pfSense: The Definitive Guide

La guía definitiva para el pfSense abierto Fuente Firewall y Router Distribución

Christopher M. Buechler
Jim Pingle

pfSense: The Definitive Guide: La guía definitiva para el pfSense Abra Firewall Router Fuente y Distribución

por Christopher M. Buechler y Jim Pingle

Sobre la base de pfSense Versión 2.1

Fecha de publicación 2012

Abstracto

La guía oficial para la distribución de cortafuegos de código abierto pfSense.

Tabla de contenidos

Prefacio xxiv
Prefacio xxvi
Autores xxvi
Chris Buechler xxvi
Jim Pingle xxvii
Agradecimientos xxvii
Diseño del libro de la cubierta xxvii
pfSense Desarrolladores xxvii
Agradecimientos personales xxviii
Revisores xxviii
Feedback xxix
Convenciones tipográficas xxix
1. Introducción 1
El inicio del proyecto 1
¿Qué significa para pfSense / media? 1
¿Por qué FreeBSD? 1
Soporte inalámbrico 1
Rendimiento de la red 2
La familiaridad y la facilidad de tenedor 2
Alternativa Soporte del sistema operativo 2
Los despliegues comunes 2
Perímetro Firewall 2
LAN o WAN Router 2
Punto de acceso inalámbrico 3
Electrodomésticos propósito especial 3
Versiones 4
2.1 Release 4
2.0.1 Release 4
2.0 Release 4
1.2.3 Release 4
1.2, 1.2.1, 1.2.2 Releases 4
1.0 Release 5
Estrenos de instantáneas 5
Plataformas 5
Live CD (incluyendo la imagen memstick USB) 5
Instalación completa 5
Embedded 5
Interfaz de denominación Terminología 6
LAN 6
WAN 7
OPT 7
OPT WAN 7
DMZ 7
FreeBSD nombramiento interfaz 7
Búsqueda de información y Obtención de ayuda 7
Búsqueda de información 7
Obtención de ayuda 8
2. Redes Conceptos 9
Entender las direcciones IP públicas y privadas 9
Direcciones IP privadas 9
Las direcciones IP públicas 10
Conceptos subredes IP 10
Dirección IP, de subred y la puerta de enlace de configuración 10
La comprensión de subred CIDR Máscara Notación 10
Entonces, ¿dónde estas cifras CIDR provienen de todos modos? 11

CIDR Summarization 12
Encontrar a una red CIDR juego 13
Broadcast Dominios 13
IPv6 13
Lo esencial 13
Firewall y VPN Preocupaciones 13
Requisitos 14
Tipos IPv6 WAN 14
Formato de dirección 14
Vecino Discovery 14
Anuncios de enrutador 14
Dirección Asignación 14
IPv6 y pfSense 14
Conexión con un Service Broker Túnel 14
3. Hardware 15
Compatibilidad de hardware 15
Adaptadores de red 15
Requisitos mínimos de hardware 16
Requisitos Base 16
Requisitos Específicos de la Plataforma 16
Selección de hardware 16
La prevención de los dolores de cabeza de hardware 16
Hardware acerca Orientación 17
Throughput Consideraciones 17
Característica Consideraciones 19
4. Instalación y actualización 21
Descarga de pfSense 21
Verificación de la integridad de la descarga 21
Instalación completa 22
Preparación de la CD 22
Arrancar el CD 23
Asignación Interfaces 24
Instalación de la unidad de disco duro 25
Instalación de Embedded 27
Instalación en Windows Embedded 27
Instalación en Linux Embedded 29
Instalación Incrustado en FreeBSD 29
Instalación Incrustado en Mac OS X 30
Finalización de la instalación Embedded 31
Técnicas de instalación alternativos 32
Instalación con unidad en una máquina diferente 32
Instalación completa de VMware con redirección USB 33
Instalación Incrustado en VMware con ..... redirección USB 34
On-the-fly imagen de NanoBSD durante el arranque del LiveCD o memstick 34
Solución de problemas de instalación 34
Iniciar desde CD en vivo falla 34
Arrancar desde el disco duro después de la instalación del CD no 35
Enlace de la interfaz hasta que no detecte 35
Solución de problemas de hardware 36
Problemas de arranque integrados en ALIX Hardware 37
Instalación de Recuperación 38
Pre-Flight Recuperación de la configuración del instalador 38
Instalado Recuperación de la configuración 38
WebGUI Recuperación 39
Actualizar una instalación existente 39
Haga una copia de seguridad ... y un plan de respaldo 39
Actualización de una Instalación de Embedded 39
Actualización de una instalación completa o NanoBSD instalar 40

La actualización de un Live CD de instalación 41
5. Configuración 42
Conexión a la WebGUI 42
Asistente de configuración 42
Pantalla de información general 43
NTP y Configuración del huso horario 43
Configuración WAN 44
Configuración de la interfaz LAN 47
Establezca la contraseña de administrador 47
Completando el Asistente para la instalación 48
Configuración de la interfaz 48
Asigne las interfaces 49
Conceptos básicos de configuración de interfaz 49
Administración de listas en la GUI 49
Navegue rápidamente la interfaz gráfica de usuario con accesos directos 50
Opciones de configuración generales 51
Opciones de configuración avanzada 52
Administrador de acceso Tab 52
Firewall / NAT Tab 55
Redes Tab 58
Tab Varios 59
Sistema optimizables Tab 62
Notificaciones 62
Fundamentos del menú de la consola 63
Asigne Interfaces 64
Interfaz del dispositivo (s) dirección IP 64
Restablecer contraseña webConfigurator 64
Restablecer los valores predeterminados de fábrica 64
Reinicie el sistema 64
Sistema Halt 64
Anfitrión Ping 64
Cáscara 65
PFtop 65
Registros Filtrar 65
Reinicie webConfigurator 65
pfSense desarrollador Shell (Formerly PHP shell) 65
Actualización de la consola 66
Activar / Desactivar Secure Shell (sshd) 67
Restaurar configuración reciente 67
Mueva el archivo de configuración de dispositivo extraíble 67
Sincronización de tiempo 67
Husos horarios 67
Al compás problemas 67
Tiempo de sincronización GPS 69
Solución de problemas 70
No se puede acceder desde WebGUI LAN 70
Sin Internet desde la LAN 70
Archivo de configuración XML de pfSense 72
Edición manual de la configuración 72
¿Qué hacer si usted consigue acceder a los ..... WebGUI 73
Contraseña Olvidada 73
He olvidado la contraseña con una consola Bloqueado 73
HTTP vs Confusión HTTPS 73
Acceso Bloqueado con reglas de firewall 74
Remotamente Eludir Firewall de bloqueo con las Reglas 74
Remotamente Circumvent Firewall Bloqueo con SSH Tunneling 75
Bloqueado debido a un error de configuración de Squid 75
Pensamientos configuración final 76

6. Tipos de interfaz y configuración 77
Interfaces físicas y virtuales 77
De grupos de interfaces 77
Sin hilos 78
VLANs 78
QinQs 78
PPP 79
GRE (Generic Routing Encapsulation) 81
GIF (interfaz de túnel genérico) 82
Puentes 83
LAGG (Link Aggregation) 83
OpenVPN 84
Configuración de la interfaz 84
Descripción 84
Dirección MAC 85
MTU (Maximum Transmission Unit) 85
MSS (Maximum Segment Size) 85
Velocidad y Dúplex 85
Bloque Redes Privadas 85
Bloquear Bogon redes 85
Tipos IPv4 WAN 86
Ninguno 86
Estática IPv4 86
DHCP 86
Tipos PPP 87
Tipos IPv6 WAN 87
Ninguno 87
IPv6 estática 87
DHCP6 88
SLAAC 88
6RD Túnel 88
Túnel 6to4 88
Track Interface 89
7. Administración de usuarios y autenticación 90
Soporte largo pfSense 90
Gestión de usuarios 90
Privilegios 90
Agregar / Editar Usuarios 91
Adición / Edición de Grupos 92
Configuración 92
Servidores de autenticación 93
RADIUS 93
LDAP 93
Solución de problemas 94
8. Administración de certificados 96
Introducción Básica a X.509 Public Key Infrastructure 96
Certificado de gestión de la Autoridad 96
Crear una nueva autoridad de certificación 96
Edición de una entidad emisora de certificados 98
Exportación de una entidad emisora de certificados 98
Quitar una entidad emisora de certificados 98
Gestión de certificados 98
Crear un nuevo certificado 98
Exportar un certificado 100
Quitar un certificado 100
Los certificados de usuario 100
Revocación de certificados Gestión de listas 101
Crear una nueva lista de certificados revocados 101

Importar una lista de certificados revocados existente 101
Exportar una lista de certificados revocados 102
Eliminación de una lista de certificados revocados 102
Revocar un Certificado 102
Actualización de una lista de certificados revocados Importado 102
Importar desde EasyRSA 102
9. Backup y recuperación 104
Estrategias de respaldo 104
Hacer copias de seguridad de los WebGUI 104
Usando el paquete AutoConfigBackup 105
Funcionalidad y Beneficios 105
pfSense Compatibilidad de versiones 105
Instalación y configuración 105
Restauración de metal desnudo 106
Comprobación del estado AutoConfigBackup 107
Técnicas de copia de seguridad remota Alternos 107
Tire con wget 107
Empuje con SCP 107
Copia de seguridad de base de SSH 108
Restauración a partir de copias de seguridad 108
Restauración con los WebGUI 108
Restauración de la Historia Config 109
Restauración con PFI 109
Restauración de Montaje de la CF / HDD 110
Rescate Config durante la instalación 110
Los archivos de copia de seguridad y directorios con el paquete de copia de seguridad 111
... 111
Copia de seguridad de datos RRD 111
Restauración de datos RRD 111
Advertencias y Gotchas 112
10. Firewall 112
Cortafuegos Fundamentos 112
Terminología básica 112
Filtrado activo 113
Ingress Filtering 113
Filtrado de salida 115
Bloquear vs Rechazar 115
Introducción a la pantalla de las reglas del cortafuegos 116
Adición de una regla de firewall 117
Edición de reglas de firewall 117
Mover reglas del cortafuegos 117
Eliminación de reglas de firewall 118
Alias 118
Configuración de los nombres 118
El uso de los nombres 120
Mejoras Alias en 2.0 120
Firewall Rule Mejores Prácticas 120
Denegación predeterminada 120
Que sea corto 121
Revise sus Reglas 121
Documentar su configuración 121
La reducción de ruido Iniciar 122
Prácticas de tala 122
Regla Metodología 122
Alta automática de reglas de firewall 125
Configuración de reglas de firewall 125
Acción 125
..... Discapacitados 125
Interfaz .....

Protocolo 125
Fuente 125
OS Fuente 125
Destino 126
Iniciar sesión 126
Opciones avanzadas 126
Tipo Estado 126
No XML-RPC Sync 127
Horario 127
Pasarela 127
Descripción 127
Métodos de uso adicional IPs públicas 127
Elegir entre direccionamiento, puente, y NAT 127
IPs virtuales 129
Proxy ARP 129
CARP 129
Otro 129
Reglas basadas en el tiempo 130
Reglas Time Based Lógica 130
Reglas del tiempo basada Advertencias 130
Configuración de Horarios para las reglas basadas en el tiempo 130
Consulta de registros Firewall 132
Visualización de las WebGUI 132
Viendo desde el Menú Consola 133
Para ver imágenes de la Shell 133
¿Por qué a veces veo bloqueado las entradas del registro para las conexiones legítimas? 134
Reglas de cortafuegos de solución de problemas 134
Revise sus registros 134
Parámetros de la regla de la opinión 134
Norma imperativa Revisión 134
Normas e interfaces 134
Habilite el registro regla 135
Solución de problemas con las capturas de paquetes 135
11. Network Address Translation 136
Por defecto Configuración NAT 136
Por defecto de configuración NAT de salida 136
Por defecto Configuración NAT entrante 136
Port Delanteros 136
Riesgos de Port Forwarding 136
Port Forwarding y Servicios Locales 137
Adición de puertos Delanteros 137
Port Forward Limitaciones 140
Servicio de Auto-Configuración con UPnP 140
La redirección de tráfico con puerto reenvía 141
NAT 01:01 141
Los riesgos de la NAT 01:01 142
Configuración de NAT 01:01 142
NAT 01:01 en la IP WAN, también conocido como "zona de distensión" en Linksys 144
..... 144
Ordenamiento de NAT y Procesamiento Firewall 145
Extrapolando a interfaces adicionales 146
Las reglas para NAT 146
Reflexión NAT 146
Configuración y uso de Reflexión NAT 146
DNS Dividir 147
NAT Saliente 147
Salida predeterminado Reglas NAT 147
Puerto estático 148
Desactivación de NAT Saliente .....

Elegir una configuración NAT 148
IP pública individual por WAN 148
Múltiples IPs públicas por WAN 148
NAT y compatibilidad Protocolo 148
FTP 148
TFTP 150
PPTP / GRE 150
Juegos Online 151
Solución de problemas 151
Port Forward Solución de problemas 151
NAT Solución de problemas Reflexión 153
Outbound NAT Solución de problemas 153
12. Enrutamiento 154
Gateways 154
Familias Gateway Address (IPv4 e IPv6) 154
Gestión de Gateways 154
Gateway Settings 154
Grupos de Gateway 156
Rutas estáticas 157
Ejemplo ruta estática 157
Bypass de reglas de firewall para el tráfico en una misma interfaz 157
ICMP Redirecciones 158
Enrutamiento IP públicas 158
Asignación IP 158
Configuración de la interfaz 159
Configuración NAT 160
Configuración de regla de cortafuegos 161
Protocolos de enrutamiento 162
RIP 162
BGP 162
OSPF 162
Ruta Solución de problemas 163
Visualización de Rutas 163
Usando traceroute 165
Rutas y VPNs 165
13. Bridging 167
Tender un puente y bucles de Capa 2 167
Tender un puente y un cortafuegos 167
Tender un puente dos redes internas 167
DHCP y Puentes Internos 167
Bridging OPT para WAN 168
Cerrando la interoperabilidad 168
Portal cautivo 168
CARP 168
Multi-WAN 172
14. LANs virtuales (VLANs) 173
Requisitos 173
Terminología 173
Trunking 173
VLAN ID 174
Interfaz de Padres 174
Puerto de acceso 174
Etiquetado doble (QinQ) 174
VLAN privada (PVLAN) 174
VLANs y Seguridad 174
La segregación de zonas de confianza 175
Uso de la VLAN1 default 175
El uso de VLAN predeterminado del puerto de línea externa 175

Limitar el acceso a los puertos troncales 175
Otros problemas con los interruptores 175
Configuración pfSense 176
Configuración de la Consola de VLAN 176
Configuración de VLAN Interfaz Web 178
Cambie Configuración 179
Cambie la configuración visión general 179
Conmutadores basados Cisco IOS 180
Conmutadores basados Cisco CatOS 181
HP ProCurve cambia 181
Netgear switches gestionados 183
Dell PowerConnect switches gestionados 188
15. Múltiples conexiones WAN 189
La elección de su conectividad a Internet 189
Caminos de cables 189
Caminos hacia la Internet 189
Mejor redundancia, más ancho de banda, menos dinero 190
Multi-WAN Terminología y conceptos 190
Política de encaminamiento 190
Grupos de Gateway 190
Failover 190
Equilibrio de carga 190
Monitorear IPs 191
Killing Estado / conmutación forzada 191
Resumen de los requisitos multi-WAN 191
Multi-WAN Advertencias y consideraciones 191
Múltiples WANs compartiendo una única puerta de enlace IP 191
Múltiple PPPoE o PPTP WANs 192
Servicios locales y multi-WAN 192
IPv6 y Multi-WAN 192
Interfaz y configuración DNS 192
Configuración de la interfaz 193
Configuración del servidor DNS 193
La ampliación a un gran número de interfaces WAN 193
Multi-WAN Casos especiales 193
Conexiones múltiples con el mismo IP del gateway 193
Multi-WAN y NAT 194
Multi-WAN y Manual salida NAT 194
Multi-WAN y Port Forwarding 194
Multi-WAN y NAT 01:01 194
Equilibrio de carga y conmutación por error 194
Configuración de un grupo de puerta de enlace para el equilibrio de carga o la conmutación por error 194
..... 196
Problemas con el equilibrio de carga 196
Comprobación de la funcionalidad 196
Pruebas de conmutación por error 197
Load Balancing Verificación Funcionalidad 198
Política de Enrutamiento, equilibrio de carga y conmutación por error Estrategias 198
Ancho de banda de agregación 198
La segregación de los servicios prioritarios 199
Failover Sólo 199
Desigual carga Costo Equilibrio 199
Multi-WAN en un palo 200
Multi-WAN para servicios que se ejecutan en el servidor de seguridad 200
Multi-WAN para IPv6 200
Advertencias 201
Requisitos 201
Disposición 201
Tácticas Alternos .....

