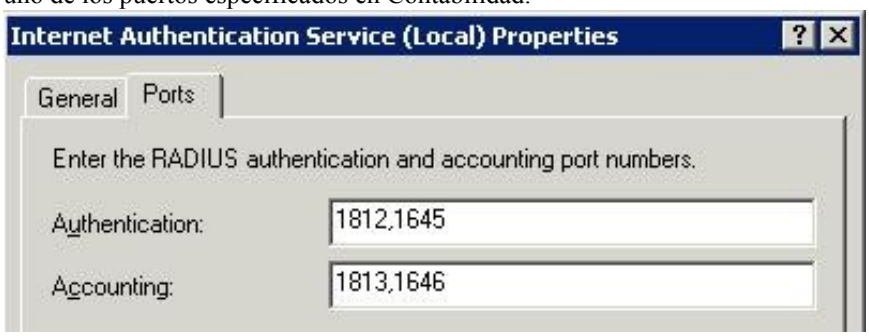


Figura 24.5. NIC Puertos

24.1.3.3.2. Compruebe Visor de sucesos

Cuando un intento de autenticación RADIUS es contestada por el servidor, los registros de NIC para el sistema registro en el Visor de sucesos con el resultado de la solicitud de autenticación y, si se deniega el acceso, la razón por la cual fue denegada. En el campo Descripción de las propiedades de evento, la línea de la razón explica por qué error en la autenticación. El común de dos fracasos son: nombre de usuario y la contraseña mal, cuando un usuario entra credenciales incorrectas, y "permiso de acceso remoto para la cuenta de usuario fue denegada" cuando la cuenta de usuario se configura para denegar el acceso o las políticas de acceso remoto configurado en la NIC no no permitir el acceso a ese usuario. Si la NIC es el registro que la autenticación se ha realizado correctamente, pero el cliente está recibiendo un mensaje de nombre de usuario o contraseña, el secreto de RADIUS configurado en la NIC y pfSense no coincide.

24.2. Libre de filtro de contenido con OpenDNS

pfSense no incluye ningún software de filtrado de contenido en el momento de escribir esto, pero hay es una gran opción gratuita en la integración OpenDNS [http://www.opendns.com]. En primer lugar usted necesita configurar su red para utilizar los servidores DNS de OpenDNS para todas las consultas recursivas.[1]

[1]Nota: Yo soy de ninguna manera afiliado con OpenDNS, sólo un usuario muy satisfecho de sus servicios en múltiples lugares, y he tenido numerosas la gente me las gracias por que me refiero a ellos. Ellos realmente tienen una oferta impresionante.

24.2.1. Configuración de pfSense utilizar OpenDNS

Visite el Sistema de → Página de configuración general, entre dos servidores DNS de OpenDNS allí, y desmarque
la "lista Permitir servidor DNS para ser reemplazado por DHCP / PPP WAN" caja (Figura 24.6, "Configuración de OpenDNS en pfSense").

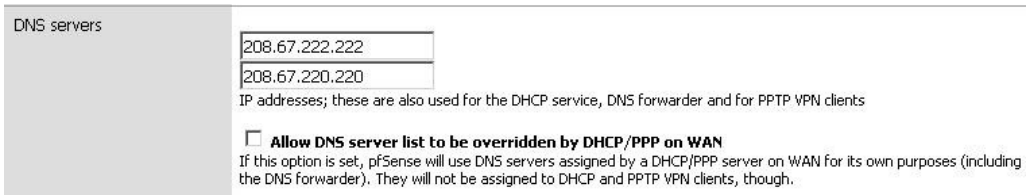


Figura 24.6. Configuración de OpenDNS en pfSense

Si las máquinas de uso interno promotor de pfSense DNS como su servidor DNS sólo, esto es todo lo que necesidad de cambio a utilizar OpenDNS para la resolución de nombres.

24.2.2. Configure los servidores DNS internos para utilizar OpenDNS

Si las máquinas de uso interno un servidor DNS interno, que debe ser configurado para enviar su consultas recursivas a los servidores de OpenDNS. Voy a explicar cómo hacerlo con Windows servidor de DNS.

24.2.2.1. Forwarders Configuración de DNS de Windows Server

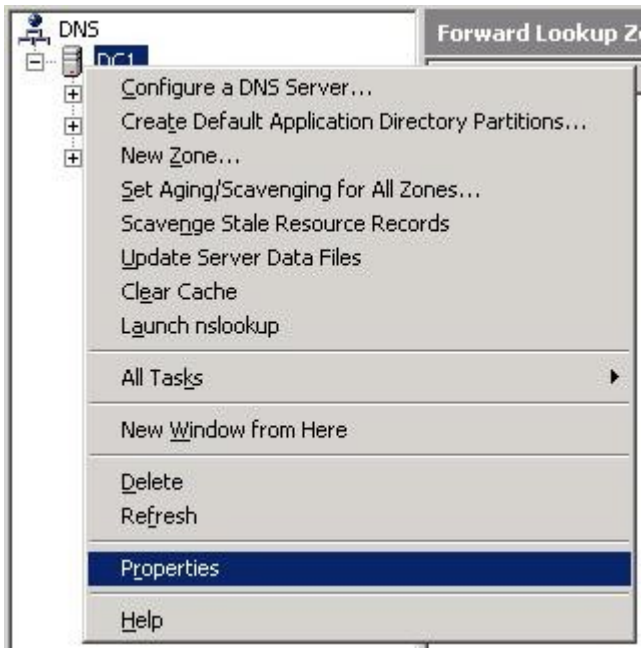


Figura 24.7. Propiedades del servidor DNS de Windows

Abra el complemento DNS de MMC en Herramientas administrativas, DNS. Haga clic derecho sobre el nombre del servidor
y haga clic en Propiedades, como se muestra en Figura 24.7, "Propiedades del servidor DNS de Windows".

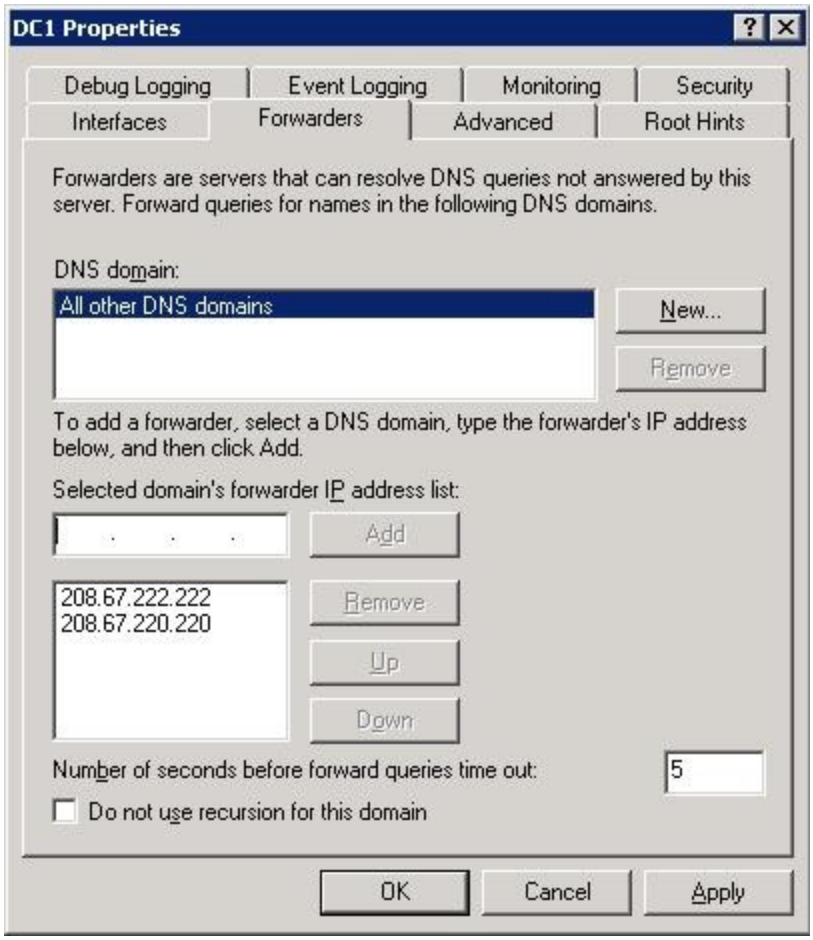


Figura 24.8. Servidor DNS de Windows Transitarios

Seleccione la ficha Reenviadores, y añadir dos servidores DNS de OpenDNS en la lista para el promotor de

"Todos los
dominios DNS ", como en Figura 24.8, "Servidor DNS de Windows Forwarders", A continuación, haga clic en Aceptar.

A continuación, repita esto para cada uno de los servidores DNS internos.

24.2.3. Configuración de filtrado de contenido OpenDNS

Ahora tiene que configurar el filtrado de contenido que desee en el sitio de OpenDNS.

24.2.3.1. Regístrate para una cuenta de OpenDNS

Examinar para http://www.opendns.com y haga clic en el enlace de entrar. A continuación, haga clic en "Crear un libre
cuenta "y pasar por el proceso de creación de la cuenta.

24.2.3.2. Definir la red (s) en OpenDNS

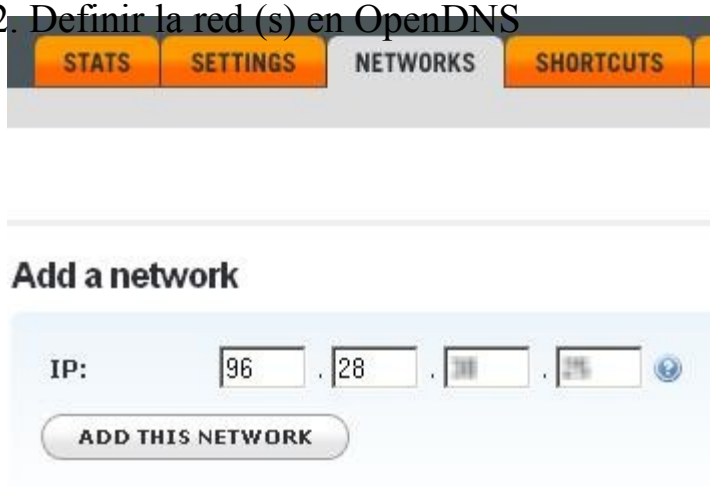


Figura 24.9. Adición de una red

OpenDNS primero tiene que ser capaz de determinar cuáles son las consultas DNS de su red que se capaz de filtrar de acuerdo a las políticas definidas en su cuenta. Después de entrar en su OpenDNS cuenta, haga clic en la pestaña "Redes" (Figura 24.9, "Adición de una red"). Se mostrará automáticamente el IP pública de la sesión HTTPS está viniendo, con un botón para añadir a esta red a su cuenta.
Haga clic en el botón Añadir esta red.