Multi-Link PPPoE (MLPPP) 201
Requisitos 201
Disposición 202
Advertencias 202
Solución de problemas 202
Verifique su configuración de reglas 202
El balanceo de carga no funciona 202
Conmutación por error no trabajar 202
16. Redes privadas virtuales 203
Despliegues comunes 203
Sitio para la conectividad de sitio 203
Acceso remoto 204
Protección para las redes inalámbricas 204
Relé Secure 204
La elección de una solución de VPN para el entorno 204
Interoperabilidad 204
Consideraciones sobre la autentificación 205
Facilidad de configuración 205
Multi-WAN capaz 205
Disponibilidad del cliente 205
Amabilidad Firewall 206
Criptográficamente seguro 207
Resumen 207
VPN y reglas de firewall 207
IPsec 207
OpenVPN 207
PPTP 208
VPNs y IPv6 208
Soporte IPv6 VPN 208
IPv6 VPN y reglas de firewall 208
17. IPsec 209
IPsec Terminología 209
Asociación de Seguridad 209
Política de Seguridad 209
Fase 1 209
Fase 2 209
IPsec y IPv6 210
Elección de las opciones de configuración 210
1 Configuración Fase 210
2 Configuración Fase 215
IPsec y las reglas del cortafuegos 216
Sitio a sitio 217
Sitio con el ejemplo de configuración de sitio 217
Enrutamiento y pasarela consideraciones 222
Enrutamiento varias subredes a través de IPsec 223
iniciado por pfSense Tráfico y IPsec 224
IPsec móvil 225
Ejemplo de configuración del servidor 225
Configuración del cliente Ejemplo 232
Prueba de conectividad IPsec 251
Solución de problemas de IPsec 251
Túnel no establece 252
Túnel establece pero no pasa tráfico 252
Algunos servidores funcionan, pero no todos 253
Conexión bloquea 253
"Al azar" Fallas Desconecta Túnel / DPD en Routers Embedded 253
Túneles Establecer y trabajo pero no logran Renegociar 253
Túnel Establece cuando se inicia, pero no cuando se responde 254

Interpretación IPsec Iniciar 254
Depuración avanzada 258
Configuración de dispositivos de terceros IPsec 259
Orientaciones generales para dispositivos IPsec de terceros 259
Cisco PIX OS 6.x 259
Cisco PIX OS 7.x, 8.x, y ASA 260
Cisco IOS Los routers 260
18. PPTP VPN 262
Advertencia PPTP Seguridad 262
PPTP y reglas de firewall 262
PPTP y Multi-WAN 262
PPTP Limitaciones 262
Configuración del Servidor PPTP 263
Direccionamiento IP 263
Autenticación 263
Requerir cifrado de 128 bits 263
Guardar cambios para iniciar el servidor PPTP 264
Configurar reglas de firewall para clientes PPTP 264
Adición de usuarios 264
Configuración del cliente PPTP 266
Windows XP 266
Windows Vista 268
De Windows 7 272
Mac OS X 272
PPTP redirección 275
PPTP Solución de problemas 275
No se puede conectar 276
Conectado con PPTP, pero no puede pasar tráfico 276
Trucos PPTP enrutamiento 276
Registros PPTP 277
19. OpenVPN 278
OpenVPN y Certificados 278
OpenVPN e IPv6 278
Opciones de configuración de OpenVPN 279
Opciones de configuración del servidor 279
Uso del Asistente OpenVPN Server para acceso remoto 284
Antes de iniciar el Asistente 284
Seleccione Tipo de autenticación 285
La elección de un servidor LDAP 285
Adición de un servidor LDAP 285
La elección de un servidor RADIUS 286
Adición de un servidor RADIUS 286
La elección de una entidad emisora de certificados 287
La creación de una autoridad de certificación 287
La elección de un certificado de servidor 288
Adición de un certificado de servidor 288
Configuración de los ajustes del servidor OpenVPN 289
Configuración de regla de cortafuegos 291
Fin del Asistente de 292
Configuración de usuarios 292
Usuarios locales 292
LDAP o RADIUS Usuarios 292
Instalación del cliente OpenVPN 292
Paquete de exportación OpenVPN Client 293
Instalación del cliente 294
Configuración del cliente 296
Sitio de Ejemplo de configuración del sitio (Shared Key) 303
Configuración de Server Side 304

Configuración del lado del cliente 304
Prueba de la conexión 305
Sitio de Ejemplo de configuración del sitio (SSL / TLS) 305
Configuración de SSL / TLS Server Side 305
Configuración de SSL / TLS Client Side 307
Prueba de la conexión 308
Comprobación del estado de clientes y servidores OpenVPN 308
Permitir el tráfico al servidor OpenVPN 308
Permitir el tráfico a través de OpenVPN Túneles 309
Clientes OpenVPN y acceso a Internet 309
NAT con conexiones OpenVPN 309
Asignación de interfaz y configuración 309
Filtrar con OpenVPN 310
NAT con OpenVPN 310
OpenVPN y Multi-WAN 312
OpenVPN asignado a un grupo de Gateway 312
Servidores OpenVPN y multi-WAN 312
Clientes OpenVPN y multi-WAN 313
OpenVPN Site-to-Site con Multi-WAN y OSPF 314
OpenVPN y CARP 315
Conexiones OpenVPN puenteados 315
Modo de Dispositivo 315
Túnel Red 316
Puente DHCP 316
Puente Interfaz 316
Puente Servidor DHCP Start / End 316
Crear el puente 316
Conéctate con Clientes 316
Opciones de configuración personalizada 317
Opciones de ruta 317
Especificar la dirección IP para utilizar 317
Compartir un puerto con OpenVPN y una ..... Servidor Web 318
Controlar parámetros del cliente a través de RADIUS 318
Solución de problemas de OpenVPN 318
Compruebe OpenVPN Estado 318
Compruebe Firewall Log 319
Algunos servidores funcionan, pero no todos 319
Compruebe los registros de OpenVPN 319
Asegúrese de que no las conexiones IPsec superpuestas 319
Compruebe la tabla de enrutamiento del sistema 320
Prueba de diferentes puntos de vista 320
Trace el tráfico con tcpdump 320
Rutas no empujar a un cliente 320
Por qué no puedo hacer ping a algunas direcciones de adaptador OpenVPN? 320
El cliente específico entrada iroute Override parece tener ningún efecto 321
¿Por qué mis clientes OpenVPN todos reciben la misma IP? 321
Importación de los parámetros DH OpenVPN 321
20. Traffic Shaper 322
Traffic Shaping Basics 322
Lo que el Traffic Shaper puede hacer por usted 322
Sigue navegando Smooth 322
Mantenga Llamadas VoIP Claro 323
Reducir Lag Gaming 323
Mantenga las aplicaciones P2P Llegada 323
Limitaciones Hardware 323
Limitaciones de la aplicación Traffic Shaper en 1.2.x 323
Sólo dos de apoyo interfaz 323
El tráfico a la interfaz LAN afectada 323

Sin inteligencia aplicación 324
Configuración de la talladora del tráfico con el Asistente 324
Inicio del Asistente 324
Redes y plazos de envío 324
Voz sobre IP 325
Penalty Box 326
Redes Peer-to-Peer 326
Network Games 327
Subir o bajar otras aplicaciones 327
Fin del Asistente de 328
Monitoreo de las colas 328
Personalización avanzada 329
Edición de la talladora Colas 329
Edición de reglas de la talladora 331
Solución de problemas de la talladora 333
¿Por qué no es el tráfico de BitTorrent va a la cola de P2P? 333
¿Por qué no es el tráfico a los puertos abiertos por UPnP correctamente en cola? 333
¿Cómo puedo calcular la cantidad de ancho de banda para asignar a las colas ACK? 333
¿Por qué es <x> no la forma adecuada? 334
21. Equilibrio de carga del servidor 335
Explicación de las opciones de configuración 335
Piscinas de servidor virtual 335
Conexiones Sticky 336
La carga del servidor Web Balancing Ejemplo de configuración 337
Entorno de red Ejemplo 337
Configuración de la piscina 337
Configuración de servidor virtual 338
Configuración de reglas de firewall 338
Visualización del estado del equilibrador de carga 339
Balanceo de carga Verificación 340
Equilibrio de carga de solución de problemas del servidor 340
Las conexiones no están equilibrados 340
Equilibrio desigual 340
Servidor de Down no marcado como sin conexión 341
Servidor Live no marcado como línea 341
22. Inalámbrico 342
Hardware inalámbrico Recomendado 342
Las tarjetas inalámbricas de grandes proveedores de nombres 342
Controladores inalámbricos incluidos en 1.2.3 342
WAN inalámbrica 343
Asignación de interfaz 343
Configuración de la red inalámbrica 343
Comprobar el estado inalámbrico 343
Mostrando las redes inalámbricas disponibles y la fuerza de la señal 344
Tender un puente e inalámbrico 344
BSS y IBSS inalámbrico y puenteo 344
El uso de un punto de acceso externo 345
En cuanto a su router inalámbrico en un punto de acceso 345
Bridging inalámbrico a su LAN 345
Tender un puente inalámbrico para una interfaz OPT 346
pfSense como punto de acceso 346
¿Debo usar un punto de acceso externo o pfSense como mi punto de acceso? 346
Configuración de pfSense como punto de acceso 347
Protección adicional para la red inalámbrica 349
Protección inalámbrica adicional con Captive Portal 350
Protección adicional con VPN 350
Configuración de un punto de acceso inalámbrico seguro 351
Enfoque firewall múltiple 352

Enfoque firewall Individual 352
Consideraciones de control de acceso y filtrado de salida 352
Solución de problemas de conexiones inalámbricas 353
Compruebe la antena 353
Pruebe con varios clientes o tarjetas inalámbricas 353
Intensidad de la señal es baja 353
23. Portal Cautivo 354
Limitaciones 354
Sólo se puede ejecutar en una sola interfaz 354
Que no sean capaces de portal inverso 354
Configuración del portal sin autenticación 354
Portal de configuración mediante autenticación local 354
Portal de configuración mediante la autenticación RADIUS 354
Opciones de configuración 354
Interfaz 355
Número máximo de conexiones simultáneas 355
Intervalo de espera inactivo 355
Tiempo de espera de disco 355
Salir ventana emergente 355
URL de redirección 355
Los inicios de sesión de usuarios concurrentes 355
Filtrado MAC 355
Autenticación 355
HTTPS sesión 356
HTTPS server name 356
Contenido de la página Portal 356
Contenido de la página de error de autenticación 357
Solución de problemas de Portal Cautivo 357
Los errores de autenticación 357
Página de Portal nunca carga (tiempo de espera) ni tampoco cualquier otra carga de la página 357
..... 358
24. Firewall de redundancia / alta disponibilidad 358
Descripción general CARP 359
pfsync general 359
pfsync y actualizaciones 359
pfSense XML-RPC Sync Información general 360
XML-RPC y actualizaciones 360
Configuración redundante Ejemplo 360
Determinar asignaciones de dirección IP 361
Configure el firewall primario 364
Configuración del servidor de seguridad secundaria 364
Configuración de la sincronización de configuración 365
Multi-WAN con CARP 365
Determinar asignaciones de dirección IP 366
Configuración NAT 367
Configuración del cortafuegos 367
Multi-WAN CARP con DMZ Diagrama 367
Verificación de conmutación por error Funcionalidad 367
Comprobar el estado de CARP 367
Comprobación de la configuración de replicación 367
Compruebe DHCP Failover Estado 368
CARP Prueba Failover 368
Proporcionar redundancia Sin NAT 368
Asignación IP públicas 368
Descripción general de la red 369
Capa 2 de redundancia 370
Cambie Configuración 370
Anfitrión Redundancia 370
Otros puntos de fallo .....

CARP con Bridging 370
CARP Solución de problemas 371
Errores de configuración comunes 371
Error Hash incorrecta 371
Ambos sistemas aparecen como MAESTRO 372
Sistema principal se ha quedado atascado como ALTERNATIVA 372
Problemas dentro de máquinas virtuales (ESX) 372
Problemas de sincronización de configuración 372
CARP y Multi-WAN Solución de problemas 373
Extracción de un VIP CARP 373
25. Servicios 374
Servidor DHCP 374
Configuración 374
Estado 377
Arrendamientos 377
Bitácoras de Servicio DHCP 377
DHCP Relay 378
Forwarder DNS 378
Configuración DNS Forwarder 378
DNS dinámico 380
El uso de DNS dinámico 380
RFC 2136 actualizaciones de DNS dinámico 380
SNMP 381
SNMP Daemon 381
SNMP Traps 381
Módulos 382
Enlazar a la interfaz LAN sólo 382
UPnP 382
Las preocupaciones de seguridad 383
Configuración 383
Estado 384
Solución de problemas 385
NTPD 385
Wake on LAN 386
Wake Up una sola máquina 386
Almacenamiento de direcciones MAC 386
Despierta una sola máquina almacenado 386
Despierta todas las máquinas almacenados 387
Reactivación desde DHCP Arrendamientos Ver 387
Sálvame de arriendos DHCP Ver 387
PPPoE servidor 387
26. Sistema de Vigilancia de 388
Registros del sistema 388
Visualización de los registros del Sistema 388
Cambiar Configuración de registro 389
Inicio de sesión remoto con Syslog 389
Salpicadero 390
Gestión Reproductores 390
Disponible Reproductores 391
Estado de la interfaz 394
Estado de los servicios 394
Gráficos RRD 395
Sistema Gráficos 396
Los gráficos de tráfico 396
Gráficos de paquetes 396
Los gráficos de calidad 396
Cola Gráficos 397
Ajustes 397

Firewall Unidos 397
Visualización de las WebGUI 397
Viendo con pftop 397
Los gráficos de tráfico 398
27. Paquetes 399
Introducción a los paquetes 399
Instalación de paquetes 400
Reinstalación y actualización de paquetes de 400
La desinstalación de paquetes 401
Desarrollar paquetes 401
28. Software de Terceros y pfSense 402
RADIUS de autenticación de Windows Server 402
La elección de un servidor para IAS 402
Instalación de la NIC 402
Configuración de la NIC 402
Filtrado de contenido gratuito con OpenDNS 404
Configuración de pfSense utilizar OpenDNS 404
Configurar los servidores DNS internos para utilizar OpenDNS 405
Configuración de OpenDNS Content Filtering 406
Configuración de las reglas del cortafuegos para prohibir otros servidores DNS 408
Finalización y otras preocupaciones 409
Syslog Server en Windows con Kiwi Syslog 409
Uso del software del Sistema de Puertos de FreeBSD (Paquetes) 409
Preocupaciones / Advertencias 409
Instalación de paquetes 410
Mantener Paquetes 411
29. Paquete Captura 412
Captura de marco de referencia 412
Seleccionar la interfaz adecuada 412
Limitar el volumen de captura 412
Captura de paquetes desde el WebGUI 413
Conseguir una captura de paquetes 413
Visualización de los datos capturados 413
Utilizando tcpdump desde la línea de comandos 413
tcpdump indicadores de línea de comando 414
tcpdump Filtros 416
Ejemplos de solución de problemas prácticos 418
Uso de Wireshark con pfSense 421
Viendo el Paquete de captura de archivo 421
Herramientas de análisis de Wireshark 421
Captura Remota en tiempo real 422
Llanura Depuración Protocolo Texto flujo TCP 423
Referencias adicionales 423
Guía A. Menu 425
Sistema 425
Interfaces 425
Firewall 426
Servicios 426
VPN 427
Estado 427
Diagnóstico 428
Índice 430

Lista de Figuras

2.1. Máscara de subred Convertidor 12
2.2. Red / Nodo Calculadora 13
4.1. Interfases de pantalla 24
5.1. Asistente de configuración de la pantalla de inicio 43
5.2. Pantalla de información general 43
5.3. NTP y la zona horaria de la pantalla de configuración 44
5.4. Configuración WAN 44
5.5. Configuración WAN general 45
5.6. Configuración de IP estática 45
5.7. DHCP Hostname Configuración 45
5.8. Configuración PPPoE 46
5.9. Configuración WAN PPTP 46
5.10. Built-in Ingress opciones de filtrado 47
5.11. Configuración de LAN 47
5.12. Cambiar contraseña administrativa 48
5.13. Actualizar pfSense WebGUI 48
5.14. Barra de acceso directo Ejemplo 50
5.15. Accesos directos en Serv 51
5.16. La creación de un puerto 80 SSH túnel en PuTTY 75
6.1. Agregar grupo Interfaz 78
6.2. Grupo de interfaz de reglas de firewall Tab 78
9.1. WebGUI copia de seguridad 105
9.2. WebGUI Restaurar 109
9.3. Historia de configuración 109
10.1. El aumento de tamaño de la tabla de estado a 50.000 112
10.2. Defecto reglas WAN 116
10.3. Por defecto las reglas de LAN 116
10.4. Añadir opciones de la regla de LAN 117
10.5. Ejemplo acoge alias .....
10.6. Ejemplo alias de red .....
10.7. Puertos Ejemplo alias .....
10.8. Autocompletado de hosts alias 119
10.9. Autocompletado de puertos alias 119
10.10. Ejemplo Regla Utilizar alias 119
10.11. Suspendido en el aire muestra el contenido Hosts 119
10.12. Suspendido en el aire muestra el contenido de Puertos 120
10.13. Regla de cortafuegos para evitar la tala Transmisiones 121
10.14. Alias para los puertos de gestión .....
10.15. Alias de hosts de gestión .....
10.16. Lista de Alias .....
10.17. Ejemplo de gestión de reglas de LAN restringido .....
10.18. De gestión de reglas de LAN restringidos - ejemplo alternativo .....
10.19. Regla Anti-bloqueo desactivado .....
10.20. Probando la resolución de nombres para las actualizaciones bogon 124
10.21. Múltiples IPs públicas en uso - bloque de IP única .....
10.22. Múltiples IPs públicas de uso - dos bloques IP .....
10.23. Adición de un rango de tiempo .....
10.24. Agregado Intervalo de tiempo .....
10.25. Programaciones después de añadir 131
10.26. La elección de un calendario para una regla de firewall 131
10.27. Firewall Listado de reglas con el Anexo 131
10.28. Entradas del registro Ejemplo vistos desde los WebGUI 132
11.1. Añadir Port Forward 137
11.2. Port Forward Ejemplo 139
11.3. Puerto Atacante Listado 140

11.4. Port Forward Firewall Rule 140
11.5. Ejemplo redirigir el puerto hacia adelante 141
11.6. 01:01 pantalla NAT Editar 142
11.7. 01:01 NAT Entrada 143
11.8. 01:01 NAT Ejemplo - dentro y fuera de ..... IP Individual .....
11.9. 01:01 entrada NAT para / 30 rango CIDR .....
11.10. Ordenamiento de NAT y Procesamiento Firewall .....
11.11. LAN a WAN Procesamiento .....
11.12. WAN a LAN Procesamiento .....
11.13. Regla de Firewall de Port Forward para LAN Host 145
11.14. Habilitar Reflexión NAT 146
11.15. Añadir DNS Forwarder Override 146
11.16. Añadir DNS Forwarder Invalidar example.com .....
11.17. Anulación Forwarder DNS para www.example.com .....
12.1. Ruta estática .....
12.2. Configuración de la ruta estática .....
12.3. Enrutamiento asimétrico 157
12.4. WAN IP y la configuración de puerta de enlace 157
12.5. Enrutamiento configuración OPT1 158
12.6. Configuración NAT de salida 159
12.7. Reglas de firewall OPT1 160
12.8. Reglas de firewall WAN 161
12.9. Ruta Display 161
13.1. Regla de cortafuegos para permitir el DHCP 162
14.1. Interfaces: Asignar 163
14.2. Lista de VLAN 168
14.3. Editar VLAN 178
14.4. Lista de VLAN 178
14.5. Lista Interfaz con VLANs 178
14.6. Grupo VLAN Configuración 179
14.7. Habilitar 802.1Q VLANs 179
14.8. Confirmar cambio de 802.1Q VLAN 183
14.9. Por defecto la configuración 802.1Q 183
14.10. Añadir nueva VLAN 184
14.11. Añadir VLAN 10 184
14.12. Añadir VLAN 20 184
14.13. Membresía Toggle VLAN 185
14.14. Configure VLAN 10 membresía 185
14.15. Configure VLAN 20 membresía 186
14.16. Ajuste PVID 186
14.17. Por defecto Configuración PVID 186
14.18. Configuración VLAN 10 y 20 PVID 187
14.19. Eliminar VLAN 1 membresía 187
15.1. Multi-WAN en un palo 187
17.1. Habilitar IPsec 187
17.2. Configuración de túnel VPN sitio 200
17.3. Del sitio de la Fase 1 Ajustes 218
17.4. Sitio Fase 2 lista (vacía) .....
17.5. Adición de una entrada de la Fase 2 a sitio .....
17.6. Configuración general 2 del sitio de la Fase .....
17.7. Del sitio de la Fase 2 Configuración .....
17.8. Sitio Keep Alive .....
17.9. Aplicar configuración de IPsec .....
17.10. Sitio B Fase 1 Ajustes .....
17.11. Sitio B Fase 2 Configuración 219
17.12. Sitio B Keep Alive 219
17.13. Sitio IPsec Estado 219
17.14. Sitio para localizar IPsec Dónde pfSense no es la puerta de enlace 220
220
220
221
221
222
222
223

17.15. Sitio para localizar IPsec 224
17.16. Del sitio - ruta estática a la subred remota 224
17.17. Sitio B - ruta estática a la subred remota 225
17.18. Habilitar los clientes móviles de IPsec 226
17.19. Autenticación de clientes móviles 226
17.20. Clientes móviles empujado Ajustes 227
17.21. Clientes móviles Fase Prompt 1 Creación 228
17.22. Los clientes móviles de la Fase 1 229
17.23. Los clientes móviles de la Fase 2 230
17.24. Aplicar Configuración de túnel Mobile 230
17.25. Mobile IPsec Grupo de Usuarios 231
17.26. Mobile Usuario IPsec 232
17.27. Motorola Android IPsec - Menú Red 234
17.28. Motorola Android IPsec - Menú VPN 235
17.29. Motorola Android IPsec - IPsec Tipo de lista 236
17.30. Motorola Android IPsec - Configuración 238
17.31. Motorola Android IPsec - Configuración (continuación) 239
17.32. Motorola Android IPsec - Conectado 240
17.33. Android 4.x IPsec - Tipos de VPN 241
17.34. Android 4.x IPsec - Configuración IPsec 242
17.35. Android 4.x IPsec - IPsec Autenticación ..... Prompt 243
17.36. Estado Conectado ..... - Android 4.x IPsec 244
17.37. Configuración de IPsec iOS 245
17.38. iOS IPsec - VPN conectado 246
17.39. Shrew Soft VPN Access Manager - No hay conexiones todavía 247
17.40. Configuración de clientes: Ficha General .....
17.41. Configuración de clientes: Tab Client .....
17.42. Configuración de clientes: Resolución de nombres Tab .....
17.43. Configuración de clientes: autenticación, la Identidad Local .....
17.44. Configuración de clientes: autenticación, la Identidad remoto .....
17.45. Configuración de clientes: autenticación, credenciales .....
17.46. Configuración de clientes: Fase 1 .....
17.47. Configuración de clientes: Fase 2 248
17.48. Configuración de clientes: Política .....
17.49. Configuración de clientes: Política, Añadir Topología .....
17.50. Configuración de clientes: Nuevo nombre de conexión .....
17.51. Lista Para Usar conexión .....
17.52. Túnel de autenticación Prompt 249
17.53. Túnel Conectado .....
18.1. PPTP direccionamiento IP .....
18.2. PPTP VPN Firewall Rule .....
18.3. Usuarios PPTP Tab .....
18.4. Adición de un usuario PPTP .....
18.5. Aplicación de cambios PPTP 250
18.6. Lista de Usuarios PPTP 250
18.7. Conexiones de red 263
18.8. Tareas de red 264
18.9. Conexión Workplace 264
18.10. Conectar a VPN 265
18.11. Nombre de conexión 265
18.12. Conexión de host 266
18.13. Terminando la conexión 266
18.14. Conecte diálogo 266
18.15. Propiedades de la conexión .....
18.16. Ficha Seguridad .....
18.17. Redes Tab .....
18.18. Pasarela Selección remota .....
18.19. Conexiones de red Vista .....

267

268

18.20. Configure una conexión 268
18.21. Conectarse a un lugar de trabajo 268
18.22. Conectar mediante VPN 268
18.23. Configuración de la conexión 269
18.24. Configuración de autenticación 269
18.25. La conexión está listo 269
18.26. Obtener propiedades de conexión .....
18.27. Configuración de seguridad de VPN .....
18.28. Configuración de red VPN 270
18.29. Gateway VPN 271
18.30. Agregar una conexión de red 272
18.31. Agregar conexión PPTP VPN 273
18.32. Configurar la conexión PPTP VPN 273
18.33. Opciones avanzadas 274
18.34. Conecte con PPTP VPN 275
18.35. Registros PPTP 275
19.1. Ejemplo OpenVPN red de acceso remoto 277
19.2. Preferencias Viscosidad 284
19.3. Viscosidad Agregar conexión 297
19.4. Configuración Viscosidad: general 297
19.5. Configuración Viscosidad: Certificados 298
19.6. Configuración Viscosidad: Opciones 299
19.7. Configuración Viscosidad: Redes 299
19.8. Viscosidad conectar 300
19.9. Menú Viscosidad 300
19.10. Detalles Viscosidad 301
19.11. Detalles Viscosidad: Estadísticas de Tráfico 301
19.12. Detalles Viscosidad: Registros 302
19.13. OpenVPN ejemplo el sitio de red del sitio 303
19.14. OpenVPN ejemplo un sitio a otro de reglas de firewall WAN 303
19.15. OpenVPN ejemplo un sitio a SSL / TLS ..... red 304
19.16. OpenVPN Estado para el servidor SSL / TLS con un cliente conectado 305
19.17. OpenVPN estado mostrando un servidor a la espera de una conexión, y un cliente que intenta vuelva a conectar 308
19.18. Servidor OpenVPN regla WAN .....
19.19. Asigne la interfaz OpenVPN .....
19.20. Un sitio a otro con subredes en conflicto .....
19.21. Sitio configuración A 01:01 NAT .....
19.22. Sitio B 1:01 configuración NAT 308
19.23. Ejemplo ruta estática para el cliente OpenVPN en OPT WAN 309
19.24. Ejemplo de configuración de OpenVPN que implica OSPF a través de múltiples redes WAN 310
20.1. Inicio del Asistente de la talladora 311
20.2. Configuración de la talladora 312
20.3. Voz sobre IP 314
20.4. Área de castigo 314
20.5. Redes Peer-to-Peer 324
20.6. Network Games 325
20.7. Suba o baje Otras aplicaciones 325
20.8. Colas básicos WAN 326
20.9. Tráfico lista Colas talladora 327
20.10. Traffic Shaper Reglas Lista 327
21.1. Carga del servidor equilibrar ejemplo red 328
21.2. Configuración piscina 328
21.3. Configuración del servidor virtual 329
21.4. Alias para servidores web 332
21.5. Adición de reglas de firewall para servidores web 337
21.6. Regla de firewall para servidores web .....
21.7. Estado del servidor virtual .....

22.1. Asignación Interface - WAN inalámbrica 343
22.2. Wireless WAN Associated ....
22.3. No portadora de WAN inalámbrica 344
22.4. Estado inalámbrico 344
22.5. Reglas para permitir sólo IPsec desde inalámbrico 350
22.6. Reglas para permitir sólo OpenVPN desde inalámbrico 351
22.7. Reglas para permitir sólo PPTP desde inalámbrico 351
23.1. Portal Cautivo en varias subredes ....
24.1. Diagrama de red Ejemplo CARP ....
24.2. WAN IP ..... CARPA .....
24.3. LAN CARP IP 362
24.4. Lista de IP virtual ....
24.5. Entrada NAT Saliente ....
24.6. Configuración NAT Saliente avanzada ....
24.7. Configuración de la interfaz pfsync ....
24.8. Regla de firewall en la interfaz pfsync ....
24.9. Diagrama de la multi-WAN CARP con DMZ 363
24.10. DHCP Failover Piscina Estado 364
24.11. Diagrama del CARP con enrutado IP ....
24.12. Diagrama del CARP con conmutadores redundantes ....
25.1. DHCP Servicio Daemon Estado 367
25.2. DNS Invalidar Ejemplo ....
25.3. Pantalla de estado de UPnP mostrando PC clientes con puertos reenviados .....
25.4. sistema pfSense como se ha visto por Windows 7 en su navegación por la red 377
26.1. Entradas del registro del sistema Ejemplo 379
26.2. Widget Barra de título 385
26.3. Estado de la interfaz 385
26.4. Estado de servicios 388
26.5. Tráfico WAN Gráfico 391
26.6. Ejemplo Unidos ....
26.7. Ejemplo WAN Gráfico ....
27.1. Recuperación de la información del paquete falló 395
27.2. Ficha Paquete 396
27.3. Post-Install Package pantalla 397
27.4. Instalado Lista del paquete ....
28.1. Añadir un nuevo cliente RADIUS ....
28.2. Añadir un nuevo cliente RADIUS - nombre y dirección del cliente 400
28.3. Añadir un nuevo cliente RADIUS - Secreto compartido 400
28.4. Listado del cliente RADIUS 400
28.5. NIC Puertos 401
28.6. Configuración de OpenDNS en pfSense 403
28.7. Propiedades de servidor DNS de Windows ....
28.8. De Windows Server Forwarders DNS ....
28.9. Adición de una red ....
28.10. Adición de una conexión IP dinámica 403
28.11. Adición de una conexión IP estática 404
28.12. Red añadido correctamente 405
28.13. Contenido nivel de filtrado 405
28.14. Administrar dominios individuales 406
28.15. Los servidores DNS alias 407
28.16. LAN reglas para restringir DNS ....
29.1. Captura referencia ....
29.2. Wireshark Captura Ver ....
29.3. Wireshark Análisis RTP ....

408
409

422

Lista de tablas

2.1. RFC 1918 Dirección IP Privado 9
2.2. RFC 4193 Único Espacio de direcciones local 9
2.3. CIDR Subred Cuadro 11
2.4. CIDR sumarización de ruta 12
3.1. El rendimiento máximo por CPU 17
3.2. 500.000 pps a distintos tamaños de bastidor 18
3.3. Grande Estado Consumo Tabla RAM 19
3.4. IPsec Throughput por Cipher - ALIX 20
3.5. IPsec Throughput por CPU 20
4.1. Opciones del Kernel 26
10.1. Tráfico de egreso requerido 114
11.1. / 30 mapeo CIDR - juego octeto final 143
11.2. / 30 mapeo CIDR - no coincidentes octeto final 144
12.1. WAN IP bloqueadas 159
12.2. Dentro de direcciones IP bloqueadas 159
12.3. Banderas y significados de la tabla de rutas 164
14.1. Netgear configuración VLAN GS108T 183
15.1. Carga de costo desigual equilibrio 199
16.1. Rasgos y características por Tipo VPN 207
17.1. Configuración del extremo de IPsec 217
24.1. Asignaciones de dirección IP WAN 360
24.2. Asignaciones de direcciones IP de la LAN 360
24.3. Asignaciones de direcciones IP pfsync 361
24.4. WAN IP Direccionamiento 365
24.5. WAN2 direccionamiento IP 366
24.6. Asignaciones de direcciones IP de la LAN 366
24.7. Asignaciones de direcciones IP DMZ 366
24.8. Asignaciones de direcciones IP pfsync 366
29.1. Bienes Interfaz vs nombres descriptivos 412
29.2. Comúnmente utilizado banderas tcpdump 414
29.3. Ejemplos de uso de tcpdump-s 415

Prefacio

Mis amigos y compañeros de trabajo saben que voy a construir firewalls. Al menos una vez al mes alguien dice "Mi empresa necesita un servidor de seguridad con X e Y, y las cotizaciones de precios He recibido decenas de miles de dólares. ¿Nos puede ayudar? "

Cualquier persona que construye firewalls sabe esta pregunta podría formularse de manera más realista
como "¿Podría venir una noche y una bofetada a algunos equipos
para mí, entonces déjame azar interrumpirle para los próximos tres a cinco años para tener
instalar nuevas características, problemas de depuración, configurar las funciones que no conocía lo suficiente como para
solicitud, asistir a las reuniones para resolver problemas que no pueden posiblemente ser problemas de firewall
pero alguien piensa que puede ser el servidor de seguridad, e identificar soluciones para mi innumerable
requisitos desconocidos? Ah, y asegúrese de probar cada caso de uso posible antes de
desplegar nada."
Rechazando estas peticiones me hace parecer grosero. La aceptación de estas solicitudes ruinas mi comportamiento alegre. Durante mucho tiempo, yo no construir cortafuegos a excepción de mi empleador.

pfSense me permite ser una persona más agradable sin tener que trabajar realmente en él.
Con pfSense puedo implementar un servidor de seguridad en tan sólo unas pocas horas - y la mayor parte de ese
es la instalación de cables y explicar la diferencia entre el "adentro" y "afuera".
amplia comunidad de usuarios de documentación y pfSense me ofrece una respuesta fácil
a las preguntas - "¿buscó eso?" Si pfSense no admite una característica, lo más probable
son que no podía apoyarla bien. Pero pfSense apoya todo lo que podía pedir, y
con una interfaz amigable para arrancar. La amplia base de usuarios significa que las características se ponen a prueba en
muchos entornos diferentes y, en general "sólo trabajo", incluso en la interacción con
Windows ME PC 'del CEO niños conectado a Internet mediante Ethernet sobre ATM
más de una paloma mensajera. Lo mejor de todo, pfSense está construida en gran parte del mismo software que había
utilizar yo mismo. Confío en que el sistema operativo FreeBSD subyacente para ser seguro, estable, y eficiente.
Las actualizaciones de seguridad? Basta con hacer clic en un
botón y reinicie.
Necesita nuevas características? Sólo enciéndalos. pfSense maneja la agrupación, el tráfico
conformación, equilibrio de carga, la integración con su equipo existente a través
RADIUS, IPSec, PPTP, monitoreo, DNS dinámico, y más.