Se abrirá una ventana solicitando si tu IP es estática o dinámica (Figura 24.10, "Adición de una conexión IP dinámica"). Si usted tiene una conexión dinámica IP, tendrá que ejecutar Updater OpenDNS para Windows en una máquina dentro de su red para asegurarse de su dirección se mantiene al día con OpenDNS. Su dirección IP es el único medio de identificación de OpenDNS tiene de su red. Si tu IP no es correcta en la configuración de OpenDNS, el filtrado de contenido no funcionará como se ha configurado en su cuenta.

Para conexiones estáticas de IP, desactive la casilla "Sí, es dinámico" caja y dar a la conexión un nombre (Figura 24.11, "Adición de una conexión de IP estática"). Para conexiones estáticas de IP, no es necesario que ejecute el cliente de actualización.

Después de agregar la red a su cuenta, usted lo verá en su lista de redes como la de Figura 24.12, "Red agregado con éxito".

La red está ahora listo para usar OpenDNS, aunque todavía tienen que configurar el deseado configuración de filtrado de contenido.

24.2.3.3. Configuración de filtrado de contenidos para la configuración de su cuenta

Para configurar las opciones de filtrado de contenido, haga clic en la ficha Configuración en la parte superior de la

OpenDNS

página web. Una lista de niveles como la de la Figura 24.13, "nivel de filtrado de contenidos" debe aparecer. Usted verá a su actual nivel de filtrado es mínimo, que sólo bloquea sitios de phishing conocidos. Usted Puede elegir entre cuatro niveles diferentes de filtrado predefinidas, o seleccione Personalizar y seleccione la que categorías que desea bloquear.

También puede bloquear o permitir determinados dominios, superando a su contenido general de filtrado configuración, en la parte inferior de esta pantalla (Figura 24.14, "Gestión de dominios individuales").

OpenDNS ofrece una serie de opciones de configuración de otros lo que le permite un gran control sobre DNS de la red. Su sitio contiene una serie de artículos base de conocimientos y el apoyo detalla algunas de las posibilidades, y toda la funcionalidad está bien descrito en todo el gestión de la interfaz. Usted no tiene que parar en sólo filtrado de contenidos - revisar todo lo demás OpenDNS tiene para ofrecer, ya que puede ser capaz de poner a buen uso.

24.2.4. Configuración de las reglas de cortafuegos para prohibir DNS servidores

Ahora que sus sistemas internos son OpenDNS utilizando como su servicio de DNS, tendrá que configurar reglas de firewall por lo que no otros servidores DNS se puede acceder. De lo contrario los usuarios internos simplemente podría cambiar sus máquinas (si tienen los derechos de usuario para hacerlo) para utilizar un DNS diferente servidor que no hace cumplir su filtrado de contenido y otras restricciones.

24.2.4.1. Crear un alias de servidores DNS

En primer lugar, se desea crear un alias que contiene los servidores DNS que las máquinas internas permiso para realizar consultas, como la de Figura 24.15, "los servidores DNS alias". La dirección IP aparece en la lista porque esta red de ejemplo se utiliza el agente de DNS como su servidor DNS interno, y esto permite DNS las preguntas de la LAN a la IP de la LAN. También permite las consultas recursivas de los servidores DNS internos, y la asignación directa de los servidores DNS de OpenDNS en las máquinas internas. Tenga en cuenta que a menos que deshabilitar la regla anti-bloqueo, no es necesario agregar la IP LAN aquí, pero la adición de recomendar

sin tener en cuenta que para mayor claridad. Consulte Sección 6.5.1.1, "Regla de Lucha contra el bloqueo" para más información.

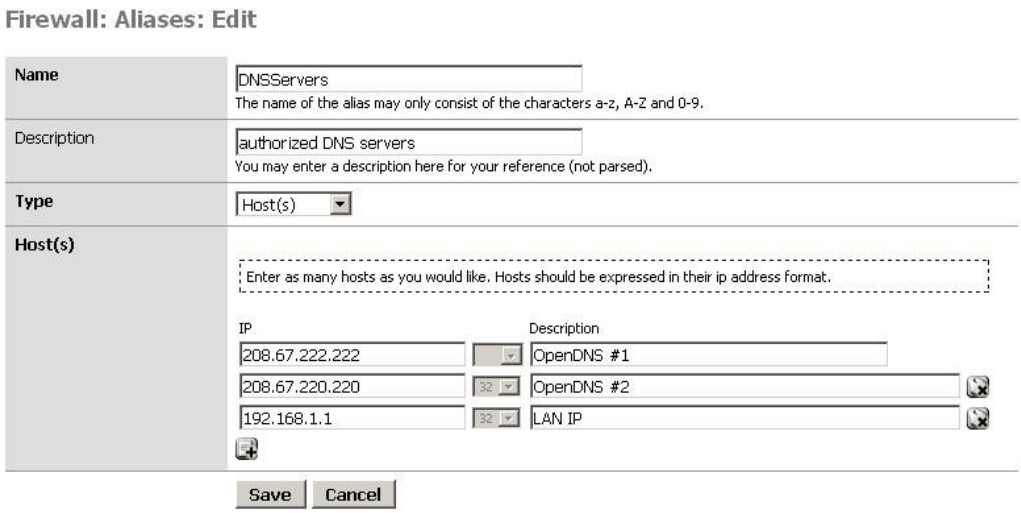


Figura 24.15. servidores DNS de alias

24.2.4.2. Configurar reglas de firewall

Ahora tiene que configurar las reglas de LAN para permitir DNS destinados creado anteriormente alias, y de bloqueo DNS a otros destinos si alguna de sus otras reglas permitiría DNS, como la regla de LAN por defecto. Como se discutió en el capítulo de firewall, yo prefiero usar rechazar las reglas para el tráfico bloqueados en las interfaces internas. El conjunto de reglas en Figura 24.16, "normas de LAN para restringir DNS" se mantiene breve y sencillo por el bien de la ilustración - Recomiendo salida mucho más fuerte de filtrado de esta muestra, tal como se describe en el capítulo de servidor de seguridad.

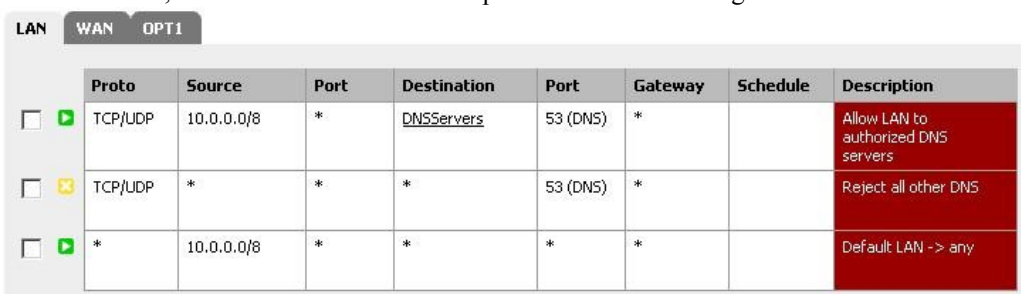


Figura 24.16. normas de LAN para restringir DNS

24.2.5. Finalización y Otras dudas

Y eso es todo. Ahora tiene un filtrado de contenidos solución integrada con pfSense en un medio que hace que sea muy difícil para el usuario medio para desplazarse. Tenga en cuenta que no es imposible conseguir alrededor, sobre todo con la mayor permisividad de un conjunto de reglas que en el ejemplo anterior muestra. Hay varias posibilidades para hacer un túnel DNS a través de ese conjunto de reglas, con las conexiones VPN, el puerto SSH expedición, y más. Pero si usted permite que todo el tráfico a través de su servidor de seguridad, que siempre va a ser una posibilidad. Correctamente bloqueado máquinas de usuario final en combinación con el anterior proporciona un fuerte contenido solución de filtrado que es difícil de conseguir alrededor.

24.3. Syslog Server en Windows con Kiwi Syslog

pfSense puede enviar los registros a un servidor externo a través del protocolo syslog (Sección 22.1.3, "Remote Inicio de sesión con Syslog "). Para usuarios de Windows, Kiwi Syslog servidor[2] es una buena opción libre para recogida de los registros de su instala pfSense. Se puede instalar como un servicio de registro a largo plazo recogida, o correr como una aplicación más cortos necesidades a largo plazo. Es compatible con el servidor y el versiones de escritorio de Windows 2000 y versiones posteriores. La instalación es muy sencillo, y no requieren una configuración mucho más. Se puede encontrar ayuda en su documentación después de la instalación.

24.4. Uso del software de los puertos de FreeBSD Sistema (paquetes)

Debido a que pfSense está basado en FreeBSD, un veterano administrador del sistema FreeBSD muchos familiarizado paquetes de FreeBSD también se puede utilizar. Instalación del software de esta manera no es para el sin experiencia, ya que podría tener efectos secundarios no deseados, y no se recomienda ni admite. Muchas partes de FreeBSD no se incluyen, por lo que la biblioteca y otras cuestiones se pueden encontrar. pfSense no incluye un compilador en el sistema base por muchas razones, y como tal software no puede ser construida a nivel local. Sin embargo, puede instalar los paquetes de paquetes pre-construidos de FreeBSD repositorio.

24.4.1. Preocupaciones / Advertencias

Antes de decidirse a instalar software adicional para pfSense que no es un paquete sancionado, no son algunos temas que necesitan ser tomadas en cuenta.

[2] http://www.kiwisyslog.com/

24.4.1.1. Las preocupaciones de seguridad

Cualquier software adicional agregado a un servidor de seguridad es un problema de seguridad, y deben ser evaluados por completo antes de
la instalación. Si la necesidad es mayor el riesgo, puede ser vale la pena tomar. Oficial paquetes de pfSense
no son inmunes a este problema tampoco. Cualquier servicio adicional es otro vector de ataque potencial.

24.4.1.2. Las preocupaciones de rendimiento

La mayoría de los sistemas de pfSense se ejecutan en hardware que puede manejar la carga de tráfico a las que están la tarea. Si usted encuentra que usted tiene potencia de sobra, no puede dañar el sistema para añadir más software. Dicho esto, tener en cuenta los recursos que serán consumidos por el software añadido.

24.4.1.3. Conflicto de software

Si instala un paquete que duplica la funcionalidad que se encuentran en el sistema base, o sustituye
un paquete de sistema de base con una versión más reciente, podría causar inestabilidad en el sistema impredecible.
Asegúrese de que el software que está después ya no existe en el sistema antes de intentar pfSense
que instalar nada.

24.4.1.4. La falta de integración

Cualquier software adicional instalado no tendrá la integración interfaz gráfica de usuario. Para algunos, esto no es un problema, pero
ha habido personas que vayan a instalar un paquete y tienen una interfaz gráfica de usuario aparece mágicamente para su configuración. Estos paquetes tendrán que ser configurados a mano. Si se trata de un servicio, que
significa también asegurarse de que todos los scripts de inicio se modifican para adaptarse a los métodos utilizados por pfSense.

También ha habido casos donde el software se ha instalado más páginas web que no son
protegidos por el proceso de autenticación de pfSense. Prueba de cualquier software instalado para asegurar que el acceso está protegida o filtrada de alguna manera.

24.4.1.5. La falta de copias de seguridad

Al instalar los paquetes de esta manera, usted debe asegurarse de que cualquier configuración de copia de seguridad o otros archivos necesarios para este software. Estos archivos no se copian durante una pfSense normal
copia de seguridad y se podrían perder o cambiado durante una actualización de firmware. Puede utilizar el complemento en el paquete
se describe en Sección 5.6, "Archivos de copia de seguridad y directorios con el paquete de copia de seguridad" una copia de seguridad
archivos arbitrarios como éstos.

24.4.2. Instalación de paquetes

Para instalar un paquete, primero debe asegurarse de que el sitio de embalaje adecuado, se utilizarán. pfSense está compilado con una rama FreeBSD-RELEASE, y los paquetes no se puede
obsoletos en un corto periodo de tiempo. Para solucionar este problema, especificar la ruta de acceso al conjunto de paquetes para FreeBSD-STABLE antes de intentar instalar un paquete:

#setenv PACKAGESITE = ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-7-stable/
#pkg_add-r flujo TCP

O usted puede proporcionar una dirección URL completa de un paquete:

#pkg_add-r ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-7-stable/Latest/iftop.tbz

El paquete debe descargar e instalar, junto con las dependencias necesarias.

También es posible construir un paquete personalizado en otro equipo que ejecuta FreeBSD y luego copiar / instalar el archivo de paquete generado en un sistema de pfSense. Debido a la complejidad de este tema, no será tratado aquí.

24.4.3. El mantenimiento de paquetes

Puede ver una lista de todos los paquetes instalados, así:

#pkg_info

Para eliminar un paquete instalado, usted debe especificar su nombre completo o utilizar un comodín:

#pkg_delete lsof-4.82, 4
#pkg_delete flujo TCP-\ *

Capítulo 25. Captura de paquetes

La captura de paquetes es el medio más eficaz de solucionar problemas con la red conectividad. Captura de paquetes (o "sniffing") herramientas como tcpdump mostrar lo que es "en el alambre" - Entrar y salir de una interfaz. Al ver la cantidad de tráfico que se recibe por el servidor de seguridad y la forma en que deja el servidor de seguridad es una gran ayuda en la reducción a problemas con las reglas del cortafuegos, NAT las entradas, y otros temas de redes. En este capítulo, cubrimos la obtención de capturas de paquetes de WebGUI, con tcpdump en la línea de comando en una concha, y el uso de Wireshark.

25.1. Captura de marco de referencia

Tenga en cuenta que la captura de paquetes de mostrar lo que está en el alambre. Es el primero en ver el tráfico cuando los paquetes que reciben y el último en ver el tráfico de la hora de enviar los paquetes a medida que fluyen a través del firewall.
Se ve el tráfico antes de cortafuegos, NAT y todo otro tipo de elaboración en el cortafuegos para el tráfico que pasa entrada en la interfaz, y después de todo lo que el procesamiento se produce para el tráfico que sale esa interfaz. Para el tráfico entrante, captura mostrará el tráfico que llega a la interfaz del servidor de seguridad independientemente de que el tráfico será bloqueado por la configuración del firewall. Figura 25.1, "Captura de referencia", donde ilustra tcpdump y también la interfaz de captura de paquetes WebGUI lazos en el orden de procesamiento.

25.2. Selección de la interfaz adecuada

Antes de empezar cualquier captura de paquetes, lo que necesita saber de donde la captura se deben adoptarse. Una captura de paquetes será diferente dependiendo de la interfaz elegida, y en ciertas situaciones es mejor para capturar en una interfaz específica, y en otros, que ejecutan varias captura simultánea en diferentes interfaces es preferible. En el uso de tcpdump en el símbolo del línea, tendrá que conocer el "verdadero" nombre de interfaz que van con los nombres descriptivos se muestra en la WebGUI. Usted puede recordar estos desde el momento en las interfaces fueron asignados originalmente, pero si no, usted puede visitar Interfaces → (Asignar) y tome nota de que las interfaces físicas, tales como `fxp0`, corresponden con las interfaces de pfSense, tales como WAN. Tabla 25.1, "Interfaz Real vs Friendly Nombres " enumera algunos nombres de interfaz que pueden surgir, dependiendo de su configuración.

Nombre real / física	Nombre descriptivo
ng0 ... ng<*x*>	WAN (WAN PPPoE o PPTP), o clientes PPTP
enc0	IPsec, el tráfico cifrado
tun0 ... tonel<*x*>	OpenVPN, el tráfico cifrado
lo0	Interfaz de bucle invertido

Nombre real / física	Nombre descriptivo
pfsync0	pfsync interfaz - de uso interno
pflog0	pf registro - de uso interno

Tabla 25.1. Real Interfaz vs nombres descriptivos

Cuando se selecciona una interfaz, que normalmente se desea iniciar con el lugar donde los flujos de tráfico en pfSense. Por ejemplo, si usted está teniendo problemas para conectarse a un puerto para la conexión desde fuera de su red, comience con la interfaz WAN, ya que es donde se origina el tráfico. Alternativamente, si usted tiene una PC cliente que no puede acceder a Internet, comience con la interfaz LAN. Cuando en duda, pruebe con múltiples interfaces y filtro de las direcciones IP o puertos en cuestión.

25.3. Limitar el volumen de captura

Cuando la captura de paquetes, es importante limitar el volumen de los paquetes capturados, pero aún así asegurar todo el tráfico relevante para el problema que se troubleshooted es capturado. En la mayoría de las redes, cuando la captura sin filtrar el tráfico capturado, incluso con capturas de cortos periodos de tiempo, usted acabar con grandes cantidades de datos a cavar hasta encontrar el problema. Puedes filtrar los post- de captura mediante el uso de filtros de visualización en Wireshark, pero filtrado adecuadamente en el momento de la captura es preferible mantener el tamaño del archivo de captura. Los filtros se discutirá más adelante en este capítulo.

25.4. Captura de paquetes de la WebGUI

El WebGUI ofrece un fácil de usar interfaz de usuario para tcpdump que le permitirá obtener capturas de paquetes que luego pueden ser vistos o descargados para un análisis más profundo en Wireshark. Debido a su simplicidad, que sólo puede ofrecer algunas opciones limitadas para filtrado de tráfico deseado, que puede complican la tarea en función del nivel de tráfico en su red y las necesidades de filtrado. Dicho esto, para muchas personas es suficiente y hace el trabajo. Si usted se siente limitado por las opciones disponibles, puede pasar hasta la siguiente sección sobre el uso de tcpdump directamente.

25.4.1. Obtener un paquete de captura

En primer lugar, vaya a Diagnósticos → Captura de paquetes para iniciar el proceso. A partir de ahí, elegir el Interfaz en la que desea capturar el tráfico. Si desea filtrar el tráfico que va o de una máquina específica, introduzca su dirección IP en el campo Dirección del host. El puerto también puede ser limitada si está capturando el tráfico TCP o UDP.

Usted puede ajustar el Paquete Longitud capturado si lo desea. Por lo general, se desea que el paquete completo, pero para captura de ejecución durante periodos más largos de tiempo en los encabezados de materia más de la carga útil del

paquetes, lo que limita este a 64 bytes o hacerlo resultará en un archivo de captura mucho más pequeños que todavía pueden
tienen datos suficientes para solucionar problemas. El cuadro de Conde determina cuántos paquetes
para capturar antes de detenerse. Si no limita la captura de cualquier manera, tenga en cuenta que esto puede
ser muy "ruidoso" y puede que tenga que aumentar este mucho más grande que el valor predeterminado de **100**.

El nivel de detalle de la opción sólo afecta a la salida como se muestra en la captura ha terminado. Lo hace
no cambiar el nivel de detalle en el archivo de captura, si usted elige para descargarlo cuando esté terminado.

En general no se recomienda comprobar búsquedas inversas DNS cuando se realiza una captura de como
que retrasará la salida como DNS inversa se lleva a cabo. También es comúnmente más fáciles de solucionar
durante la visualización de direcciones IP en lugar de nombres de host y DNS inverso a veces puede ser inexacta.
Esto puede ser útil en ocasiones, sin embargo.