Proveedores de la industria de renombre cobran tarifas exorbitantes para apoyar lo que pfSense libremente
proporciona. Si su empleador insiste en pagar por contratos de soporte, o si lo que sientes

más seguro sabiendo que puede tomar el teléfono y gritar para pedir ayuda, usted puede conseguir pfSense acuerdos de apoyo muy razonable. Si usted no necesita un contrato de soporte,
Me he enterado de que Chris, Jim, o cualquier otra persona con un pfSense se comprometen poco dejará
usuarios agradecidos pfSense a comprar una cerveza o seis.

Personalmente, yo no construyo firewalls desde cero más. Cuando necesito un servidor de seguridad, Yo uso pfSense.

-Michael W. Lucas

Prefacio

Bienvenido a La guía definitiva para pfSense. Escrito por pfSense co-fundador Chris Buechler y consultor pfSense Jim Pingle, este libro cubre la instalación y configuración básica a través de avanzada creación de redes y cortafuegos con el servidor de seguridad de código abierto populares y distribución router.

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

• Una introducción a pfSense y sus características.

• Hardware y planificación del sistema.

• Instalación y actualización de pfSense.

• Utilización de la interfaz de configuración basada en web.

• Copia de seguridad y restauración.

• Cortafuegos fundamentos y reglas que definen y solución de problemas.

• El reenvío de puertos y traducción de direcciones de red (NAT).

• Red General y configuración de enrutamiento.

• Bridging, redes de área local virtuales (VLAN), y Multi-WAN.

• Redes privadas virtuales que utilizan IPSec, PPTP y OpenVPN.

• la modulación del tráfico y balanceo de carga.

• La red inalámbrica y las configuraciones de portal cautivo.

• firewalls redundantes y de alta disponibilidad.

• Diversos servicios relacionados con la red.

• Monitorización de la instalación, la explotación forestal, análisis de tráfico, oler, captura de paquetes y solución de problemas.
• Paquetes de software y software de terceros instalaciones y actualizaciones.

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

Autores

Chris Buechler

Chris es uno de los fundadores del proyecto pfSense, y uno de sus promotores más activos. Él tiene estado trabajando en la industria de TI durante más de una década, trabajando intensamente con los firewalls y FreeBSD para la mayor parte de ese tiempo. Él ha proporcionado la seguridad, la red y los servicios relacionados para las organizaciones en el del sector público y privado, que van desde pequeñas organizaciones a compañías Fortune 500 y numeroso público organizaciones del sector. Actualmente se gana la vida ayudando a las organizaciones con necesidades pfSense relacionados incluyendo el diseño de redes, planificación de implementación, asistencia para la configuración, la conversión de los actuales firewalls, desarrollo y más. Él tiene su sede en Louisville, Kentucky EE.UU. y proporciona servicios para los clientes de todo el mundo. Tiene numerosas certificaciones de la industria, incluyendo el CISSP, SSCP, MCSE y CCNA entre otros. Su página web personal se puede encontrar en http://chrisbuechler.com.

Jim Pingle

Jim ha estado trabajando con FreeBSD para más de diez años, profesionalmente durante los últimos ocho años. Ahora un empleado de tiempo completo de BSD Perimeter, LLC, que provee apoyo global para pfSense comercial suscriptores de apoyo. Como administrador del sistema con HPC Internet, un ISP local en Bedford, Indiana, EE.UU. trabaja con servidores FreeBSD, diversos equipos de enrutamiento y circuitos, y por supuesto, firewalls basados en pfSense tanto interna como para muchos clientes. Jim tiene una Licenciatura en Sistemas de Información de Indiana-Purdue Fort Wayne, y se graduó en 2002. Él 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, la lectura, la toma de fotografías, y de ser un adicto a la televisión. Su página web personal se puede encontrar en http://pingle.org.

Agradecimientos

Este libro, y el propio pfSense no sería posible sin un gran equipo de desarrolladores, contribuyentes, patrocinadores corporativos, y una comunidad maravillosa. El proyecto ha recibido contribuciones de código de más de 100 personas, con 29 personas que han contribuido considerablemente suficiente para obtener cometer acceso. 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 e IRC.
Nuestro agradecimiento a todos los que han hecho su parte para hacer que el proyecto del gran éxito que se ha convertido.

Diseño del libro de la cubierta

Gracias a Holger Bauer para el diseño de la cubierta. Holger fue uno de los primeros contribuyentes a la proyecto, habiendo hecho buena parte del trabajo de tematización, gráficos, y es el creador de los fondos que han utilizado en nuestras presentaciones en seis conferencias de BSD en los últimos cinco años.

pfSense Desarrolladores

El equipo de desarrollo de pfSense activa actual, que se enumeran por orden de antigüedad.

• Co-Fundador de Scott Ullrich

• Co-Fundador Chris Buechler

• Bill Marquette

• Holger Bauer

• Erik Kristensen

• Seth Mos

• Dale a Scott

• Martin Fuchs

• Ermal Luçi

• Mateo novios

• Grúas Marcos

• Rob Zelaya

• Renato Botelho

• Erik Fonnesbeck

• Warren Baker,

• Luiz Costa

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

• Max Laier

• Christian S.J. Perón

• Andrew Thompson

• Bjoern A. Zeeb

Agradecimientos personales

De Chris

Tengo que dar las gracias a mi esposa y un crédito considerable para la realización de este libro, y el éxito del proyecto en general. Este libro y el proyecto han llevado a un sinnúmero de largos días 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 adquirido nuestro apoyo y distribuidor suscripciones, lo que permite que yo haga el salto a trabajar a tiempo completo en el proyecto a principios de 2009.

También debo agradecer a Jim para saltar adentro en este libro y proporcionando una ayuda considerable en la realización de él.
Ya han pasado dos años en la fabricación, y mucho más trabajo de lo que me había imaginado. Puede haber sido obsoleto antes de que llegara terminado si no fuera por su ayuda en los últimos meses. También gracias a Jeremy
Reed, nuestro director y editor, por su ayuda con el libro.

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

De Jim

Me gustaría dar las gracias a mi esposa e hijo, que me aguantan a través de mi participación en la redacción proceso, no sólo para el primer libro pero el segundo también. Sin ellos, me habría vuelto loco
Hace mucho tiempo.

También me gustaría dar las gracias a Rick Yaney de HPC Internet, por ser de apoyo de pfSense,
El software de código de FreeBSD, y abierto en general.

La comunidad entera pfSense merece incluso más gracias también, es la mejor y más
grupo de apoyo de los usuarios y colaboradores que me he encontrado el software de código abierto.

Revisores

Las siguientes personas proporcionaron muy necesaria retroalimentación y conocimiento para ayudar a mejorar el libro y su exactitud. Listado en orden alfabético por apellido.

• Jon Bruce

• Mark Foster

• Bryan Irvine

• Warren Midgley

• Eirik Øverby

Feedback

El editor y los autores animan a sus comentarios en este libro y la distribución pfSense.
Por favor envíe sus sugerencias, críticas y / o elogios por La guía definitiva para el libro de pfSense
<info@reedmedia.net>. Página web de la editorial para el libro está en http://www.reedmedia.net/
libros / pfSense /.

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

Convenciones tipográficas

A lo largo del libro una serie de convenciones se utilizan para denotar ciertos conceptos, información o acciones. La siguiente lista ofrece ejemplos de cómo estos tienen el formato del libro.

Selecciones de menú	Firewall □ Reglas
Labels GUI artículo / Nombres	Destino
Botones	Aplicar cambios
Preguntar por la entrada	¿Quieres continuar?
Entrada del usuario	Descripción de la regla
Nombres de archivo	/ Boot / loader.conf
Nombres de comandos o programas	gzip
Comandos escritos en la línea de comandos	#ls-l
Los artículos que deben ser reemplazados con valores específicos de su instalación	192.168.1.1
Notas especiales	Nota Cuidado con esto!

Líneas literales largas en ejemplos de salida pueden ser divididos con el # (hookleftarrow). Comando-Long shell ejemplos de línea se pueden dividir usando la barra invertida (\) como continuación de línea shell.

Capítulo 1. Introducción

pfSense es una distribución libre, de código abierto personalizada de FreeBSD adaptado para su uso como un servidor de seguridad y
router, administrado en su totalidad en un formato fácil de usar interfaz web. Esta interfaz web se conoce como la web-configurador basado en GUI o WebGUI para abreviar. No se requieren conocimientos de FreeBSD para implementar y utilizar pfSense, y de hecho la mayoría de la base de usuarios nunca ha usado FreeBSD fuera de pfSense. En Además de ser un potente cortafuegos, flexible y una plataforma de enrutamiento, que incluye una larga lista de relacionados
características y un sistema de paquetes que permite mayor capacidad de expansión sin necesidad de añadir la hinchazón y el potencial
vulnerabilidades de seguridad a la distribución base. pfSense es un proyecto popular, con más de 1 millón de descargas desde su creación, y ha demostrado en innumerables instalaciones que van desde pequeñas redes domésticas la protección de un solo equipo a las grandes corporaciones, universidades y otras organizaciones que protegen miles de dispositivos de red.

El inicio del proyecto

Este proyecto fue fundado en 2004 por Chris Buechler y Scott Ullrich. Chris había estado contribuyendo a M0n0wall durante algún tiempo antes de eso, y nos pareció que es una gran solución. Sin embargo, mientras que encantados con
el proyecto, muchos usuarios anhelaba más capacidades que se pueden alojar en un proyecto estrictamente enfocado hacia los dispositivos integrados y de sus recursos de hardware limitados. Introduzca pfSense. Moderno hardware embebido es también hoy bien apoyado y popular con pfSense. En 2004, había
numerosas soluciones integradas con 64 MB de RAM que no se pueden alojar con la deseada conjunto de características de pfSense.

¿Qué significa para pfSense / media?

El proyecto duró un par de meses sin nombre. De hecho, la cárcel FreeBSD que corre nuestro servidor CVS todavía se llama `projectx`.

Scott y Chris fueron los dos únicos miembros del proyecto en el tiempo, como sus fundadores. Corrimos a través de numerosas posibilidades, con la dificultad principal que se está encontrando algo con dominio nombres disponibles. De Scott llegó con pfSense, pf ser el software de filtrado de paquetes se utiliza, como en la toma de sentido de PF. Respuesta de Chris fue menos que entusiasta. Pero después de un par de semanas sin mejores opciones, nos fuimos con él. Se llegó a decir: "Bueno, siempre podemos cambiarlo."

Desde entonces, un cambio de nombre fue considerado entre los desarrolladores, sin que esté tomando importancia como la mayoría de la gente era indiferente y nadie sentía la necesidad imperiosa de un cambio. A mediados de 2007, una discusión
de nombrar se inició por una entrada del blog, y la gran respuesta de la comunidad a través de correo electrónico y los comentarios del blog era "mantener el nombre!"

¿Por qué FreeBSD?

Dado que muchos de los componentes básicos en pfSense provienen de OpenBSD, usted puede preguntarse por qué elegimos
FreeBSD en lugar de OpenBSD. Hubo numerosos factores en cuenta a la hora de elegir un OS para este proyecto. Esta sección resume las principales razones para la elección de FreeBSD.

Soporte inalámbrico

Sabíamos soporte inalámbrico sería una característica crítica para muchos usuarios. En el momento este proyecto fue fundada en 2004, soporte inalámbrico de OpenBSD era muy limitado. Su compatibilidad con el controlador era mucho más
limitado que FreeBSD, y no tenía soporte para las cosas importantes, como WPA (Wi-Fi Protected Access) y WPA2 sin planes de implementar alguna vez ese apoyo en el momento. Algo de esto ha cambiado desde 2004, pero sigue siendo FreeBSD adelante en las capacidades inalámbricas.

Rendimiento de la red

Rendimiento de la red de FreeBSD es significativamente mejor que la de OpenBSD. Para pequeñas y de tamaño medio despliegues, por regla general, no es de ninguna preocupación, como la escalabilidad superior es la principal preocupación 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 a los sistemas FreeBSD PF para manejar los altos paquetes por segundo tasa requeridos en porciones de su red. Esto se ha convertido en un problema menor en OpenBSD desde 2004, pero sigue siendo válida.

La familiaridad y la facilidad de tenedor

Desde la base de código pfSense partió de m0n0wall, que se basa en FreeBSD, era más fácil para quedarse con FreeBSD. Cambiar el sistema operativo requeriría modificar casi todas las partes del sistema. Scott y Chris, los fundadores, también están más familiarizados con FreeBSD y había trabajado anteriormente juntos en un solución de firewall ahora extinta comercial basado en FreeBSD. Esto en sí mismo no era un convincente razón, pero combinado con los dos factores anteriores, fue otra de las cosas que nos apuntan en esta dirección.

Alternativa Compatibilidad con sistemas operativos

En este momento, no hay planes de apoyo a cualquier otro sistema operativo, simplemente por razones de recursos limitaciones. Sería una empresa considerable de portar a cualquiera de los otros sistemas BSD como nosotros confiamos en
parte de la funcionalidad que sólo está disponible en FreeBSD, lo que tendría que ser completamente reprogramado.

Los despliegues comunes

pfSense se utiliza en casi todos los tipos y tamaños de entorno de red imaginable, y es casi ciertamente compatible con su red si contiene un ordenador, o miles de personas. En esta sección se delinear las implementaciones más comunes.

Perímetro Firewall

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

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

Algunos usuarios también se suman BGP capacidades (Border Gateway Protocol) para proporcionar redundancia de conexión
y equilibrio de carga. Esto se describe con más detalle en el capítulo 12, Routing.

LAN o WAN Router

El segundo despliegue más común de pfSense es como una LAN o router WAN. Esta es una función separada desde el servidor de seguridad perimetral en tamaño medio a grandes redes, y puede ser integrado en el perímetro firewall en entornos más pequeños.

LAN Router

En redes grandes que utilizan varios segmentos de red interna, pfSense es una solución probada para conectar estos segmentos internos. Esto se implementa normalmente mediante el uso de VLAN 802.1Q con concentración de enlaces,
que se describe en el Capítulo 14, LAN virtuales (VLAN). Múltiples interfaces Ethernet son también utilizado en algunos entornos.

> **Nota**
>
> En entornos que requieren más de 3 Gbps de rendimiento sostenido, o más de 500.000 paquetes por segundo, ningún enrutador basada en hardware ofrece un rendimiento adecuado.

Dichos entornos necesitan desplegar conmutadores de capa 3 (enrutamiento hecho en hardware por el interruptor)
o routers de gama alta basados en ASIC. A medida que aumenta el hardware de los productos básicos en el rendimiento, y
sistemas operativos de propósito general como FreeBSD mejorar las capacidades de procesamiento de paquetes en
línea con lo que las nuevas capacidades de hardware pueden apoyar, escalabilidad seguirá mejorando con el tiempo.

WAN Router

Para los servicios WAN que proporciona un puerto Ethernet para el cliente, pfSense es una gran solución para la privada Routers WAN. Ofrece toda la funcionalidad de la mayoría de las redes necesitan ya un precio mucho más bajo que las ofertas comerciales de renombre.

Punto de acceso inalámbrico

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

Electrodomésticos para aplicaciones especiales

Muchos desplegar pfSense como un aparato de propósito especial. Los siguientes son los cuatro escenarios que conocemos,
y no están seguros de ser muchos casos similares que no somos conscientes. La mayoría de cualquier de la funcionalidad de
pfSense puede utilizarse en una implementación de tipo aparato. Usted puede encontrar algo único a su entorno en el que este tipo de despliegue es un gran ajuste. Como el proyecto ha madurado, ha habido considerable enfoque en el uso como un marco de creación de aparato, sobre todo en la versión 2.0. Algunos aparatos de propósito especial estarán disponibles en el futuro.

VPN Appliance

Algunos usuarios caen en pfSense como un dispositivo VPN detrás de un firewall existente, para añadir capacidades de VPN
sin crear ninguna interrupción en la infraestructura existente en el cortafuegos. La mayoría de las implementaciones de pfSense VPN
también actúan como un servidor de seguridad perimetral, pero este es un mejor ajuste en algunas circunstancias.

Appliance Servidor DNS

pfSense ofrece un DNS (Domain Name System) paquete de servidor basado en TinyDNS, un pequeño, rápido y seguro Servidor DNS. No es cargado con las características, por lo que no es capaz de ser utilizado para algunos propósitos, tales como Microsoft
Active Directory, pero es un gran ajuste para la celebración de DNS de Internet. Recuerde la vulnerabilidad DNS charla en julio de 2008? Daniel J. Bernstein, autor de TinyDNS, se le atribuye la idea original y implementación de los puertos de origen aleatorios en la resolución de DNS, la resolución de esa vulnerabilidad. De hecho, TinyDNS era el único servidor DNS principal que no necesita ser parcheado en julio de 2008. Tiene utiliza puertos de origen aleatorios desde su creación. Hace varios años, Bernstein incluso poner $ 1,000 USD de su propio dinero en la línea de la primera persona para encontrar un agujero de seguridad de escalada de privilegios. Se mantiene
sin reclamar. Si usted es el anfitrión sólo DNS de Internet, TinyDNS deben considerar fuertemente. La pfSense paquete también agrega capacidades de failover, y el apoyo más fácil para las direcciones IPv6 (AAAA y PTR) en la GUI.