Pulse Iniciar para iniciar la captura de datos. La pantalla mostrará "Captura de paquetes se ejecuta" a través de
la parte inferior, lo que indica la captura está en proceso. Pulse Detener para finalizar la captura y ver el resultado.
Si ha especificado una cantidad de paquetes máxima se detendrá automáticamente cuando lo que cuenta es llegar,
o puede hacer clic en **Detener** para ponerle fin en cualquier momento.

25.4.2. Viendo los datos capturados

La salida de captura se puede ver en la WebGUI, o descargados para su posterior visualización en un programa de
como Wireshark. Para obtener más detalles sobre el uso de Wireshark para ver un archivo de captura, consulte Sección 25.6.1,
"Visualización de archivos de paquetes de captura" más adelante en este capítulo. Haga clic en Descargar para descargar la captura de este
archivo para su posterior visualización.

El resultado que se muestra en el marco de los paquetes capturados se muestran en el estilo de tcpdump estándar.

25.5. Uso de tcpdump de la línea de comandos

tcpdump es la línea de comandos de paquetes de utilidad de captura de siempre con la mayoría de UNIX y

UNIX-como
distribuciones de sistemas operativos, incluyendo FreeBSD. También se incluye con pfSense, y utilizables
de un intérprete de comandos en la consola o por SSH. Es una herramienta muy poderosa, pero que hace también
es desalentador para el usuario no iniciado. El binario de tcpdump en FreeBSD 7.2 soporta 36 diferentes
banderas de línea de comandos, las posibilidades ilimitadas con las expresiones de filtro, y su página de manual, proporcionando
sólo un breve resumen de todas sus opciones, es casi un 30 impresos 8.5x11 "páginas. Después de aprender
Para usarlo, usted también debe saber cómo interpretar los datos que proporciona, que puede requerir un análisis en profundidad
comprensión de los protocolos de red.

Una revisión completa de la captura de paquetes y la interpretación de los resultados está fuera del alcance de este libro. De hecho, libros enteros se han escrito sobre este tema solo. Para aquellos con sed durante más de conocimientos básicos en este ámbito, algunas recomendaciones para la lectura adicionales

Al final de este capítulo. Esta sección tiene por objeto proporcionar una introducción a este tema, y te vas con el conocimiento suficiente para solucionar problemas básicos.

25.5.1. tcpdump banderas de línea de comandos

La siguiente tabla muestra las banderas de comandos más utilizados de acuerdo con tcpdump. Cada opción se discutirá con más detalle en esta sección.

Bandera	Descripción
`-I` <*interface*>	Escuchar en <*interface*>,. Por ejemplo, `-I fxp0`
`-N`	No resolver direcciones IP usando DNS inversa.
`-W` <*filename*>	Guardar la captura en formato pcap a <nombreArchivo>, por ejemplo, `-W / tmp / wan.pcap`
`-S`	Ajustar la longitud - la cantidad de datos a ser capturados de cada cuadro
`-C` <*packets*>	Salir después de recibir un número específico de paquetes.
`-P`	No poner la interfaz en modo promiscuo.
`-V`	Verboso
`-E`	Imprimir capa de enlace de cabecera en cada línea. Muestra la fuente y la dirección MAC de destino, y Información de las etiquetas VLAN para el tráfico agregó.

Tabla 25.2. De uso común banderas tcpdump

25.5.1.1. -I bandera

La `-I` bandera especifica la interfaz en la que tcpdump va a escuchar. Puede utilizar la interfaz de FreeBSD nombre aquí, como `fxp0`,`Em0`,`rl0`, Etc

25.5.1.2. -N del pabellón

No resolver direcciones IP usando DNS inversa. Cuando esta opción no se especifica, tcpdump llevará a cabo un DNS inverso (PTR) de búsqueda para cada dirección IP. Esto genera una cantidad significativa de DNS el tráfico en las capturas que muestra grandes volúmenes de tráfico. Es posible que desee desactivar esta para evitar la adición de la carga a los servidores DNS. Yo prefiero usar siempre `-N` porque elimina el retraso entre la captura de un paquete y su pantalla que es causada por realizar la búsqueda inversa. También

Las direcciones IP suelen ser más fáciles de leer y de entender que sus registros PTR. Esa es una cuestión de preferencia personal, sin embargo, y en entornos que conozco donde sé que el PTR registros los nombres de host real de los dispositivos, que se puede ejecutar sin capturas `-N` para mostrar los nombres de host.

Otra razón para usar `-N`, Aunque nunca se debe capturar en cualquier entorno en el que se trata de de forma remota una preocupación, es si usted quiere ser "astuto". Uno de los medios de detección de captura de paquetes es en busca de picos y patrones en las búsquedas de DNS PTR.

25.5.1.3. -W bandera

tcpdump permite guardar archivos de captura en formato pcap, para su posterior análisis o análisis en otro del sistema. Esto se hace comúnmente con los productos de línea de comandos sólo como pfSense lo que el archivo puede se copian en un host que ejecute Wireshark [http://www.wireshark.org] o de otra red gráfica analizador de protocolos y revisado allí. Al guardar un archivo utilizando `-W`, Los cuadros no se que aparecen en su terminal, ya que de otro modo lo son. (Véase Sección 25.6, "Utilización de Wireshark con pfSense " sobre el uso de Wireshark con pfSense.)

25.5.1.4. -S bandera

De forma predeterminada, cuando se captura a un archivo, tcpdump sólo se graban los primeros 64 bytes de cada fotograma.

Esto es suficiente para obtener el encabezado IP y el protocolo para la mayoría de los protocolos, pero limita la utilidad de capturar archivos. Al utilizar el `-S` bandera, se puede decir tcpdump qué parte de la trama a la captura, en bytes. Esto se conoce como la longitud de complemento.

Bandera	Descripción
`-S 500`	Captura de los primeros 500 bytes de cada frame
`-S 0`	Captura de cada cuadro en su totalidad

Tabla 25.3. Ejemplos de uso de tcpdump-s

Por lo general, tendrá que usar `-S 0` cuando se captura a un archivo para su análisis en otro sistema. La única excepción a esto es escenarios en los que usted necesita para capturar una gran cantidad de tráfico a través de un período de tiempo más largo. Si conoce la información que busca está en la cabecera, se puede guardar sólo el valor predeterminado de 64 bytes de cada cuadro y obtener la información que necesitan, mientras que de manera significativa reducir el tamaño del archivo de captura resultante.

25.5.1.5. -C bandera

Puede indicar tcpdump para capturar un cierto número de fotogramas y luego la salida mediante el `-C` bandera. Ejemplo de uso: tcpdump saldrá después de capturar 100 imágenes especificando `-C 100`.

25.5.1.6. -P bandera

Normalmente, cuando la captura de tráfico con tcpdump, que pone a su interfaz de red en promiscua modo. Cuando no se ejecuta en modo promiscuo, la NIC sólo recibe marcos destinados a su propia dirección MAC, así como las direcciones de difusión y multidifusión. Cuando se enciende en modo promiscuo, la interfaz muestra todos los fotogramas en el alambre. En una red conmutada, este por lo general tiene poco impacto en su captura. En las redes en el dispositivo que se captura desde está conectado a un concentrador, utilizando `-P` pueden limitar significativamente el ruido en su captura cuando el único tráfico
de interés es que desde y hacia el sistema desde el que se captura.

25.5.1.7. -V bandera

La `-V` bandera controla el detalle, o nivel de detalle, de la salida. El uso de más "v" Opciones de rendimiento más detalle, para que pueda utilizar `-V`,`-Vs`O `-Vvv` para ver más detalle en la impresión a la consola. Esta opción no afecta a los detalles almacenados en un archivo de captura cuando se utiliza el `-W` interruptor,
sino que hará que el proceso de informar el número de paquetes capturados cada 10 segundos.

25.5.1.8. E-bandera

Normalmente tcpdump no muestra toda la información de capa de enlace. Especificar `-E` para mostrar la fuente y el destino las direcciones MAC y VLAN información de la etiqueta para el tráfico con la etiqueta 802.1q VLAN.

25.5.1.8.1. Ejemplo de captura sin-e

Esta captura muestra la salida predeterminada, que no contengan información capa de enlace.

#tcpdump-ni Em0-c 5

```
tcpdump: salida detallada suprimida, v uso-o-vs para decodificar el
protocolo completo de
escucha en Em0, enlace de tipo EN10MB (Ethernet), la captura de tamaño 96
bytes

23:18:15.830851 IP 10.0.64.210.22> 10.0.64.15.1395: P 116:232 (116) un
acuse de recibo de ganar 65.535
23:18:15.831256 IP 10.0.64.15.1395> 10.0.64.210.22:. ack 116 gana 65.299

23:18:16.006407 IP 10.0.64.15.1395> 10.0.64.210.22:. ack 232 gana 65.183
5 paquetes capturados
```

25.5.1.8.2. Ejemplo de captura con-e

Aquí puede ver la información de la capa de enlace incluido. Tenga en cuenta la fuente y las direcciones MAC de destino
además de la fuente y las direcciones IP de destino.

#tcpdump-ni Em0-e-c 5

```
tcpdump: salida detallada suprimida, v uso-o-vs para decodificar el
protocolo completo de
escucha en Em0, enlace de tipo EN10MB (Ethernet), la captura de tamaño 96
bytes




5 paquetes capturados
```

25.5.2. Filtros tcpdump

En la mayoría de servidores de seguridad, sin filtros tcpdump producirá la salida tanto que será muy difícil encontrar el tráfico de interés. Hay numerosas expresiones de filtrado disponibles que permiten a limitar el tráfico que aparecen o capturado a sólo lo que se interese

25.5.2.1. Anfitrión filtros

Para hacer un filtro para una máquina específica, anexe `de acogida` y la dirección IP con el comando tcpdump. Para filtrar
para el host 192.168.1.100 puede utilizar el siguiente comando.

#tcpdump-ni Em0 host 192.168.1.100

Que capturar todo el tráfico hacia y desde ese host. Si sólo desea capturar el tráfico que se inició por ese host, puede utilizar el `src` Directiva.

#tcpdump-ni Em0 acogida src 192.168.1.100

Del mismo modo, también puede filtrar el tráfico destinado a esa dirección IP especificando `dst`.

#tcpdump-ni Em0 dst host 192.168.1.100

25.5.2.2. Red de filtros

filtros de red le permite reducir su captura a una subred específica con el `neta` expresión.
Después de `neta`, Puede especificar un quad de puntos (*192.168.1.1*), Triple de puntos (*192.168.1*), par de puntos (*192.168*) O simplemente un número (*192*). A cuatro puntos es equivalente a especificar `de acogida`, Un triple de puntos utiliza una máscara de subred 255.255.255.0, un par de puntos utiliza 255.255.0.0, y
un número solo usa 255.0.0.0.

El comando siguiente muestra el tráfico hacia o desde cualquier equipo con una dirección IP 192.168.1.x.

#tcpdump-ni Em0 red 192.168.1

El comando siguiente es un ejemplo que captura el tráfico hacia o desde cualquier equipo con una 10.xxx dirección IP.

#tcpdump-ni Em0 neto 10

Los ejemplos se captura todo el tráfico desde o hacia la red especificada. También se puede especificar `src` o `dst` la misma que con `de acogida` filtros para capturar el tráfico sólo se inicia por o destinadas a la específicos de las redes.

#tcpdump-ni Em0 neto src 10

También es posible especificar una máscara CIDR como argumento para `neta`.

#ni tcpdump-Em0 red 172.16.0.0/12 src

25.5.2.3. Protocolo y filtros de puerto

Estrechamiento por host o una red con frecuencia no es suficiente para eliminar el tráfico innecesario de su captura. O es posible que no se preocupan por el origen o destino del tráfico, y simplemente desea capturar un determinado tipo de tráfico. En otros casos es posible que desee filtrar todo el tráfico de un tipo específico para reducir el ruido.

25.5.2.3.1. TCP y UDP puerto filtros

Para filtrar los puertos TCP y UDP se utiliza el `puerto` Directiva. Esta captura TCP y UDP el tráfico con el puerto especificado, ya sea como origen o puerto de destino. Se puede combinar con `tcp` o `udp` para especificar el protocolo, y `src` o `dst` para especificar una fuente o puerto de destino.

25.5.2.3.1.1. Capture todos tráfico HTTP

#tcpdump-ni Em0 tcp puerto 80

25.5.2.3.1.2. Capture todos los DNS de tráfico

Capture todos los DNS de tráfico (generalmente UDP, pero algunas consultas utilizar TCP).

#tcpdump-ni Em0 el puerto 53

25.5.2.3.2. Protocolo de filtros

Usted puede filtrar por protocolos específicos con el `proto` Directiva. Protocolo se pueden especificar utilizando el número de protocolo IP o uno de los nombres `icmp`,`igmp`,`igrp`,`pim`,`ah`,`esp`,`vrrp`,`udp`,

o `tcp`. Especificar `vrrp` también capturar el tráfico de CARP como el uso de dos el mismo protocolo IP número. Un uso común de la `proto` Directiva es filtrar el tráfico CARP. Debido a que el nombres normales protocolo son palabras reservadas, que debe ser escapado con una o dos barras invertidas, en función de la cáscara. El intérprete de comandos disponibles en pfSense requiere dos barras invertidas para escapar de estas nombres de protocolo. Si recibe un error de sintaxis, compruebe que el nombre del protocolo está correctamente escapado. La captura siguiente le mostrará todas las carpas y el tráfico en la VRRP `Em0` interfaz, que puede ser útil para asegurar el tráfico CARP se envían y se reciben en la interfaz especificada.

#tcpdump-ni Em0 proto \ \ vrrp

25.5.2.4. Negar un partido de filtro

Además de hacer coincidir parámetros específicos, se puede negar un partido de filtro especificando `no` frente a la expresión de filtro. Si está solucionando algo más que CARP y su latidos de multidifusión se saturan su salida de la captura, puede excluir de la siguiente manera.

**#vrrp tcpdump-ni Em0 no proto \ **

25.5.2.5. La combinación de filtros

Puede combinar cualquiera de los filtros antes mencionados con `y` o `o`. En las siguientes secciones citar algunos ejemplos.

25.5.2.5.1. Mostrar todos los HTTP tráfico hacia y desde un host

Para mostrar todo el tráfico HTTP desde el host 192.168.1.11, utilice el siguiente comando.

#puerto tcpdump-ni Em0 host 192.168.1.11 y tcp 80

25.5.2.5.2. Mostrar todos los HTTP tráfico hacia y desde múltiples hosts

Para mostrar todo el tráfico HTTP desde los hosts 192.168.1.11 y 192.168.1.15, utilice el siguiente comandos.

#tcpdump-ni Em0 anfitrión o host 192.168.1.11 192.168.1.15 y el puerto TCP 80

25.5.2.6. Filtro uso de la expresión

Las expresiones de filtro debe venir después de cada indicador de línea de comandos utilizados. Agregar cualquier banderas después de un filtro expresión resultará en un error de sintaxis.

25.5.2.6.1. Ordenación incorrecta

```
#tcpdump-ni en1 proto \\ vrrp-c 2
tcpdump: error de sintaxis
```

25.5.2.6.2. Ordenación correcta

```
#tcpdump-ni en1-c 2 proto \\ vrrp
tcpdump: salida detallada suprimida, v uso-o-vs para decodificar el
protocolo completo de
escucha en en1, enlace de tipo EN10MB (Ethernet), la captura de tamaño 96
bytes


2 paquetes capturados
80 paquetes recibidos por el filtro
0 paquetes perdidos por el kernel
```

25.5.2.7. Más información sobre Filtros

Esta sección cubre las más utilizadas expresiones de filtro tcpdump, y cubre, probablemente toda la sintaxis que necesita. Sin embargo, esto apenas roza la superficie de las posibilidades. No Son muchos los documentos en la web que cubren tcpdump en general y específicamente de filtrado. Ver Sección 25.8, "Referencias adicionales" al final de este capítulo para obtener enlaces a referencias adicionales sobre el tema.

25.5.3. Solución de problemas prácticos ejemplos

Esta sección detalla un enfoque preferido por nosotros para solucionar algunos problemas específicos. Hay múltiples maneras de abordar cualquier problema, pero la captura de paquetes raramente puede ser vencido por su eficacia. Examinar el tráfico en el cable proporciona un nivel de visibilidad de lo que es realmente sucediendo en la red

25.5.3.1. Puerto no de trabajo previsto

Usted acaba de agregar un puerto para la conexión, y están tratando de usarlo desde un host en Internet, pero los dados no.

Los pasos de solución de problemas descritos en Sección 7.9.1, "Puerto Adelante Solución de problemas" ofrece una manera de abordar esto, pero a veces captura de paquetes es la única manera más fácil o para encontrar la fuente del problema.

25.5.3.1.1. Empezar desde WAN

En primer lugar usted necesita para asegurarse de que el tráfico está llegando a su interfaz WAN. Inicie una sesión de tcpdump en su interfaz WAN, y velar por el tráfico de venir pulg

#tcpdump-ni vlan0 puerto TCP 5900

```
tcpdump: salida detallada suprimida, v uso-o-vs para decodificar el
protocolo completo de
escucha en vlan0, enlace de tipo EN10MB (Ethernet), la captura de tamaño 96
bytes
```

En este caso, vemos un paquete de llegar de la WAN, por lo que lo está haciendo tan lejos. Tenga en cuenta que el
primera parte del protocolo de enlace TCP, un paquete con sólo SYN (la S se muestra), nos está alcanzando. Si el
puerto de avanzar es trabajar podrás ver un paquete SYN ACK en respuesta al SYN. Sin retorno
tráfico visible, podría ser una regla de firewall o el sistema de destino puede ser inalcanzable (apagado, no escuchando en el puerto especificado, firewall de host bloqueando el tráfico, etc.)

25.5.3.1.2. Compruebe la interfaz interna

El paso siguiente sería ejecutar una sesión de tcpdump en la interfaz interna asociada con la
puerto hacia adelante.

#tcpdump-ni fxp0 puerto TCP 5900

```
tcpdump: salida detallada suprimida, v uso-o-vs para decodificar el protocolo
completo de
escucha en fxp0, enlace de tipo EN10MB (Ethernet), la captura de tamaño 96
bytes
```

Mirando el tráfico interno, vemos que la conexión se fue dentro de la interfaz, y el
dirección IP local fue traducido correctamente. Si esta dirección local coincide con lo que se esperaba, a continuación,
tanto en el puerto para la conexión y la regla de firewall están funcionando correctamente, y la conectividad a los locales
PC debe ser confirmada por otros medios. Si no ve salida alguna, entonces no es un problema
con la regla de firewall o el puerto para la conexión puede haber sido mal definido. Para este ejemplo,
Me había desconectado el PC.

25.5.3.2. túnel IPsec no se conecta

Debido a tcpdump tiene un cierto conocimiento de los protocolos utilizados, puede ser muy útil para
pelearse con los problemas con los túneles IPsec. Los ejemplos próximos mostrar el error de cómo ciertos
condiciones se pueden presentar cuando la vigilancia con tcpdump. Los registros de IPsec puede ser
más útil en algunos casos, pero esto se puede confirmar lo que en realidad es ser visto por el router. Por
el tráfico cifrado como IPsec, la captura de paquetes del tráfico es de menor valor ya que no puede
examinar la capacidad de carga de los paquetes capturados sin parámetros adicionales, pero es útil
determinar si el tráfico desde el extremo remoto está llegando a su servidor de seguridad y que las fases completas.