Sniffer Appliance

Un usuario estaba buscando un aparato succionador de desplegar a un número de ubicaciones de las sucursales. Aparatos rastreadores comerciales están disponibles con numerosos campanas y silbidos, pero a un muy significativo costará sobre todo cuando se multiplica por un número de sucursales. pfSense ofrece una interfaz web para tcpdump que permite la descarga del archivo pcap resultante cuando se termina la captura. Este
permite a esta empresa para capturar paquetes en una red de sucursales, descargue el archivo de captura resultante, y abrir en Wireshark [http://www.wireshark.org] para el análisis.

pfSense no es tan elegante como los aparatos rastreadores comerciales, pero ofrece una funcionalidad adecuada para muchos propósitos, a un costo mucho menor.

Para obtener más información sobre cómo utilizar las funciones de captura de paquetes de pfSense, consulte el Capítulo 29, Paquete
Captura.

En pfSense 2.0 también puede agregar un puerto SPAN como parte de un puente, que retransmite una copia de cada trama recibida en el puente. Esto puede ser usado para monitorear pasivamente el tráfico en otro dispositivo, tal como un sistema que ejecuta snort para el análisis del tráfico, sin interrumpir el flujo de tráfico.

DHCP Server Appliance

Un usuario despliega pfSense instala estrictamente como DHCP servidores (Protocolo de configuración dinámica de host)
para distribuir direcciones IP de su red. En la mayoría de los entornos de esto probablemente no tiene mucho sentido. Pero en este caso, el personal de los usuarios ya estaban familiarizados y cómodos con pfSense y esto permitido nuevos despliegues sin capacitación adicional para los administradores, que fue un importante consideración en este despliegue.

Versiones

En esta sección se describen las distintas versiones pfSense disponibles actualmente y en el pasado.

2.1 de estreno

El comunicado de pfSense 2.1 es la versión actual recomendada para todas las instalaciones. Las mejoras en el punto 2.1 se centran principalmente en torno a la adición de soporte para IPv6, lo que ha sido toda una tarea de gran envergadura,
que afecta a casi todas las partes del sistema. pfSense 2.1 se basa en FreeBSD 8.3-RELEASE. Porque esta es la última versión oficial, que es la única versión que recibirá correcciones de errores y actualizaciones de seguridad.
Puede encontrar la versión actual recomendada por la navegación a www.pfsense.org / versiones [http://www.pfsense.org / versiones]. A menos que se indique lo contrario, las características mencionadas en este libro sólo pueden ser
disponibles en 2.1, pero los fundamentos deben ser similares en las versiones más recientes.

2.0.1 Release

pfSense 2.0.1 fue lanzado como una versión de seguridad y corrección de errores / Mejora menor. Se dirigió a una de seguridad
problema con la generación de los certificados y trajo algunas correcciones de errores y mejoras para las cosas que se encuentra después de 2.0 fue lanzado. Todavía se basa en FreeBSD 8.1-RELEASE.

2.0 de estreno

La 2.0 versión pfSense (anteriormente conocida como 1.3) es la versión recomendada para todas las instalaciones. Lo contiene numerosas mejoras significativas con respecto a versiones anteriores que se tratarán a lo largo de este libro. Se basa en FreeBSD 8.1-RELEASE. El ciclo de lanzamiento de 2,0 pasó mucho más tiempo que esperado, pero se trata de un lanzamiento muy ambicioso en cuanto a características adicionales y mejoras. Como tal, se requiere mucho más extensas pruebas y depuración. Tenemos la esperanza de acortar el ciclo de liberación de futuras versiones, quizá liberando cada 6 meses más o menos.

1.2.3 Release

Sigue siendo bastante popular, esta versión anterior se utiliza en muchas áreas que aún no se han actualizado a 2.0 para diversas razones. La versión 1.2.3 proporciona una serie de correcciones de errores y mejoras de la 1.2.2, y actualizado el sistema operativo de base a FreeBSD 7.2. En este libro, a 1.2 en su mayoría incluyen cada versión 1.2.x, aunque algunas cosas mencionadas en este libro sólo existen en 1.2.3 y versiones posteriores.

1.2, 1.2.1, 1.2.2 Releases

1.2 fue la primera versión estable en la línea de comunicados de 1,2, y se puso a disposición el 25 de febrero, 2008. La actualización 1.2.1 proporciona una serie de correcciones de errores y algunas actualizaciones de seguridad de menor importancia, y se actualiza
el sistema operativo de base a FreeBSD 7.0. La versión 1.2.2 añade un par de correcciones de errores.

1.0 de estreno

Esta fue la primera versión de pfSense clasifica como estable. Fue lanzado el 4 de octubre de 2006, con un seguimiento 1.0.1 versión de corrección de errores de 20 de octubre de 2006. Aunque sabemos de las instalaciones aún en marcha algunos
versiones alpha temprana y un sinnúmero de sitios aún en marcha 1.0, ya no se admite y fuertemente Recomendamos a todos los usuarios actualizar a 1.2.3. 1.0.1 contiene varias vulnerabilidades de seguridad de menor importancia fijos en
ya sea 1.2 o 1.2.1.

Estrenos de instantáneas

El servidor de instantáneas pfSense construye una nueva imagen a partir del código actualmente en nuestro repositorio de código fuente
o bien cada 24 horas, o antes si existe un compromiso con el árbol. Estos son principalmente para los desarrolladores y usuarios de prueba correcciones de errores, a petición de un desarrollador. Las instantáneas no siempre pueden estar disponibles, dependiendo
en el punto en el ciclo de lanzamiento. Poco después de la versión 1.2, las instantáneas fueron tomadas fuera de línea, el construir infraestructura se ha actualizado para FreeBSD 7.0 y el 1.3 (en ese momento, más tarde convertido en el 2.0) nota estuvo preparada para las primeras versiones disponibles públicamente. Lo mismo se hizo entre 2,0 y 2,1.
Pueden existir situaciones similares en el futuro. Usted puede ver lo que las instantáneas, si los hay, están disponibles visitando
el servidor de la instantánea [http://snapshots.pfsense.org]. La instantánea se basa son detenidos frecuentemente si hay es un gran lote de confirmaciones en curso u otra depuración de construcción pasando.

Plataformas

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

Live CD (incluyendo la imagen memstick USB)

La plataforma Live CD le permite ejecutar directamente desde el CD (o lápiz de memoria USB) sin la instalación en un disco duro o la tarjeta Compact Flash. Las referencias al "Live CD" en todo el libro también se refieren a la imagen memstick USB. La configuración se puede guardar en un disquete o flash USB conducir. El CD no se accede con frecuencia después de arrancar desde el sistema funciona principalmente desde la RAM en ese
punto, pero no debe ser eliminado de un sistema en funcionamiento. En la mayoría de las circunstancias, esto sólo debería ser
utilizado como una evaluación del software con el hardware en particular. Muchas personas no lo usan a largo plazo, pero se recomienda el uso de las instalaciones nuevas en su lugar. Usuarios de Live CD no pueden utilizar los paquetes, y lo histórico
gráficos de rendimiento se pierden al reiniciar.

Instale completa

El Live CD incluye una opción de instalación para instalar pfSense en el disco duro en su sistema. Es el medio preferido para correr pfSense. El disco duro entero debe ser sobrescrito; el arranque dual con otro sistema operativo no es compatible. Las instalaciones nuevas se recomienda para la mayoría de las implementaciones. De descarga
estadísticas podemos suponer al menos el 80% de todos los despliegues de pfSense son las instalaciones nuevas. La mayoría de los
los desarrolladores utilizar las instalaciones nuevas, principalmente si no del todo. Por lo tanto, es la más ampliamente probado y mejor
versión compatible. No tiene algunas de las limitaciones de las otras plataformas.

Embedded

La versión incorporada está diseñado específicamente para su uso con cualquier hardware usando Compact Flash (CF) en lugar de un disco duro. Las tarjetas CF pueden manejar solamente un número limitado de escrituras, así que la versión incorporada
carreras de sólo lectura de CF, con los sistemas de archivos de lectura / escritura como discos RAM. Incluso con esta limitación, que están
ampliamente apoyada en hardware embebido y vía convertidores-IDE-a CF. Aunque las tarjetas CF son más pequeños de un conector de disco duro ATA tradicional, el número de pines es la misma y que son compatibles.
Esto hace que sea más fácil de aplicar para los dispositivos que ya soportan IDE. CF siendo los medios de estado sólido, usted también no tiene la posible quiebra de un disco giratorio que preocuparse.

Los sistemas empotrados son populares por muchas razones, pero las más convincentes es que por lo general tienen pocas o ninguna pieza móvil, y consumir mucha menos energía y producen menos calor que el mayor sistemas mientras que todavía realizar lo suficientemente bien como para las necesidades de la mayoría de las redes. En este caso, menos movimiento
piezas significa menos puntos de falla, menos calor, y pueden funcionar completamente en silencio.

Históricamente, ha sido incorporado un ciudadano de segunda clase con pfSense, como las instalaciones nuevas han sido la
objetivo principal del proyecto. Esto ha cambiado con la generación actual de embebido, basado en NanoBSD.

Uno de los inconvenientes de los sistemas embebidos es que algunos de los datos de gráficos históricos RRDtool está perdido si
el sistema no se cierra correctamente. Por ejemplo, un corte de energía causará algo de pérdida de datos gráfica. Esto no afecta a la funcionalidad, pero dejará puntos en blanco en sus gráficos históricos. Usted puede configurar Las copias de seguridad periódicas de los datos RRD, que mitiga este riesgo algo. Datos RRD también se pueden respaldar
con la config.

Antiguo Embedded (pre-1.2.3 release)

Los paquetes no se admiten en las versiones más antiguas incrustadas 1.2.2 y anteriores. Older incrustado actualizaciones también no siempre funcionan de forma fiable. El único 100% garantizado medio fiable de mejora instalaciones embebidas era una copia de seguridad de la configuración, re-flash de la CF, y restaurar la configuración. Estas limitaciones han sido eliminados en la nueva configuración incrustado.

NanoBSD Embedded

NanoBSD es un medio estándar de la construcción de FreeBSD en una manera amistosa incrustado. Es compatible con dual firmware, y es fiable actualizable. En el momento de escribir estas líneas, NanoBSD incrustado es totalmente funcional y que se utiliza en la producción. La versión 1.2.3 comenzó a utilizar esta metodología integrada, momento en el que el viejo incrustado se interrumpió. 2.0 y más recientes liberaciones sólo utilizan el nuevo metodología incrustado.

Además de la compatibilidad con varios firmware Habilitación para la conmutación entre dos instalaciones diferentes, esto
trae dos beneficios adicionales importantes. Los paquetes son compatibles, por las que son adecuadas para un embebido medio ambiente. También permite la creación de cruz para arquitecturas de hardware que no sean x86, con MIPS y potencialmente plataformas ARM están apoyando en el futuro.

Interfaz Terminología de nomenclatura

Esta sección describe la terminología nombrar interfaz utilizada en pfSense y FreeBSD. La mayoría de la gente están familiarizados con las dos divisiones básicas de la red: "WAN" y "LAN", pero no puede haber tantos segmentos como se puede imaginar. Usted está limitado únicamente por el número de interfaces (o VLAN) que tiene a su disposición. Comenzando con pfSense 2.0, puede cambiar el nombre de cada interfaz para el nombre que quiera. En versiones anteriores, sólo se podía cambiar el nombre de las interfaces opcionales, no WAN / LAN.

Durante el examen de los nombres de interfaz, el tema de la segmentación de la red también viene a la mente. Es un buena práctica para mantener diferentes conjuntos de sistemas separados unos de otros. Por ejemplo, usted no desea que su
servidor web de acceso público en la misma red que su red LAN. Si el servidor se ha visto comprometida, la atacante podría llegar fácilmente a cualquier sistema de la LAN. Si usted ha dedicado los servidores de bases de datos, estos pueden
ser aislado de todo lo demás y se asegura de todo, excepto los servidores de base de datos que necesitan acceso. Al igual que en el ejemplo anterior, un servidor web comprometido no pondría en peligro la base de datos servidores casi tanto como si estuvieran en el mismo segmento sin un firewall en el medio.

LAN

La interfaz LAN es la primera interfaz interna del servidor de seguridad. Abreviatura de red de área local, es más comúnmente el lado privado de un router que a menudo utiliza un esquema de dirección IP privada. En pequeña despliegues, esto es normalmente la única interfaz interna.

WAN

La interfaz WAN se utiliza para la conexión a Internet, conexión a Internet o primaria en un multi-Despliegue de WAN. Abreviatura de Red de área amplia, que es la red pública no es de confianza fuera de su router. Las conexiones de Internet llegarán a través de la interfaz WAN.

OPT

Opt o Interfaces opcionales se refieren a las interfaces conectadas a las redes locales distintos de LAN. OPT interfaces se utilizan comúnmente para la segunda segmentos LAN, segmentos DMZ, redes inalámbricas y mucho más.

OPT WAN

OPT WAN se refiere a las conexiones a Internet mediante una interfaz OPT, tanto las configuradas por DHCP o especificar una dirección IP de puerta de enlace. Esto se discute en detalle en el capítulo 15, Múltiples conexiones WAN.

DMZ

Corto para la zona desmilitarizada. El término fue tomado de su significado militar, que se refiere a una especie de amortiguación entre un área protegida y una zona de guerra. En las redes, es un área donde su público servidores residen es accesible desde Internet a través de la WAN, sino que también está aislada de la red LAN de manera
que un compromiso en la DMZ no ponga en peligro los sistemas de otros segmentos.

Algunas empresas emplean mal el término "zona de distensión" en sus productos de servidor de seguridad en referencia a NAT 01:01 en el
WAN IP que expone una serie en la LAN. Hay más información sobre este tema en la sección llamado "NAT 01:01 en la IP WAN, también conocido como" zona de distensión "en Linksys".

Interfaz de FreeBSD nombramiento

Nombres de FreeBSD sus interfaces por el controlador de red utilizado, seguido por un número que comienza en 0 y incrementando en uno para cada interfaz adicional usando ese controlador. Por ejemplo, un conductor común es `em`, utilizado por Intel PRO/1000 tarjetas. La primera tarjeta de Pro/1000 en un sistema será `em0`, la segunda es `em1`, y así sucesivamente. Otras de las más comunes son `IGB` (También Intel Pro/1000), `bge` (varios chipsets Broadcom), `rl`
(Realtek 8129/8139), entre muchos otros. Si el sistema se mezcla una tarjeta Pro/100 y una Realtek 8139, las interfaces estarán `fxp0` y `rl0` respectivamente. Asignaciones de interfaz y nombres son más cubierto en el Capítulo 4, Instalación y actualización.

Búsqueda de información y Obtención de ayuda

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

Búsqueda de información

La forma más fácil de encontrar información sobre un tema específico en este libro es comprobar el Índice. Todos los más
características e implementaciones comunes de pfSense se tratan en este libro, y el Índice le ayudará 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 información adicional y experiencias de usuario disponibles en los diversos sitios pfsense.org. La mejor manera de buscar todos estos sitios es a la cabeza a Google, escriba los términos que usted está buscando, y añadir sitio: pfsense.org a su consulta. Esto buscará la página web, foro, CVSTrac, wikis, 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. Este también localizar información en las porciones de libre acceso de este libro.

Obtención de ayuda

En pfSense 2.0 y versiones posteriores, hay un icono de ayuda en casi cada página,. Al hacer clic en este icono de ayuda se llevará a
usted a una página asociada en nuestra wiki de documentación con información adicional sobre la página que están viendo, o la función general que está utilizando. El proyecto pfSense ofrece otras maneras de obtener ayuda, incluyendo un foro [http://forum.pfsense.org], wiki documentación [http://doc.pfsense.org], listas de correo e IRC (Internet Relay Chat, # # pfSense en irc.freenode.net). Soporte comercial es
También está disponible mediante suscripción de los fundadores del proyecto pfSense en el Portal de pfSense [https://portal.pfsense.org]. Usted puede encontrar más información sobre todas estas vías de apoyo en la obtención de Soporte [http://www.pfsense.org/support] página en el sitio pfSense. Muchos de ellos también están vinculados de el 2.0 GUI pfSense en el menú Ayuda.

Capítulo 2. Conceptos de Redes

Si bien este no es un libro de introducción de redes, hay ciertos conceptos de red que son importante entender. Esta parte del libro no proporcionará cobertura adecuada para los que carecen de conocimientos básicos de redes fundamental. Si usted no posee este conocimiento, es probable que necesite para buscar material de la creación de redes de introducción adicional.

Los lectores con un conocimiento significativo de IP pública y privada de direccionamiento, las subredes IP, notación CIDR
y resumen CIDR puede saltar al siguiente capítulo. Habrá alguna mención de IPv6 relacionados
temas aquí, pero la cobertura más profunda se pueden encontrar en la sección denominada "IPv6". Nosotros normalmente referirse a las direcciones IP tradicionales como direcciones IPv4 para mayor claridad. La mayoría de las funciones trabajarán con cualquiera
Direcciones IPv4 o IPv6, excepto donde se indique lo contrario, por lo que si nos referimos a una dirección IP en general, puede significar una de cualquiera de familia de direcciones.