Este primer túnel tiene un punto inalcanzable:

#tcpdump-ni vr0 host 192.168.10.6

```
tcpdump: salida detallada suprimida, v uso-o-vs para decodificar el
protocolo completo de
escucha en vr0, enlace de tipo EN10MB (Ethernet), la captura de tamaño 96
bytes

19:11:11.542976 IP 192.168.10.5.500> 192.168.10.6.500: ISAKMP: la fase 1
que agr
19:11:21.544644 IP 192.168.10.5.500> 192.168.10.6.500: ISAKMP: la fase 1
que agr
```

Este intento de túnel tiene una PSK no coincidentes, observe la forma en que los intentos de pasar a la fase 2,

pero luego

se detiene:

#tcpdump-ni vr0 host 192.168.10.6

```
tcpdump: salida detallada suprimida, v uso-o-vs para decodificar el protocolo
completo de
escucha en vr0, enlace de tipo EN10MB (Ethernet), la captura de tamaño 96
bytes
19:15:05.566352 IP 192.168.10.5.500> 192.168.10.6.500: ISAKMP: la fase 1
que agr
19:15:05.623288 IP 192.168.10.6.500> 192.168.10.5.500: ISAKMP: fase 1 agr I
```

Ahora la fase 1 está bien, pero hay un desajuste en la fase 2 de la información. En repetidas ocasiones se intenta la fase 2 de tráfico, pero no verá ningún tráfico en el túnel.

#tcpdump-ni vr0 host 192.168.10.6

```
tcpdump: salida detallada suprimida, v uso-o-vs para decodificar el protocolo
completo de
escucha en vr0, enlace de tipo EN10MB (Ethernet), la captura de tamaño 96
bytes
19:17:18.447952 IP 192.168.10.5.500> 192.168.10.6.500: ISAKMP: la fase 1
que agr
19:17:18.490278 IP 192.168.10.6.500> 192.168.10.5.500: ISAKMP: fase 1 agr I
19:17:18.520149 IP 192.168.10.5.500> 192.168.10.6.500: ISAKMP: la fase 1
que agr
```

Finalmente, después de un túnel en pleno funcionamiento con el tráfico en ambos sentidos la Fase 1 y Fase 2 han terminado!

#tcpdump-ni vr1 host 192.168.10.6

```
tcpdump: salida detallada suprimida, v uso-o-vs para decodificar el protocolo
completo de
escucha en VR1, enlace de tipo EN10MB (Ethernet), la captura de tamaño 96
```

```
bytes
21:50:11.238263 IP 192.168.10.5.500> 192.168.10.6.500: ISAKMP: la fase 1
que agr
21:50:11.713364 IP 192.168.10.6.500> 192.168.10.5.500: ISAKMP: fase 1 agr I
21:50:11.799162 IP 192.168.10.5.500> 192.168.10.6.500: ISAKMP: la fase 1
que agr
```

25.5.3.3. El tráfico que atraviesa un túnel IPSec

Con algunos ajustes adicionales para inicializar el proceso, también puede ver el tráfico que atraviesa su IPsec túneles. Esto puede ayudar a determinar si el tráfico está tratando de llegar al otro extremo utilizando el túnel.
En versiones anteriores a la liberación 1.2.3, antes de tcpdump funciona en la interfaz IPsec que había para establecer dos variables sysctl que el control de lo que es visible a tcpdump. Si está utilizando versión 1.2.3 o más reciente, tcpdump funcionará sin ninguna manipulación adicional.

En el siguiente ejemplo, una máquina a un lado del túnel con éxito el envío de un eco ICMP petición (ping) a la cara oculta, y recibir respuestas.

```
#net.enc.out.ipsec_bpf_mask sysctl-w = 0x00000001
net.enc.out.ipsec_bpf_mask: 0000000000 -> 0x00000001
#net.enc.in.ipsec_bpf_mask sysctl-w = 0x00000001
net.enc.in.ipsec_bpf_mask: 0000000000 -> 0x00000001
#tcpdump-ni enc0
ADVERTENCIA:: tcpdump enc0: sin dirección IPv4 asignada
tcpdump: salida detallada suprimida, v uso-o-vs para decodificar el
protocolo completo de
escucha en enc0, enlace de tipo ENC (OpenBSD encapsulado IP), el tamaño de
captura de 96 bytes
22:09:18.331506 (auténtico, confidencial): 0x09bf945f SPI:
                IP 10.0.20.1> 10.0.30.1:
                Solicitud de eco ICMP, id 14140, ss 0, longitud 64
22:09:18.334777 (auténtico, confidencial): SPI 0x0a6f9257:
              IP 192.168.10.6> 192.168.10.5: IP 10.0.30.1> 10.0.20.1:
              Respuesta de eco ICMP, id 14140, ss 0, longitud 64 (ipip-proto-4)
22:09:19.336613 (confidencial auténtico): 0x09bf945f SPI:
                IP 10.0.20.1> 10.0.30.1:
                Solicitud de eco ICMP, id 14140, ss 1, longitud 64
22:09:19.339590 (auténtico, confidencial): SPI 0x0a6f9257:
              IP 192.168.10.6> 192.168.10.5: IP 10.0.30.1> 10.0.20.1:
              Respuesta de eco ICMP, id 14140, ss 1, longitud 64 (ipip-proto-4)
```

Si el tráfico no estaba debidamente entrar en el túnel, no se ve ninguna salida. Si hay un firewall o asunto interno de enrutamiento en el lado opuesto, puede ver el tráfico que sale, pero devolver nada.

25.5.3.4. Solución de problemas de NAT Saliente

Para entornos complejos donde Avanzada de salida NAT es necesario, tcpdump puede ser de gran asistencia en la solución de problemas de la configuración NAT de salida. Una buena captura de usar es Buscar para el tráfico con direcciones IP privadas en su interfaz WAN, como todo lo que ve en su WAN debe NAT a una IP pública. La captura siguiente mostrará todo el tráfico con RFC 1.918 direcciones IP como origen o destino. Esto le mostrará todo el tráfico que no se pongan en venta una de las reglas NAT de salida, proporcionando información para ayudar a revisar su salida NAT de configuración para encontrar el problema.

#tcpdump-ni Em0 neta de 10 o neto 192,168 o red 172.16.0.0/12

25.6. Uso de Wireshark con pfSense

Wireshark, antes conocido como Ethereal, es un análisis de protocolo interfaz gráfica de usuario y la herramienta de captura de paquetes que se puede utilizar para ver y capturar el tráfico al igual que tcpdump. Es un software de código abierto, libre disponible en http://www.wireshark.org/. También puede utilizarse para analizar archivos de captura generados por el pfSense WebGUI, tcpdump, Ethereal, o cualquier otro software que escribe los archivos en la norma pcap formato de archivo.

25.6.1. Visualización de archivos de paquetes de captura

Para ver un archivo de captura de Wireshark, inicie el programa y luego ir a Archivo → Abrir. Busque el archivo de captura, a continuación, haga clic en el botón Abrir. También puede hacer doble clic sobre cualquier archivo con un `. Pcap` de extensión en Windows y OS X con la configuración por defecto tras la instalación de Wireshark. Usted verá una pantalla similar a la Figura 25.2, "Captura de Wireshark Ver" en la que los datos de la captura archivo se muestra.

Como se observa en la Figura 25.2, "Captura de Wireshark Ver", una lista que resume los paquetes en la captura archivo se mostrará en la lista de los mejores, con un paquete por la línea. Si hay demasiados, puede filtrar los resultados mediante el cuadro de filtro en la barra de herramientas. Al hacer clic en un paquete, los cuadros inferiores se mostrar los detalles de lo que contenía en su interior. El primer panel inferior muestra un desglose de la estructura de los paquetes, y cada uno de estos elementos se puede ampliar para más detalles. Si el paquete es de un protocolo de apoyo, en algunos casos puede interpretar los datos y mostrar los detalles más. La panel inferior muestra una representación hexadecimal y ASCII de los datos contenidos en el paquete. Viendo la captura de esta manera, es fácil ver el flujo de tráfico con detalle tanto o tan poco como según sea necesario.

25.6.2. Wireshark Herramientas de análisis

Mientras que algunos problemas se requieren amplios conocimientos de cómo los protocolos subyacentes función, las herramientas de análisis integradas en Wireshark que ayuda a disminuir la necesidad de muchos protocolos. Bajo
Analizar las estadísticas y los menús, encontrará algunas opciones que automatizan algunos de los análisis y proporcionar resumen de las opiniones de lo que figura en la captura. El Experto en Información de opciones Analizar el menú mostrará una lista de errores, advertencias y notas que figuran las conversaciones de la red en la captura.

Nota

Que comúnmente se ven errores en Wireshark para las sumas de comprobación incorrecta. Esto es porque la mayoría de tarjetas de red añadir la suma de comprobación en el hardware directamente antes de ponerlo en la
alambre. Esta es la única excepción a la nota anterior diciendo lo que usted ve en un paquete captura es lo que está en el alambre. El tráfico enviado desde el sistema donde la captura se toma tendrá las sumas de comprobación incorrecta en el que se realizan en el hardware, aunque el tráfico que viene desde un sistema remoto debe tener siempre las sumas de comprobación correcta. Puede desactivar la comprobación de descarga para asegurarse de que están viendo el tráfico como el anfitrión es
ponerlo en el cable, aunque por lo general esto es algo que simplemente ignoran. En caso de usted necesita para verificar las sumas de comprobación, lo normal es que quieres capturar el tráfico de otro sistema utilizando una red grifo o interruptor de puerto span.

El menú de la telefonía es un ejemplo de análisis automatizado de Wireshark puede realizar para hacer es fácil ver los problemas con VoIP. En este caso particular, el tráfico de VoIP se atraviesa un MPLS Circuito con routers WAN del proveedor conectado a una interfaz OPT de pfSense en ambos lados. Una captura de la interfaz de TPO en el extremo de iniciar mostró ninguna pérdida, lo que indica el tráfico era de ser enviado al router del proveedor, pero la interfaz opcional en el extremo opuesto mostraron considerables la pérdida de paquetes en una dirección cuando varias llamadas al mismo tiempo se activa. Estos paquetes de captura ayudó a convencer al distribuidor de un problema en su red, y encontró que fija y una calidad de servicio problema de configuración de su lado. Al ver una captura de paquetes que contiene tráfico de RTP, haga clic en **Telefonía**,**RTP**,**Mostrar todas las corrientes** para ver esta pantalla.