Comprensión Pública y Private IP Direcciones

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

Direcciones IP privadas

Las direcciones IP privadas son las que dentro de una subred reservado, para uso exclusivamente interno. El estándar de red
RFC 1918 [http://www.faqs.org/rfcs/rfc1918.html] define subredes IPv4 reservadas para su uso en privado redes (Tabla 2.1, "RFC 1918 Dirección IP Private Space"), y RFC 4193 [http://tools.ietf.org/html/rfc4193] define direcciones locales únicas (ULA) para IPv6 (Tabla 2.2, "RFC 4193 Unique Local Espacio de direcciones "). En la mayoría de los entornos, se elige una subred IP privada de RFC 1918 y utilizado en todos los dispositivos de la red interna, que luego se conectan a Internet a través de un firewall o router la implementación de la traducción de direcciones de red (NAT), como pfSense. Para IPv6, se debe utilizar Direcciones Global Unicast (GUA), que están completamente enrutados, incluso en sus redes internas, sin NAT. NAT se explicará en el capítulo 11, La traducción de direcciones de red.

Cuadro 2.1. RFC 1918 Dirección IP Privado

Rango CIDR	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

Cuadro 2.2. RFC 4193 Único espacio de direcciones locales

Prefijo	Intervalo de direcciones IP
FC00 :: / 7	FC00 :: - fdff: ffff: ffff: ffff: ffff: ffff: ffff: ffff

Para IPv4 han sido históricamente reservadas otras gamas como 1.0.0.0 / 8 y 2.0.0.0 / 8, pero estos No se reservan de forma permanente, como las direcciones RFC 1918 y muchos ya se han asignado como el espacio de direcciones IPv4 se ha agotado. Era tentador utilizar estos, y en algunas redes puede seguir usando ellos, sino porque esas redes se han asignado, sin dejar de utilizar esas IPs dará lugar a la imposibilidad de llegar a cualquier sistema en esas nuevas redes. También debe evitar el uso de 169.254.0.0/16, que de acuerdo con RFC 3927 se reserva para la autoconfiguración "de enlace local" -, pero no debe ser asignada por DHCP o manualmente. Hay más que suficiente espacio de direcciones reservado por la RFC 1918, como se muestra en la Tabla 2.1, "RFC 1918 Dirección IP Private Space", por lo que hay poco incentivo para desviarse de esa lista. Nos hemos encontrado con las redes con todo tipo de direccionamiento incorrecto, y será conducir a problemas - no es una cuestión de "si", sino "cuándo" van a surgir problemas. Si usted se encuentra trabajar en una red existente mediante un espacio de direcciones inadecuada, lo mejor es corregir el direccionamiento

tan pronto como sea posible. Una lista completa de uso especial las redes IPv4 se puede encontrar en el RFC 3330 [http://tools.ietf.org/html/rfc3330].

Las direcciones IP públicas

Las direcciones IP públicas son los asignados por su ISP para todos, pero los más grandes redes. Redes que requieren cientos o miles de direcciones IP públicas suelen tener espacio de direcciones asignado directamente desde el Registro Regional de Internet que cubre su región del mundo. Registros Regionales de Internet son el organizaciones que supervisan la asignación y el registro de la dirección IP pública de su región designada del mundo.

La mayoría de las conexiones de Internet residenciales vienen con una sola dirección IPv4 pública, mientras que la mayoría de negocios
conexiones de clase vienen con la opción de utilizar varias direcciones IP públicas si es necesario. Una sola dirección IP pública
es adecuada en muchas circunstancias y puede ser utilizado en conjunción con NAT para conectar cientos de dirigida privadamente sistemas a Internet. El contenido en este libro le ayudará a determinar la número de IPs públicas que requiere la red.
La mayoría de las implementaciones de IPv6 le dará al usuario final al menos una red de prefijo / 64 para su uso como un interno encaminado
red, que es de aproximadamente 264 direcciones IPv6, o 18 quintillón direcciones de su sitio, totalmente enrutada desde Internet sin necesidad de NAT.

Conceptos IP de subredes

Al configurar los parámetros de TCP / IP en un dispositivo, una máscara de subred (o longitud de prefijo para IPv6) deben ser
especificado. Esta máscara permite al sistema determinar qué direcciones IP están en la red local, y que debe ser alcanzado por una puerta de entrada en la tabla de enrutamiento del sistema. El valor predeterminado 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 discute en la sección denominada "Entendimiento CIDR Máscara de subred Notación".

Dirección IP, subred y la puerta Configuración

La configuración TCP / IP de un host se compone de tres cosas principales - dirección, máscara de subred (o prefijo longitud para IPv6) y la puerta de enlace. La dirección IP y la máscara de subred combinado es cómo sabe el anfitrión las direcciones IP que están en su red local. Para cualquier dirección fuera de la red local, se envía el tráfico (Enrutado) a la puerta de enlace predeterminada configurada que debe saber cómo llegar al destino deseado. Un excepción a esta regla es una ruta estática, que indica a un router o un sistema de cómo ponerse en contacto específica subredes no locales accesibles a través de los routers conectados localmente. Esta lista de pasarelas y rutas estáticas es mantiene en cada host en su tabla de enrutamiento. Para ver la tabla de enrutamiento utilizado por pfSense, consulte la sección llamada
"Visualización de rutas". Más información sobre el enrutamiento se puede encontrar en el capítulo 12, Routing.

En una implementación típica pfSense, los anfitriones se les asignará una dirección IP dentro del rango de la LAN de pfSense,
la misma máscara de subred que la interfaz LAN de pfSense, y el uso de IP LAN de pfSense como su defecto puerta de enlace. Lo mismo se aplica a los hosts conectados a una interfaz que no sea LAN, utilizando el apropiado configuración para la interfaz a la que está conectado el dispositivo.

Las máquinas de una sola red se comunican 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 la comunicación
dentro de un segmento de red. Si se requiere esta funcionalidad, ya sea anfitriones necesitan ser segmentados a través de la utilización
de múltiples conmutadores o VLANs o funcionalidad de switch equivalente como PVLAN debe ser empleada.
Las VLAN se tratan en el Capítulo 14, LAN virtuales (VLAN).

La comprensión de subred CIDR Máscara Notación

pfSense utiliza un formato de máscara de subred es posible que no esté familiarizado. En lugar de la 255.x.x.x común, utiliza CIDR (classless InterDomain Routing) notación.

Se puede hacer referencia a la Tabla 2.3, "subred en CIDR Tabla" para encontrar el equivalente CIDR de su máscara de subred.

Cuadro 2.3. CIDR Subred Cuadro

Máscara de subred	CIDR Prefijo	Total Direcciones	IP utilizable Direcciones	IP Número de / 24 redes
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	1 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	16384	16382	64
255.255.128.0	/ 17	32768	32766	128
255.255.0.0	/ 16	65536	65534	256
255.254.0.0	/ 15	131072	131070	512
255.252.0.0	/ 14	262144	262142	1024
255.248.0.0	/ 13	524288	524286	2048
255.240.0.0	/ 12	1048576	1048574	4096
255.224.0.0	/ 11	2097152	2097150	8192
255.192.0.0	/ 10	4194304	4194302	16384
255.128.0.0	/ 9	8388608	8388606	32768
255.0.0.0	/ 8	16777216	16777214	65536
254.0.0.0	/ 7	33554432	33554430	131072
252.0.0.0	/ 6	67108864	67108862	262144
248.0.0.0	/ 5	134217728	134217726	1048576
240.0.0.0	/ 4	268435456	268435454	2097152
224.0.0.0	/ 3	536870912	536870910	4194304
192.0.0.0	/ 2	1073741824	1073741822	8388608
128.0.0.0	/ 1	2147483648	2147483646	16777216
0.0.0.0	/ 0	4294967296	4294967294	33554432

Entonces, ¿dónde estas cifras CIDR provienen 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. Este se suma a los 24 o / 24 (pronunciado "slash veinticuatro ').

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

CIDR Summarization

Además de especificar las máscaras de subred, CIDR también se puede emplear para IP o red de resúmenes propósitos. La columna "Direcciones IP Total" en la tabla de subred CIDR indica cuántas direcciones una máscara CIDR dado resumirá. Para los propósitos de resumen de red, el "número de / 24 redes columna "es útil. CIDR resumen se puede utilizar en varias partes de la web pfSense interfaz, incluyendo las reglas de firewall, NAT, IPs virtuales, IPsec, rutas estáticas, y más.

IPs o redes que pueden estar contenidos en una sola máscara CIDR se conocen como CIDR summarizable.

En el diseño de una red usted debe asegurarse de que todas las subredes IP privadas en uso en un lugar en particular son Summarizable CIDR. Por ejemplo, si necesita tres / 24 subredes en un solo lugar, utilice una red / 22 subredes en cuatro / 24 redes. La siguiente tabla muestra los cuatro / 24 subredes puede usar con la subred 10.70.64.0/22.

Cuadro 2.4. CIDR de resumen de ruta

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

Esto ayuda a mantener el enrutamiento más manejable para redes multi-sitio (aquellos conectados a otro físico ubicación a través de la utilización de un circuito de WAN privada o VPN). Con subredes summarizable CIDR, usted tiene uno
destino de la ruta que cubre todas las redes en cada lugar. Sin ella, usted tiene varias diferentes redes de destino al lugar.

Ahora, si usted no es un gurú de la división en subredes, te estás preguntando cómo diablos se me ocurrió la tabla anterior. Comience eligiendo un prefijo CIDR para su red, de acuerdo con el número de redes que se requieren. A continuación, elija una red / 24 que desea utilizar. Para ese ejemplo, elegí 10.70.64.0/24. Sé de la memoria que xx64.0/24 habrá primera red / 24 en un / 22, pero no tienes que escoger el primera red. Se puede calcular fácilmente este uso de las herramientas disponibles en el subnetmask.info [http://www.subnetmask.info] Sitio web.

Una de las herramientas será convertir de decimal con puntos para la máscara CIDR, y viceversa, esta función se muestra En la Figura 2.1, "Convertidor Máscara de subred". Si usted no tuvo la Tabla 2.3, "Tabla de subred CIDR" de anteriormente en este capítulo, en frente de usted, usted puede convertir su prefijo CIDR elegido decimal con puntos notación uso de esta herramienta. Introduzca un prefijo CIDR y haga clic en el botón Calcular a su derecha, o introduzca un punteada
máscara decimal y haga clic en el botón Calcular a su derecha.

Figura 2.1. Máscara de subred Convertidor

Armado con la máscara decimal con puntos, ahora vaya a la sección de red / nodo Calculadora. Ponga en el máscara de subred y una de las / 24 redes que desea utilizar. Luego haga clic en Calcular. Las cajas inferiores rellenará, y le mostrará el rango cubierto por esa particular / 24, que se puede ver en la Figura 2.2,

"Red / Nodo Calculadora". En este caso, la dirección de red será 10.70.64.0/22, y se puede ver que los utilizable / 24 redes serán de 64 a 67. "Dirección de difusión" no es la terminología relevante cuando se utiliza esta herramienta para determinar un rango CIDR, que es simplemente la dirección más alta en la gama.

Figura 2.2. Red / Calculadora Nodo

Encontrar a una red CIDR juego

Intervalos de IP en el formato de xxxx-aaaa se admiten en los nombres en 2.0. Un rango de direcciones IP de forma automática
convertido al conjunto equivalente de bloques CIDR. Vea la sección llamada "Alias" para obtener más información.

Si usted no necesita necesariamente una coincidencia exacta, se puede conectar en número a la Calculadora de red / nodo para acercarse a su resumen deseada.

Broadcast Dominios

Un dominio de difusión es la parte de una red de compartir el mismo segmento de la capa dos de red. En una red con un solo interruptor, el dominio de difusión es que todo cambia. En una red con múltiples conmutadores interconectados sin el uso de VLAN, el dominio de difusión incluye todos los interruptores.

Un único dominio de difusión lata contener más de un IPv4 o IPv6 de subred, sin embargo, que es generalmente no se considera un buen diseño de red. Subredes IP deben ser segregados en dominios de difusión separados a través de el uso de interruptores separados, o VLAN. La excepción a esto, implícita en la frase anterior, es que se puede ejecutar redes IPv4 e IPv6 dentro de un único dominio de difusión. Esto se llama de doble apilar, y es una técnica común y útil tener tanto IPv4 como IPv6 conectividad para los anfitriones.

Dominios de difusión pueden ser combinados, cerrando dos interfaces de red en conjunto, pero se debe tener tomado para evitar bucles de conmutación en este escenario. También hay algunos sustitutos de ciertos protocolos que no combine dominios de difusión, pero le dará el mismo efecto, como un relé DHCP que relés DHCP solicita al dominio de la difusión de otra interfaz. Más información sobre los dominios de difusión y cómo combinar las mismas puede encontrarse en el capítulo 13, Tender un puente.

IPv6

Lo esencial

Las preocupaciones de Firewall y VPN

Vea la sección llamada "IPv6 VPN y reglas del cortafuegos" para una discusión más a fondo.

Requerimientos

Tipos IPv6 WAN

Formato de dirección

Vecino Discovery

Router Advertisements

Asignación de direcciones

DHCPv6 Prefijo Delegación

IPv6 y pfSense

Paquetes pfSense

Conexión con un Service Broker Túnel

Capítulo 3. Hardware

pfSense es compatible con cualquier hardware que sea compatible con la versión de FreeBSD en uso, en i386 y plataformas de hardware AMD64. Arquitecturas de hardware alternativos tales como PowerPC, MIPS, ARM, SPARC, etc, no son compatibles en este momento. El nuevo incrustado puede traer MIPS y ARM algún apoyo en el futuro, a pesar de que no está disponible en el momento de este escrito. Comenzando con pfSense 2.0, hay ahora tanto una versión de 64 bits (amd64) y 32 de liberación bit (i386). Las versiones anteriores eran sólo de 32 bits, aunque la liberación de 32 bits se ejecuta bien en hardware de 64 bits. Vea la sección llamada "32 bits vs 64 bits" para más información sobre 32 bits vs 64 bits arquitecturas.

Compatibilidad de hardware

El mejor recurso para determinar el hardware compatible es las Notas Hardware FreeBSD para la liberación versión utilizada por la liberación pfSense que está instalando. pfSense 2.1 se basa en FreeBSD 8.3, por lo tanto una referencia definitiva sobre el hardware compatible serían las notas de hardware en http://www.freebsd.org/releases/8.3R/hardware.html. El más general FreeBSD hardware FAQ es otro buen recurso para utilizar para ayudar a la selección de hardware. Se puede encontrar en http://www.freebsd.org/doc/en_US.ISO8859-1/libros / faq / hardware.html. En esta sección se proporcionará orientación sobre el hardware mejor soportado disponibles a los efectos de cortafuegos y enrutamiento. La consideración primordial y única recomendación fuera de las notas de hardware es para los adaptadores de red.

Adaptadores de red

Prácticamente todas las tarjetas Ethernet con cables (NIC) son apoyados por pfSense. Sin embargo, no todos los adaptadores de red son creados iguales. El hardware utilizado puede variar en gran medida en la calidad de un fabricante a otro, y en algunos casos, mientras que FreeBSD puede soportar un NIC particular, la compatibilidad de controladores puede ser pobre con una implementación específica del chipset.

Intel PRO/1000 Pro/100 y tarjetas de red son los más comúnmente recomendada porque no tienen conductor sólido apoyo en FreeBSD escrito por los empleados de Intel, y un buen desempeño. En el otro extremo del espectro, Realtek 8139 `rl` tarjetas son muy comunes pero muy pobre hardware de calidad. 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 hecha por SMC. "exacerbando el problema es el hecho de que numerosos fabricantes incorporar este conjunto de chips en sus tarjetas de red, con muy diferentes grados de calidad. Usted encontrará 8139 tarjetas integrado en un hardware integrado, y los que en general son fiables y funcionan correctamente. De los varias tarjetas PCI que existen, algunos funcionan bien, y algunos tienen varias cosas que están rotas. VLANs puede no funcionar correctamente o en absoluto, y el modo promiscuo requerido para puentear puede no funcionar, entre muchas otras posibilidades.

Si usted tiene tarjetas de red disponibles y está construyendo un sistema de piezas de repuesto, vale la pena probar lo que tener a mano. Muchas veces ellos no tendrán ningún problema. Si usted está buscando para comprar hardware para la implementación, ir con tarjetas Intel. En las redes donde la fiabilidad y el rendimiento son de suma preocupación, no lo hagas escatimar en costes mediante el uso de cualquier NICs le sucede a haber por ahí (a menos que los que resultan ser Intels).

Si utiliza VLAN, asegúrese de seleccionar los adaptadores que soportan el procesamiento de VLAN en el hardware. Es discutido en el Capítulo 14, LAN virtuales (VLAN).

Adaptadores de red USB

Muchos adaptadores de red USB son compatibles, pero generalmente no se recomiendan. Ellos funcionan mal, especialmente en los sistemas que no soporten USB 2.0, o con adaptadores que son estrictamente USB 1.1. USB NICs son grandes en un apuro, o al añadir conectividad de red a una PC de escritorio, y están muy bien para algunas implementaciones de firewall a casa, pero para un rendimiento fiable en el centro de datos no deben ser considerado.

Adaptadores Inalámbricos

Adaptadores y recomendaciones inalámbricos compatibles se tratan en la sección llamada "drivers inalámbricos incluido en 1.2.3 ".