Src IP addr	Src port	Dest IP addr	Dest port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter (ms)	Mean Jitter (ms)	Pb?
10	13114	192	2244	0x63B69143	ITU-T G.711 PCMU	2103	0 (0.0%)	20.07	0.12	0.01	X
192.1	2244	1	13114	0x6F1D173B	ITU-T G.711 PCMU	1646	477 (22.5%)	179.89	51.24	1.84	X
10	11224	192	2268	[illegible]	ITU-T G.711 PCMU	1321	0 (0.0%)	99.99	5.03	0.07	X
192.1	2268	1	11224	0x6C5B26A1	ITU-T G.711 PCMU	879	460 (34.4%)	340.79	49.96	2.67	X
10	17924	192	2242	0x393CBA89	ITU-T G.711 PCMU	480	0 (0.0%)	20.04	0.15	0.01	X
192.1	2242	1	17924	0x6177246E	ITU-T G.711 PCMU	133	366 (73.3%)	339.79	71.38	9.17	X

Figura 25.3. Wireshark Análisis de RTP

25.6.3. Remoto en tiempo real de captura

Desde un host UNIX que ha Wireshark disponibles, puede ejecutar una captura en tiempo real a distancia por reorientación de la salida de una sesión SSH. Esto ha sido probado y se sabe que funcionan en FreeBSD y Ubuntu.

Con el fin de utilizar esta técnica, SSH debe estar habilitado en el sistema de pfSense y que usted necesita utilizar una clave SSH (véase Sección 4.5.2, "Secure Shell (SSH)"). La primera clave se debe cargar en ssh-agent o generados sin una contraseña, porque la redirección no se le permitirá entrar en una contraseña. Usar ssh-agent es muy recomendable, ya que cualquier clave sin una palabra de paso es muy inseguridad.

Antes de intentar esta técnica, asegúrese de que puede conectarse a su router utilizando pfSense una clave SSH sin necesidad de teclear la contraseña. La primera vez que se conecte, se le le pide que guarde la clave de host, por lo que también debe hacerse antes de intentar iniciar Wireshark. Usted puede comenzar a ssh-agent desde una ventana de terminal o depósito de este modo:

#eval `ssh-agent»
```
Agente pid 29047
```
#ssh-add
```
Introduzca contraseña para / home / jim / .ssh / id_rsa:
Identidad agregó: / home / jim / .ssh / id_rsa (/ home / jim / .ssh /
id_rsa)
```

A continuación, iniciar una sesión SSH, como de costumbre:

#ssh root *@192.168.1.1*
```
La autenticidad de host '192 .168.1.1 (192.168.1.1) no puede ser
establecida.
huella digital de claves DSA es 9e: c0: b0: 5a: b9: 9b: f4: ec: 7f: 1d: 8a:
2d: 4a: 49:01:1 B.
¿Está seguro que desea continuar la conexión (sí / no)? sí
Advertencia: Permanentemente agregó .168.1.1 '192 '(DSA) a la lista de hosts
conocidos.

*** Bienvenidos a pfSense-1.2.3 de pfSense ExCo-rtr ***
[...]
```

Después de haber confirmado que la conexión SSH funciona, inicie la captura remota de la siguiente manera:

#Wireshark-k-i <(ssh root *@192.168.1.1* tcpdump-i *vr0* -U-w - no el puerto TCP 22)

Cuando la parte de la dirección IP es la dirección de su sistema de pfSense. El "**no tcp puerto 22**" parte se excluye el tráfico de su sesión de SSH, que de lo contrario va a tapar la salida de la captura. Lo anterior está escrito en la "fiesta al estilo de" la sintaxis, pero puede funcionar con otros shells. Usted puede ajustar el

tcpdump argumentos para la interfaz, y agregar expresiones adicionales, pero el `-U` y `-W -` se necesarias para que se escribe la salida a stdout, y escribe cada paquete que llega.

Véase también la Configuración de captura / Tubos [http://wiki.wireshark.org/CaptureSetup/Pipespágina] en el Wireshark wiki de otras técnicas relacionadas.

25.7. Texto sin formato Protocolo de depuración con flujo TCP

flujo TCP es otro paquete similar a tcpdump que le permitirá ver el contenido del texto paquetes en tiempo real en lugar de la cabecera del paquete y la información de transporte. flujo TCP utiliza sintaxis similar a tcpdump, con una notable excepción: Por defecto se escribe el texto del paquete de archivos en lugar de la consola. Para ver la salida en la consola, utilice la `-C` opción.

Si bien no está disponible en una instalación de pfSense stock, flujo TCP se puede agregar desde el símbolo del línea mediante la instalación del paquete de FreeBSD. Se trata de un pequeño paquete con ninguna dependencia, lo que la instalación no debe dañar el sistema. Para instalar flujo TCP en pfSense, ejecute el comando siguiente desde una concha pfSense:

#pkg_add-r flujo TCP
#refrito

Si estás teniendo problemas con una conexión FTP de una red LAN, usted puede supervisar el control canal en el lado WAN, así:

#flujo TCP-i-c vlan0 172.17.11.9 host y el puerto 21

```
flujo TCP [13899]: escucha en vlan0

010.000.073.005.23747-172.017.011.009.00021: fieldtech USUARIO
172.017.011.009.00021-010.000.073.005.23747: 331 Por favor, especifique la
contraseña.
010.000.073.005.23747-172.017.011.009.00021: PASO abc123
172.017.011.009.00021-010.000.073.005.23747: 230 Nombre de éxito.
010.000.073.005.23747-172.017.011.009.00021: PUERTO 10,0,73,5,194,240

010.000.073.005.23747-172.017.011.009.00021: NLST
172.017.011.009.00021-010.000.073.005.23747: 150 Aquí viene la lista de
directorios.
172.017.011.009.00021-010.000.073.005.23747: 226 Directorio de enviar en
Aceptar.
```

Como se puede ver en esta salida, es fácil de controlar el flujo de protocolos de control de texto sin formato como FTP. Usted puede ver los comandos y la salida en ambas direcciones, y lo más importante que puede ver que el proxy FTP hizo su trabajo y traducido el comando PORT al utilizar la IP WAN dirección de pfSense lugar, lo que permite el modo activo para que funcione correctamente. Si en lugar de ver la

dirección IP que aparece en el comando PORT, usted sabría que comprobar la configuración de proxy FTP o cambiar al modo PASV en el cliente.

Después de haber flujo TCP todo ha sido muy útil en mi experiencia, y hace un buen complemento tcpdump para cuando se desea centrarse en el contenido de los paquetes en lugar de su estructura.

25.8. Referencias adicionales

Esta captura sólo roza la superficie de las posibilidades de captura de paquetes. Éstos son algunos de recursos adicionales para los interesados en un conocimiento más a fondo. Captura de paquetes es una muy potente medio de solución de problemas de conectividad de red, y encontrarán su habilidades de solución de problemas mucho mejor si usted aprende las posibilidades con mayor profundidad.

Redes de Computadoras: Protocolos de Internet en Acción [Http://www.amazon.com/gp/product/0471661864?
es decir, = UTF8 & tag = pfSense-20 y linkCode = AS2 y campo = 1789 = 9325 y creativa y creativeASIN = 0471661864]
por Jeanna Matthews

Tcpdump Filtros [Http://www.whitehats.ca/main/members/Malik/malik_tcpdump_filters/] Malik_tcpdump_filters.html por Jamie francés

Tcpdump Filtros avanzados [http://acs.lbl.gov/ ~ jason / tcpdump_advanced_filters.txt] Por Sebastien Wains

Tcpdump Filtros [Http://www.cs.ucr.edu/ ~ marios / tcpdump.pdf etéreo] de Marios Iliofotou

FreeBSD Hombre Page de tcpdump [http://www.freebsd.org/cgi/man.cgi?query = tcpdump y propósito = 0 & sektion = 0 & manpath = FreeBSD 7.2-RELEASE & format = html]

Apéndice A. Guía de menús

Esta guía de las opciones del menú estándar disponibles en pfSense debería ayudar a identificar rápidamente con el fin de una opción de menú determinado, y se refieren a los lugares en el libro, donde las opciones son tratará con mayor detalle.

Los paquetes se pueden agregar elementos a cualquier menú, así que usted puede tener que ver todos ellos para localizar el menú
opciones para todos los paquetes instalados. Normalmente, los paquetes de instalación en el menú Servicios, pero no muchos de los que ocupan los otros menús también.

A.1. Sistema de

El menú Sistema contiene opciones para el propio sistema, generales y opciones avanzadas, el firmware actualizaciones, paquetes adicionales, y las rutas estáticas.

Avanzada	Configuración avanzada del sistema para el servidor de seguridad, hardware, SSH, SSL certificados, y muchos otros. Ver Sección 4.5, "Configuración avanzada Opciones ".
Firmware	Actualizar o cambiar la versión del firmware del sistema. (Por ejemplo, actualización de pfSense 1.2.2 a 1.2.3). Ver Sección 3.7.3.1, "Aumentar el uso de la WebGUI".
Configuración General	Configuración general del sistema, como el nombre de host, dominio, servidores DNS, etc Ver Sección 4.4, "Opciones de configuración generales".
Paquetes	Adicional de software add-ons para pfSense para ampliar su funcionalidad. Ver Capítulo 23, Paquetes.
Asistente de configuración	El asistente de configuración le guía a través del proceso de realización de la base la configuración inicial. Ver Sección 4.2, "Asistente de configuración".
Rutas estáticas	Las rutas estáticas que pfSense saber cómo llegar a las subredes no locales a través de local routers accesible. Ver Sección 8.1, "rutas estáticas".

A.2. Interfaces

El menú tiene elementos de interfaces para las interfaces de asignación, y un elemento para cada interfaz asignado.

WAN y LAN aparecerá siempre, mientras que otros aparecen como OPTX o el nombre que han sido determinado.

(Asignar)	Asignar interfaces a las funciones de lógica (por ejemplo, LAN, WAN, OPT), y crear o mantener las VLAN. Ver Sección 4.3.1, "Asignar interfaces " y Capítulo 10, LAN virtuales (VLAN).
<title> </ WAN Title>	Configurar la interfaz WAN. Ver Sección 4.3.2, "WAN Interface ".
<title> <LAN / Title>	Configurar la interfaz LAN. Ver Sección 4.3.3, "LAN Interface ".
<title> OPTX </ Title>	Configure las interfaces opcionales adicionales. Ver Sección 4.3.3, "interfaz de LAN".

A.3. Servidor de seguridad

Los elementos de menú para la configuración de Firewall de diversas partes de las reglas del firewall, las reglas NAT, y su estructura de soporte.

<title> Alias </ Title>	Permite gestionar las colecciones de direcciones IP, redes, o los puertos para simplificar la creación de reglas y de gestión. Ver Sección 6.3, "Alias".
<title> </ NAT Title>	Mantener NAT reglas que controlan el puerto hacia delante, NAT 1:1, NAT y el comportamiento de salida. Ver Capítulo 7, Red Traducción de direcciones.
<title> Reglas </ Title>	Configurar reglas de firewall. Debe haber una ficha en este pantalla para cada interfaz configurada. Ver Sección 6.2, "Introducción a la pantalla de Reglas de cortafuegos".
<title> Listas </ Title>	Configuración basada en los calendarios previstos regla. Ver Sección 6.9, "Tiempo Reglas de base ".
<title> Tráfico Shaper </ Title>	Configurar de tráfico / Calidad de Servicio (QoS) ajustes. Ver Capítulo 16, Traffic Shaper.
<title> Virtual IP </ Title>	Configurar direcciones IP virtuales que permiten manejar pfSense el tráfico de más de una dirección IP por cada interfaz, general de las reglas NAT o de conmutación por error CARP. Ver Sección 6.8, "IPs virtuales".

A.4. Servicios

El menú Servicios contiene los elementos que le permiten controlar los diferentes servicios prestados por los demonios ejecutándose en pfSense. Ver Capítulo 21, Servicios.

Portal cautivo	Controla el Portal Cautivo servicio que te permite dirigir a los usuarios a una primera web para la autenticación antes de permitir el acceso a Internet de la página. Ver Capítulo 19, Portal Cautivo.
DNS forwarder	Configura pfSense incorporada en el almacenamiento en caché de resolución DNS. Ver Sección 21.3, "DNS Forwarder".
Relé DHCP	Configura el servicio de retransmisión de DHCP que proxy peticiones DHCP de un segmento de red a otro. Ver Sección 21.2, "DHCP Relay".
Servidor DHCP	Configura el servicio DHCP que proporciona dirección IP automática configuración para los clientes en las interfaces internas. Ver Sección 21.1, "DHCP Servidor ".
DNS dinámico	Configura los servicios de DNS dinámico (DynDNS), que se actualizará un mando a distancia sistema cuando este router WAN de pfSense dirección IP ha cambiado. Ver Sección 21.4, "DNS dinámica".
Equilibrador de carga	Configura el equilibrador de carga, que en modo Gateway equilibrio conexiones de salida a través de múltiples enlaces WAN, o en modo de servidor se equilibrio de las conexiones entrantes a través de servidores múltiples. Ver Capítulo 17, Servidor de equilibrio de carga.
OLSR	Configura Optimizado estado de los vínculos de enrutamiento, una malla de enlace dinámico demonio, que soporta redes inalámbricas de malla.
Servidor PPPoE	Configurar el servidor PPPoE que permiten pfSense para aceptar y autenticar las conexiones de los clientes PPPoE. Ver Sección 21.9, "PPPoE Servidor ".
RIP	Configura el demonio de enrutamiento RIP. Ver Sección 8.3.1, "RIP".
SNMP	Configura el Simple Network Management Protocol (SNMP) demonio para permitir la recolección de la red basado en las estadísticas de este router. Ver Sección 21.5, "SNMP".
UPnP	Configurar el Universal Plug and Play (UPnP) que puede configurar automáticamente las reglas de NAT y firewall para los dispositivos que compatibles con el estándar UPnP. Ver Sección 21.6, "UPnP".

OpenNTPD	Configurar el demonio del servidor de tiempo de red Protocolo. Ver Sección 21.7, "OpenNTPD".
Wake on LAN	Configurar Wake on LAN servicios que le permiten despertar remotamente cliente de acceso desde el sistema de pfSense PC. Ver Sección 21.8, "Wake on LAN ".

A.5. VPN

El menú VPN contiene elementos relacionados con las redes privadas virtuales (VPN), incluyendo IPSec, OpenVPN y PPTP. Ver Capítulo 12, Redes privadas virtuales.

IPsec	Configuración de túneles VPN IPsec, IPsec opciones móviles y los usuarios, y los certificados. Ver Capítulo 13, IPsec.
OpenVPN	OpenVPN configurar servidores y clientes, así como la configuración específica del cliente. Ver Capítulo 15, OpenVPN.
PPTP	Configurar PPTP servicios y usuarios, o el relé. Ver Capítulo 14, PPTP VPN.

A.6. Condición Jurídica y Social

El menú Estado le permite comprobar el estado de varios componentes del sistema y servicios, así como ver los registros.

Portal Cautivo	Cuando Portal Cautivo está habilitado, puede ver el estado del usuario. Ver Capítulo 19, Portal Cautivo.
CARP (failover)	Ver el estado de CARP direcciones IP en este sistema. Mostrará MASTER / estado del respaldo. Ver Sección 20.6.1, "CARP Compruebe estado ".
DHCP arrendamientos	Ver una lista de todas las concesiones DHCP asignada por el router. Usted También puede eliminar los arrendamientos en línea, enviar Wake on LAN a las solicitudes sistemas en línea, o crear arrendamientos estática de las entradas actuales. Ver Sección 21.1.3, "Arrendamientos".
Filtro Actualizar estado	

Muestra el estado de los filtros de recarga peticiones que son (o fueron) pendientes. El filtro se vuelve a cargar cada vez que se aplican los cambios.

Si no hay cambios se han hecho, esta pantalla sólo debe informar que una actualización se ha completado.

Interfaces	Le permite ver el estado del hardware de las interfaces de red, equivale a utilizar ifconfig en la consola. Ver Sección 22.3, "Estado de la interfaz".
IPsec	Puntos de vista el estado de cualquier configurar túneles IPsec. Ver Capítulo 13, IPsec.
Equilibrador de carga	Puntos de vista el estado de las piscinas del equilibrador de carga. Para una carga de puerta de enlace de equilibrio, ver Sección 11.9.1, "Prueba de conmutación por error". Para el servidor balanceo de carga véase Sección 17.2.5, "Visualización de equilibrador de carga estado ".
Paquete de registros	Ver los registros de determinados paquetes de apoyo.
Colas	Ver el estado de las colas de tráfico. Ver Sección 16.6, "Monitoreo de las colas".
RRD Gráficos	Ver un gráfico de datos para las estadísticas del sistema, tales como ancho de banda utilizado, uso de la CPU, los estados de firewall, y así sucesivamente. Ver Sección 22.5, "RRD Gráficos ".
Servicios	Monitorear el estado de los servicios del sistema y el paquete y / o servicios. Ver Sección 22.4, "Estado del servicio".
Sistema de	Un atajo de vuelta a la página principal del router que pfSense muestra información general del sistema. Ver Sección 22.2, "Sistema de Condición Jurídica y Social ".
Los registros del sistema	Ver los registros del sistema y los servicios del sistema como el firewall, DHCP, VPN, etc Ver Sección 22.1, "Sistema de Registros".
Tráfico gráfica	Ver un gráfico dinámico en tiempo real el tráfico de SVG basada en una interfaz. Ver Sección 22.7, "los gráficos de tráfico".
UPnP	Ver una lista de los delanteros puerto activo UPnP. Ver Sección 21.6, "UPnP".
Wi-fi	Ver una lista de todas las redes inalámbricas disponibles en la actualidad en el rango. Ver Sección 18.2.4, "Listado inalámbrica disponible redes y la intensidad de la señal ".

A.7. Diagnóstico

Elementos en el menú Diagnósticos realizar diversas tareas de diagnóstico y administrativos.

Tablas ARP	Ver una lista de los sistemas como se ve a nivel local por el router. La lista incluye una dirección IP, dirección MAC, nombre de host, y la interfaz de la que el sistema fue visto.
Backup / Restore	Copia de seguridad y restaurar archivos de configuración. Ver Sección 5.2, "Realización de Copias de seguridad en la WebGUI ", Sección 5.5.1, "Restauración de la WebGUI ", Y Sección 5.5.2, "Restauración de la Historia de configuración".
Símbolo del sistema	Ejecutar comandos de shell o el código de PHP, y carga y descarga de archivos el sistema de pfSense. Utilice con precaución.
Editar archivo	Editar un archivo en el sistema de pfSense.
valores predeterminados de fábrica	Restablece la configuración por defecto. Tenga en cuenta, sin embargo, que esta no altera el sistema de archivos o desinstalar los paquetes, sólo los cambios ajustes de configuración.
Detener el sistema	Apague el router y desconectar la alimentación cuando sea posible.
NanoBSD	Sólo visible en la NanoBSD (integrado) de la plataforma. Permite la clonación de la división de trabajo sobre la rebanada de suplentes, y elegir cuál de ellos debe usarse para arrancar el router.
Ping	Enviar tres peticiones de eco ICMP a una dirección IP, enviado a través de un elegido interfaz. No es compatible con multi-Wan.
Reinicio del sistema	Reinicie el router pfSense. Dependiendo del hardware, esto podría tardar varios minutos.
Rutas	Muestra el contenido de la tabla de enrutamiento del sistema. Ver Sección 8.4.1, "Rutas de visión".
Estados	Ver los estados de firewall activo. Ver Sección 22.6.1, "Viendo en la WebGUI".
Trazado	Trazar la ruta que toman los paquetes entre el router y un pfSense sistema remoto. Ver Sección 8.4.2, "Utilización de traceroute".
Captura de paquetes	Realizar una captura de paquetes para inspeccionar el tráfico, a continuación, ver o descargar los resultados. Ver Sección 25.4, "Paquete de Captura de la WebGUI".

Índice

Símbolos

Un

B

C

D

E

I

K

L

M

N

Q

R

S

T

U

V

W

X