Requisitos mínimos de hardware

A continuación se describen los requisitos mínimos de hardware para pfSense 2.1. Tenga en cuenta el mínimo requisitos no son adecuados para todos los entornos; consulte la sección llamada "Hardware acerca de Orientación" como guía el hardware utilizado.

Requisitos Base

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

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

Requisitos Específicos de la Plataforma

Requisitos específicos de las plataformas individuales siguen.

Live CD

• CD-ROM, DVD u otra unidad óptica capaz de arrancar un CD-ROM
• unidad flash USB o una unidad de disco flexible para almacenar el archivo de configuración

Instalación completa

• CD-ROM o una unidad USB de arranque para la instalación inicial
• Disco duro 1 GB o más

NanoBSD Embedded

• 512 MB o más Tarjeta Compact Flash
• Puerto serie para la consola
• Cable de módem nulo para conectar al puerto de consola

A partir de pfSense 2.0.1 también ofrecemos imágenes nanobsd para sistemas con consolas VGA, por lo que la serie consola ya no es un requisito para sistemas capaces de utilizar esas imágenes.

Selección de hardware

Los sistemas operativos de código abierto pueden inducir numerosos dolores de cabeza con la compatibilidad de hardware. Mientras
una determinada pieza de hardware puede ser apoyado, una implementación específica de que puede no funcionar correctamente, o ciertas combinaciones de hardware no pueden funcionar. Esto no se limita a FreeBSD (y por lo tanto pfSense) - las distribuciones de Linux también sufren el mismo destino. En más de una década de experiencia en el uso BSD y varias distribuciones de Linux en una amplia variedad de hardware, he visto a este en innumerables ocasiones. Algunos sistemas que funcionan bien con Windows no van a funcionar con BSD o Linux, algunos funcionan bien con BSD, pero no Linux, algunas con Linux pero no BSD. Si le sucede a correr en el hardware relacionado problemas, la sección "Solución de problemas de hardware" ofrece consejos que va a resolver estos problemas en algunos casos.

La prevención de los dolores de cabeza de hardware

Esta sección ofrece algunos consejos sobre cómo evitar problemas de hardware.

Utilice el hardware de los desarrolladores utilizan

A través de los años, varios fabricantes de hardware han donado mucho equipo de prueba necesarios para nuestros desarrolladores.
Mediante el uso de este equipo con estos proveedores, se asegura de que el dispositivo que está comprando está bien probado, y
si se producen regresiones de FreeBSD que afectan al hardware en el futuro, van a ser fijos, incluso antes de sabían que existían. Animamos a nuestra base de usuarios para apoyar a las empresas que apoyan el proyecto.
También estamos en las etapas de planificación de oferta de venta de hardware directos, ofreciendo hardware preinstalado
plataformas que usan, y saben que es sólida como una roca y es totalmente compatible. Visita http://www.pfsense.org/ vendedores de la más actualizada información actualizada sobre los proveedores de hardware recomendados.

Búsqueda de las experiencias de los demás

Si está utilizando una pieza de hardware de un fabricante importante, si escribe su marca, el modelo, y sitio: pfsense.org en Google, hay una alta probabilidad de que usted encontrará a alguien que ha tratado o es el uso de ese hardware. También puede intentar la búsqueda de la marca, el modelo, y pfSense a encontrar experiencias de personas han reportado en otros sitios web o los archivos de las listas. Informes de fracaso que no debe necesariamente ser considerados como definitivos, ya que los problemas de un único usuario en un sistema en particular podría
ser el resultado de hardware defectuoso u otra anomalía en lugar de incompatibilidad. La repetición de estos mismas búsquedas con FreeBSD en lugar de pfSense también pueden aparecer experiencias de usuario útiles.

32 bits vs 64 bits

El principal beneficio que ofrece una versión de 64 bits en relación con los cortafuegos es la capacidad para abordar de manera más
memoria, y aunque incluso el más grande pfSense instala proteger miles de máquinas no utilizan 4 GB de RAM con el sistema base, si usted está usando los paquetes de add-on puede ser necesaria la memoria RAM adicional. La
Versión de 32 bits de pfSense se ejecuta en hardware de 64 bits, por lo que es un lugar seguro para empezar si hay alguna incertidumbre.

Convenciones de nomenclatura

A lo largo de este libro, podemos referirnos a la versión de 64 bits como amd64, que es la denominación utilizada por FreeBSD para la arquitectura. Intel adoptó la arquitectura creada por AMD para x86-64, por lo tanto el nombrar amd64. La plataforma 32 bits se conoce como i386, que también es la designación usada por FreeBSD por su arquitectura de 32 bits.

Hardware Orientación acerca de

Al dimensionar el hardware para su uso con pfSense, dos factores principales deben ser considerados: el rendimiento necesarios y se utilizarán atributos. Las secciones próximos cubren estas consideraciones.

Consideraciones de rendimiento

Si necesita menos de 10 Mbps de rendimiento, puede llegar a funcionar con los requisitos mínimos. Para requisitos de rendimiento más altas se aconseja utilizar algunas directrices, basadas en nuestra amplia pruebas y experiencia de implementación. Estas directrices ofrecen un poco de espacio para respirar, ya que nunca desee ejecutar el hardware a su máxima capacidad durante períodos prolongados.

Su elección de la tarjeta de red tiene un impacto significativo en el rendimiento máximo alcanzable, dependiendo de la velocidad de su CPU. Tabla 3.1, "Máximo Throughput por CPU" muestra la máxima rendimiento alcanzable utilizando dos Realtek 8139 NIC en comparación con dos de escritorio Intel PRO/1000 GT NIC para las plataformas de hardware con ranuras PCI.

Cuadro 3.1. El rendimiento máximo de la CPU

CPU	Onboard MaxRealtekMax Pro/1000Max Rendimiento (Mbps) Rendimiento (Mbps) Rendimiento (Mbps)		
Pentium MMX 200 MHz	n / a	25 Mbps	40 Mbps

CPU	Onboard MaxRealtekMax Pro/1000Max Rendimiento (Mbps) Rendimiento (Mbps) Rendimiento (Mbps)		
WRAP - 266 MHz Geode	24 Mbps	n / a	n / a
ALIX - 500 MHz Geode	85 Mbps	n / a	n / a
VIA 1 GHz	93 Mbps (100 Mb n / a velocidad de cable)		n / a
Netgate Hamakua (1 GHz Celeron)	250 Mbps	n / a	n / a
Netgate FW-7535 (1,6 GHz D510 Atom)	485 Mbps	n / a	(A bordo es Pro/1000)
Pentium II 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 365 Mbps velocidad de cable)	

Diferencia de rendimiento por tipo de adaptador de red

Su elección de la NIC tendrá un impacto significativo en el rendimiento. Baratos tarjetas de gama baja como Realteks consumirá significativamente más CPU que las tarjetas de gran calidad tales como Intel. Su primer cuello de botella con rendimiento de firewall será su CPU. Usted puede obtener mucho más rendimiento de una CPU dada usando una mejor calidad de NIC, como se muestra en la Tabla 3.1, "Rendimiento máximo por la CPU" con la más lenta CPUs. Si usted tiene una CPU capaz de mucho más rendimiento que usted requiere, la elección de NIC tendrá poco o ningún impacto en el rendimiento, aunque NICs de menor calidad pueden resultar poco fiables en algunas circunstancias.

El tamaño de los rendimiento gigabit

Al dimensionar para implementaciones Gigabit, primero tiene que determinar la cantidad de rendimiento que realmente necesita - velocidad del cable 1 Gbps o simplemente más de 100 Mbps. En muchas redes no existen sistemas capaces de llenado 1 Gbps con los datos del disco, como el disco I de los sistemas de E / S es incapaz de tal ejercicio. Si sólo quiero ser capaz de golpear 200 Mbps, cualquier sistema de 1 GHz con tarjetas de red de buena calidad será suficiente. Para arriba a 400-500 Mbps, un servidor de 2-3 GHz mayores será suficiente, o una solución basada en Atom.

El tamaño de los múltiples gigabits por segundo despliegues

Los números en la tabla 3.1, "El rendimiento máximo por CPU" se detienen en un nivel relativamente bajo, porque eso es en la medida de lo que podemos probar razonablemente en nuestro laboratorio. Prueba múltiples Gbps servidores capaces requiere el servidores y varios sistemas capaces de empujar a 1 Gbps de velocidad de cable. No tenemos el equipo adecuado para esa escala de las pruebas. Pero eso no quiere decir que pfSense no es adecuado en un ambiente así; de hecho se utiliza en numerosos despliegues de empuje superiores a 1 Gbps.

Al dimensionar para implementaciones con varios Gbps, el factor principal es la de paquetes por segundo, no Gbps. Usted llegará al límite de FreeBSD y de más rápido hardware de servidor de cuatro núcleos de hoy en alrededor de 500.000 paquetes por segundo (pps). ¿Cuánto rendimiento que esto equivaldría a depende de su entorno de red, con algunas referencias proporcionadas en la Tabla 3.2, "500.000 pps a distintos tamaños de marco".

Cuadro 3.2. 500.000 pps a distintos tamaños de bastidor

Tamaño de la trama	El rendimiento en 500Kpps
64 bytes	244 Mbps

Tamaño de la trama	El rendimiento en 500Kpps
500 bytes	1.87 Gbps
1000 bytes	3.73 Gbps
1500 bytes	5.59 Gbps

Para implementaciones que buscan alcanzar la velocidad del cable 1 Gbps entre dos interfaces, un Pentium 4 a 3 GHz o CPU más rápida con PCI-X o PCI-e NICs debe ser utilizado. PCI le permitirá alcanzar varios cientos de Mbps, pero las limitaciones de velocidad de bus PCI le impedirá lograr un rendimiento a velocidad de cable con dos 1 Gbps NIC.

Si el hardware utilizado para algo capaz de un rendimiento a velocidad de cable Gigabit sobre múltiples interfases, conseguir un nuevo servidor con un procesador de cuatro núcleos y PCI-e NICs y usted estará en buena forma. Si usted necesita empujar más de 500.000 paquetes por segundo, puede superar la capacidad de los productos básicos Hardware de PC para empujar los paquetes. Consulte la sección llamada "LAN Router" para obtener más información.

Característica Consideraciones

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

Las tablas de estado grandes

La tabla de estado de servidor de seguridad es el lugar donde se realiza el seguimiento de conexiones de red activas a través del firewall, con cada
conexión que consume un estado. Unidos están cubiertos en el Capítulo 10, Firewall. Entornos
que requiere un gran número de conexiones simultáneas (y por consiguiente los Estados) requerirá RAM adicional. Cada estado tiene aproximadamente 1 KB de RAM. Tabla 3.3, "Gran Consumo Tabla de memoria de señal" proporciona una guía para la cantidad de memoria necesaria para un gran número de estados. Tener en mente esto es únicamente la memoria utilizada para el seguimiento del estado, los otros componentes de pfSense se requieren por lo
menos 32-48 MB de RAM adicional en la parte superior de este, y posiblemente más, dependiendo de las características en uso.

Cuadro 3.3. Gran Consumo Tabla de memoria de señal

Unidos	RAM requerida
100000	~ 97 MB
500000	~ 488 MB
1000000	~ 976 MB
3000000	~ 2900 MB

VPN (todos los tipos)

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

El cifrar y descifrar el tráfico de red con todos los tipos de VPN es muy intensivo de la CPU. pfSense ofrece varias opciones de cifrado para su uso con IPsec: DES, 3DES, cast128, Blowfish 128-256 bits (en 8 incrementos de bits), y AES de 128, 192 y 256 bits. Los diversos sistemas de cifrado actúan de forma diferente, y el el máximo rendimiento de su servidor de seguridad depende del cifrado utilizado. 3DES es ampliamente utilizado porque de su interoperabilidad con casi todos los dispositivos de IPsec, sin embargo, es el más lento de todos los sistemas de cifrado
apoyado por pfSense en ausencia de un acelerador de cifrado de hardware. Aceleradores criptográficos de hardware tales cartas como compatibles de Hifn aumentan en gran medida el máximo rendimiento de VPN, y en gran medida eliminar la diferencia de rendimiento entre los sistemas de cifrado. Tabla 3.4, "IPsec Throughput por Cipher - ALIX" espectáculos el rendimiento máximo por sistema de cifrado de hardware Motores ALIX PC (500 MHz Geode) y sin
con un acelerador criptográfico Soekris vpn1411 Hifn.

Cuadro 3.4. IPsec Throughput por Cipher - ALIX

Protocolo de cifrado	Rendimiento Máximo	Rendimiento máximo (con Hifn)
DES	13,7 Mbps	34,6 Mbps
3DES	8.4 Mbps	34,3 Mbps
Blowfish	16,5 Mbps	no acelerado (sin cambios)
CAST128	16,3 Mbps	no acelerado (sin cambios)
AES	19,4 Mbps	34,2 Mbps
AES 256	13,5 Mbps	34,2 Mbps

Tabla 3.5, "IPsec Throughput por CPU" muestra el máximo rendimiento de IPsec por la CPU para la Cifrado Blowfish de 128 bits, para ilustrar la capacidad máxima de rendimiento de varias CPUs.

Cuadro 3.5. IPsec rendimiento por la CPU

CPU	Blowfish Rendimiento (Mbps)
Pentium II 350	12,4 Mbps
ALIX (500 MHz)	16,5 Mbps
Pentium III 700	32,9 Mbps
Pentium 4 1.7 GHz	53,9 Mbps

Aceleradores criptográficos de hardware deben ser utilizados cuando se requiere gran ancho de banda a través de IPsec, excepto
con CPU dual o quad core, como aquellas CPUs realizan cripto más rápido que un acelerador, evitando
la comunicación en el bus PCI. Algunos chipsets VIA también apoyan el acelerador VIA candado crypto,
que también puede ayudar. En futuras versiones pfSense, el cortafuegos será capaz de tomar ventaja de AES-NI que debería mejorar drásticamente el rendimiento de cifrado de AES en los chipsets soportados,
a saber, Core i5 de Intel y la línea i7. Soporte para AES-NI no fue incluida en FreeBSD 8.1, así que no era
posible que pfSense 2.0 para incluir la función.

Paquetes

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

Bufido

Snort, el sistema de detección de intrusiones de red disponible en el sistema de paquetes pfSense, puede requerir una importante cantidad de RAM, dependiendo de su configuración. 256 MB deben considerarse un mínimo, y algunas configuraciones pueden necesitar 1 GB o más.

Calamar

Squid es un servidor HTTP proxy de memoria caché disponible como un paquete pfSense, y el rendimiento de disco E / S es una
consideración importante para los usuarios de calamar, ya que determina el rendimiento de caché. En contraste, para la mayoría
usuarios de pfSense es en gran medida irrelevante, ya que el único impacto significativo que la velocidad del disco tiene en pfSense
es tiempo de arranque y actualizar el tiempo, no tiene relevancia a rendimiento de la red o de otra operación normal.

En entornos pequeños, incluso para Squid, cualquier disco duro es suficiente. Para implementaciones 200 + usuario utilizando
Calamar, usted debe considerar 10K RPM SATA o SCSI. Utilice 15K SCSI RPM o discos SAS para
mejores prestaciones en entornos de gran tamaño.

pfSense soporta la mayoría de los controladores RAID de hardware se encuentran en el hardware del servidor. El uso de RAID
10 en sus arrays RAID puede mejorar aún más el rendimiento del calamar, y se recomendaría para la
implementaciones con miles de usuarios.

Capítulo 4. Instalación y actualización

El hardware ha sido elegido, junto con la versión pfSense y la plataforma para ser utilizado. Ahora bien, es tiempo para descargar el comunicado de pfSense apropiado e instalarlo en el dispositivo de destino. Después de descargar la versión correcta, continúe a la sección que describe la instalación de la plataforma que se ha elegido: Instalación completa o incrustado. Si algo sale mal durante el proceso, consulte la sección llamada "Solución de problemas de instalación", más adelante en el capítulo.

En este capítulo, también hablamos de los métodos de instalación de recuperación y cómo actualizar pfSense. Recuperación instalaciones (la sección llamada "Instalación de Recuperación") son las formas para volver a instalar pfSense con una existente configuración, por lo general con tiempo de inactividad mínimo. Actualización de pfSense (la sección llamada "Actualización una instalación existente ") mantendrá su actual sistema, añadir nuevas funciones, o corregir errores. La actualización es un proceso bastante sencillo que se puede lograr de varias maneras diferentes.

Descarga de pfSense

Busque www.pfsense.org [http://www.pfsense.org] y haga clic en el Descargas enlace. Por Página de descargas, haga clic en el enlace para las nuevas instalaciones. Esto le llevará a la página de selección de espejo. Recoger un espejo geográficamente cerca de tu ubicación para un mejor rendimiento. Una vez que un espejo se ha seleccionado, un listado de directorio aparecerá con los archivos de la versión pfSense actuales para las nuevas instalaciones.

Para CD en vivo o instalaciones completas, se puede descargar el `. Iso` la imagen memstick archivo o que es el mismo que el Live CD, pero con formato para grabar en un medio USB. El 2,1 Nombre del archivo de la liberación es `pfSense-2.1-RELEASE-arch.iso.gz` o `pfSense memstick-2.1-RELEASE-arch.img.gz.` Si va a descargar la versión de 32 bits, arco será i386; Para el 64 bit versión, arco será amd64. También hay un archivo MD5 disponible por el mismo nombre, pero que termina en `. Md5.` Este archivo contiene un valor hash del archivo ISO o IMG, que puede ser usado para asegurar la descarga completado correctamente. También hay imágenes memstick de serie, que funcionan como el memstick regular, pero la salida a la consola serie en su lugar. Estas imágenes son útiles para las unidades incrustadas con unidades de disco duro o SSDs que carecen de una salida VGA, pero pueden arrancar desde USB.

Para instalaciones embebidas, descargue el tamaño adecuado NanoBSD `. Img.gz` presentar. El 2,1 Nombre del archivo de la liberación es `pfSense-2.1-RELEASE-size-arch-nanobsd.img.gz,` donde tamaño es uno de los 512M, 1G, 2G o 4G, para reflejar el tamaño de la tarjeta CF para que esa imagen se pretendía (tamaños están en M para megabytes y G para gigabytes), y arco será un i386 o amd64, dependiendo de si desea que la versión de 32 bits o 64 bits. Típicamente usted quiere para que coincida con el tamaño de la imagen para el tamaño de la tarjeta CF, pero puede utilizar una imagen de tamaño más pequeño en una tarjeta CF de mayor tamaño, como una imagen de 1G en una tarjeta CF 2G. Este archivo es una imagen comprimida con gzip. No es necesario extraer el archivo, ya que el proceso de instalación se describe más adelante en este capítulo se encargará de eso. También hay una variación de la Archivo de imagen de NanoBSD para cada tamaño que está configurado para utilizar una consola VGA en lugar de en serie, los que llevan el nombre `pfSense-2.1-RELEASE-size-arch-nanobsd-vga.img.gz` siguiendo las mismas reglas que anteriormente para tamaño y arch.

Si en cualquier punto de la instalación algo no sale como se describe, consulte la sección llamada "Solución de problemas de instalación".

Verificación de la integridad de la descarga

Los archivos MD5 y SHA256 acompañan se pueden utilizar para verificar la descarga completado con éxito, y que se está utilizando una versión oficial.

Verificación de hash en Windows

Los usuarios de Windows pueden instalar HashTab [http://implbits.com/Products/HashTab.aspx] o similar programa para ver MD5 o SHA256 hash de cualquier archivo dado. Con HashTab instalado, haga clic en el archivo descargado y habrá un archivo hashes pestaña que contiene el hash MD5, entre otros. La generada hash MD5 se puede comparar con el contenido de la `. Md5` archivo descargado desde el pfSense

sitio web, que se puede ver en cualquier editor de texto simple como el Bloc de notas. Si usted no ve un hash SHA256, haga clic derecho en la vista de hash y haga clic en Configuración, y luego marque la casilla para SHA256 y haga clic en Aceptar.

Verificación de hash en BSD y Linux

La md5 comando viene de serie en FreeBSD, y muchos otros UNIX y operativo tipo UNIX sistemas. Un hash MD5 puede generarse ejecutando el siguiente comando desde el directorio contiene el archivo descargado:

```
#md5 pfSense-1.2.3-LiveCD-Installer.iso
```

Comparar el valor hash resultante con el contenido del `.Md5` archivo descargado desde el sitio web de pfSense. Sistemas GNU o Linux proporcionan una md5sum comando que funciona de manera similar. Para verificar el uso de SHA256,
los comandos funcionan de manera similar, sólo necesita reemplazar las referencias a md5 con sha256 en el comando y los nombres de archivo.

Verificación de hash en OS X

OS X también incluye la md5 comando como FreeBSD, pero también hay aplicaciones GUI disponible como MD5 de Eternal Tormentas [http://www.eternalstorms.at/md5/]. HashTab [http://implbits.com/ Productos / HashTab.aspx] también está disponible para OSX.

Instalación completa

En esta sección se describe el proceso de instalación de pfSense en un disco duro. En pocas palabras, se trata de arrancar desde el Live CD, realizar una configuración básica, y luego invocar el instalador desde el CD. Si encuentra problemas al intentar arrancar o instalar desde el CD, consulte la sección llamada "Solución de problemas de instalación", más adelante en el capítulo. Si desea usar la imagen en lugar de memstick el Live CD, las instrucciones para escribir la imagen es lo mismo que escribir la imagen incrustada cubierta de la sección "Instalación de Embedded". Después de escribir la imagen memstick, vaya a la sección llamado "Arrancar el CD".

Nota

Si el hardware de destino no tiene una unidad de CD-ROM y no puede arrancar desde USB, una diferente la máquina se puede utilizar para instalar en el disco duro de destino. Vea Técnicas de instalación alternativos (La sección llamada "Técnicas de instalación alternativos") para obtener más información.

Preparación de la CD

Necesitará un CD para ser quemado de la imagen ISO descargada en la sección anterior. Desde el archivo descargado es una imagen de CD, tendrá que ser quemado apropiadamente para archivos de imagen - no como los datos
CD que contiene el único archivo ISO. Procedimientos para hacerlo variarán por el OS y el software disponible.

Antes de que la imagen puede ser quemado, debe ser descomprimido. La `.Gz` extensión del archivo indica que se comprime con gzip. Esto puede ser descomprimido en Windows con 7-Zip [http://www.7-zip.org /], o en BSD / Linux / Mac con el gunzip o gzip-d los comandos.

Quemar en Windows

Virtualmente cada paquete de software de grabación de CD importante para Windows incluye la capacidad de grabar ISO imágenes. Consulte la documentación del programa de grabación de CD que se utilice. Una búsqueda en Google con la nombre del software de grabación y "quemadura iso " debería ayudar a localizar las instrucciones.

La quema 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 ser necesario seleccionar Chose programa predeterminado

y luego recoger Nero de la lista. Este mismo proceso se debe trabajar con otra grabación de CD comercial de software.

Ardiendo de 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 ISO Grabadora para el sistema operativo que se utiliza, a continuación, busque la carpeta en la unidad que contiene el pfSense ISO, haga clic derecho sobre él y haga clic en Copiar imagen a CD.

Otro Free Burning Software

Otras opciones gratuitas para los usuarios de Windows incluyen CDBurnerXP [http://www.cdburnerxp.se/], InfraRecorder [http://infrarecorder.org/] y ImgBurn [http://www.imgburn.com/], entre otros.
Antes de descargar e instalar cualquier programa, compruebe su lista de características para asegurarse de que es capaz de quemar una imagen ISO.

Quemar en Linux

Distribuciones de Linux como Ubuntu suelen incluir algún tipo de interfaz gráfica de usuario CD de la aplicación de grabación que
puede manejar imágenes ISO. Si uno se integra con el gestor de ventanas, haga clic derecho sobre el archivo ISO y elegir discos Escribir al. Otras opciones populares incluyen K3B y Brasero Disc Burner.

Si no hay un programa de grabación GUI instalado, todavía puede ser posible grabar desde el comando line. En primer lugar, determinar SCSI ID / LUN del dispositivo de grabación (número de unidad lógica), con el siguiente comando:

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

Tenga en cuenta el ID SCSI / LUN es 0,0,0. Grabar la imagen como en el siguiente ejemplo, la sustitución <Max Velocidad> con la velocidad del quemador y lun con el SCSI ID / LUN de la grabadora:

```
#cdrecord - dev = lun - velocidad = <max Velocidad> \
  pfSense-2.0-RELEASE-i386-LiveCD-Installer.iso
```

Ardor en FreeBSD

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

```
#datos burncd-s max-e pfSense-2.0-RELEASE-i386-LiveCD-Installer.iso Fixate
```

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

Verificación de la CD

Ahora que se prepara el CD, compruebe que se quemó correctamente mirando los archivos contenidos en el CD. Más de 20 carpetas deben ser visibles, incluyendo bin, boot, cf, conf, y más. Si sólo hay un gran ISO archivo se ve, el CD no se quemó correctamente. Repita los pasos indicados anteriormente para grabar un CD, y estar Asegúrese de grabar el archivo ISO como una imagen de CD y no como un archivo de datos.

Arrancando desde el CD

Ahora el poder del sistema de destino y coloque el CD en la unidad. pfSense debe empezar a arrancar, y mostrará una interfaz asignaciones rápidos, que se trata en una sección posterior.

Nota

Si está utilizando una unidad óptica USB opción se debe pulsar 3en el menú de inicio, Boot pfSense usando el dispositivo USB. Esto introduce un retardo en el proceso de arranque 10, que permite la detección completa de dispositivos USB antes de que continúe arranque. Sin esta opción, muchos Inicio de Sistemas fallará en un `mountroot>` pedirá. Esto se hace automáticamente cuando arrancar la imagen memstick USB. Para otros problemas de arranque, consulte la sección "Instalación Solución de problemas ", más adelante en el capítulo.

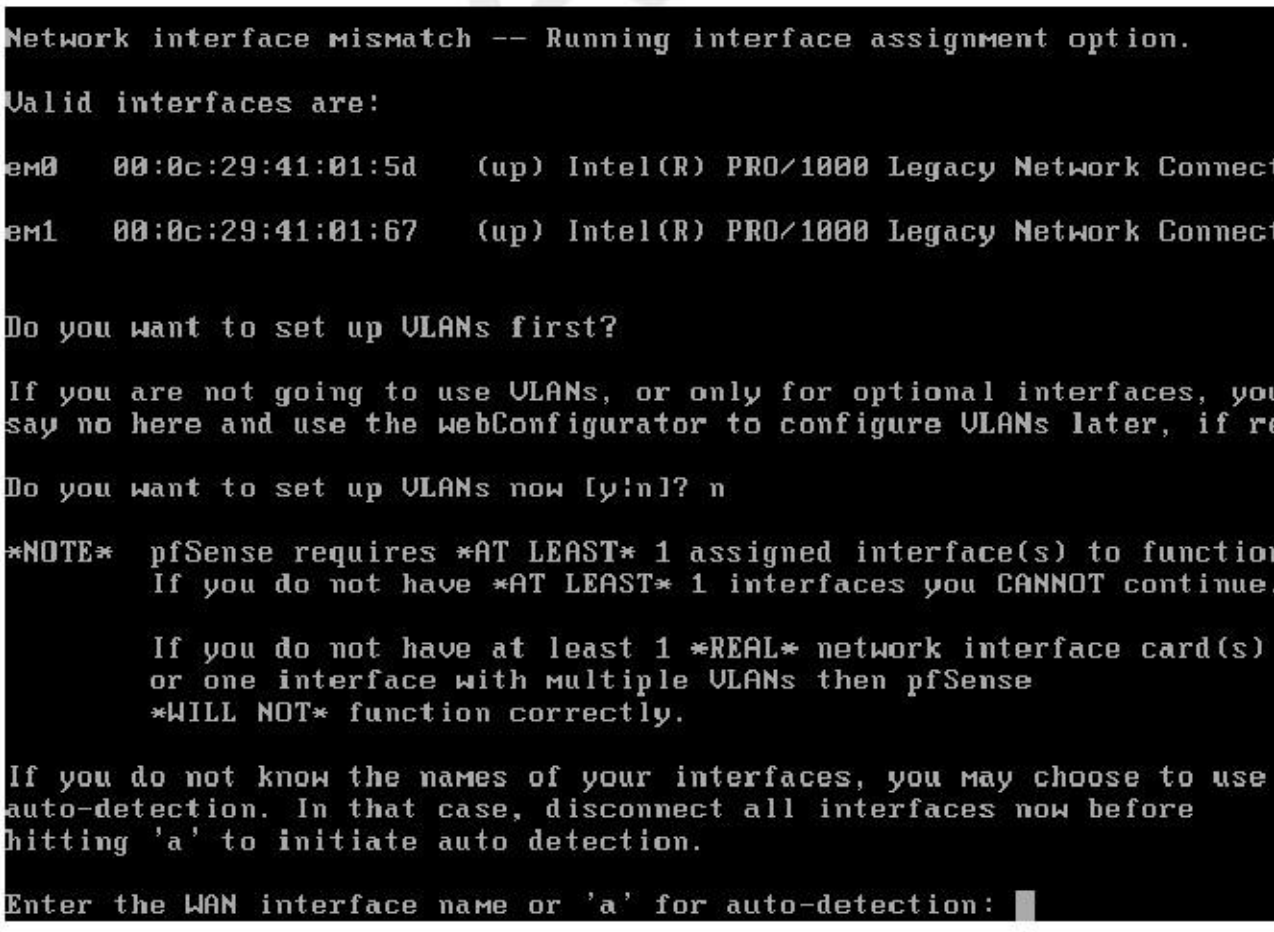
Especificar orden de arranque en la BIOS

Si el sistema de destino no arranque desde el CD o la memory stick USB, la razón más probable es que el dispositivo dado no era lo suficientemente temprano en la lista de medios de arranque en la BIOS. Muchas placas base más nuevas
También permitirá a la educación de un menú de inicio para una sola vez pulsando una tecla durante el POST, comúnmente Esc o F12.
De no ser así, cambie el orden de arranque en la BIOS. En primer lugar, encienda el sistema y entre en la configuración BIOS.
Por lo general se encuentra bajo un Boot o Boot Priority partida, pero podría estar en cualquier lugar. Si el arranque desde CD-ROM o USB no está activado, o tiene una prioridad menor que el arranque desde el disco duro y la unidad contiene otro sistema operativo, el sistema no podrá arrancar desde el medio de pfSense. Consulte la placa base manual para obtener información más detallada sobre la alteración de la secuencia de arranque.

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 la Figura 4.1, "Asignación de interfaz de la pantalla". Aquí es donde instalan las tarjetas de red en el sistema reciben sus papeles como WAN, LAN, y las interfaces opcionales (OPT1, OPT2 ... OPTN).

Figura 4.1. Pantalla de asignación de interfaz



Aparecerá una lista de las interfaces de red y sus direcciones MAC que se encontraban en el sistema, junto con una indicación de su estado de enlace si es apoyada por la tarjeta de red. El estado del enlace es denotado por "(arriba)" que aparece después de la dirección MAC si se detecta un enlace en la interfaz. El MAC (Media Access Control) de la dirección de una tarjeta de red es un identificador único asignado a cada tarjeta, y hay dos tarjetas de red deben tener la misma dirección MAC. (En la práctica, esto no es del todo cierto, la dirección MAC la duplicación ocurre bastante a menudo.) Después de eso, el símbolo se mostrará para la configuración VLAN. Si Las VLAN se desean, consulte el Capítulo 14, LAN virtuales (VLAN) más tarde en el libro de los detalles de su configuración
y el uso. De lo contrario, el tipo de ny pulse enter.

La interfaz WAN está configurado primero. Como que a menudo tienen más de una tarjeta de red, un dilema puede presentarse: ¿Cómo decir cuál es cuál? Si la identidad de cada tarjeta ya se conoce, simplemente introducir los nombres de los dispositivos adecuados para cada interfaz. Si no se conoce la diferencia entre las tarjetas de red,
la forma más fácil de averiguarlo sería utilizar la función de detección automática.

Para la asignación automática de interfaz, primero desenchufe todos los cables de la red del sistema, a continuación, escriba uny
pulse enter. Ahora conectar un cable de red en la interfaz que debe conectarse a la WAN, y pulse entrar. Si todo ha ido bien, pfSense debe saber ahora qué interfaz usar para la WAN. Lo mismo proceso se puede repetir para la LAN, y las interfaces opcionales que serán necesarios. Si un mensaje se muestra como No vinculación detectada, consulte el la sección "Solución de problemas de instalación" para más información sobre la clasificación de las identidades de la tarjeta de red.

Después de las interfaces que desee se hayan configurado, pulse Enter cuando se le preguntó a otra interfaz y aparecerá un mensaje pidiendo `¿Quieres continuar?`. Si la asignación de interfaz de red parece correcta, el tipo Y, luego presione Intro. Si la misión ya no es el adecuado, el tipo ny pulse Enter para repetir este proceso.

Nota

pfSense 2.0 y más tarde, sólo la asignación de una única interfaz. Esto se conoce como modo Appliance. En este modo, el sistema se moverá la regla anti-bloqueo de interfaz gráfica de usuario para la interfaz WAN para que
puede acceder al servidor de seguridad a partir de ahí. Las funciones de enrutamiento usuales no sería activo desde
no hay una interfaz de "interno". Este tipo de configuración es útil para aplicaciones VPN, DNS servidores, y así sucesivamente.

Instalación de la unidad de disco duro

Una vez que la asignación de interfaz se haya completado, aparecerá un menú con las tareas adicionales que puedan ser realizado. Para instalar pfSense en el disco duro de este sistema, la opción de elegir 99 que pondrá en marcha el proceso de instalación.

La primera pantalla que aparece le pedirá para ajustar la configuración de la consola. A menos que un teclado de idioma alternativo es
que se utiliza, elegir aceptar esta configuración y pasar a la siguiente etapa.

A continuación, se presenta una lista de tareas. Si sólo hay un disco duro instalado en el sistema y le no es necesario establecer ninguna otra opción de encargo, Quick / Easy Install puede ser elegido. Esto instalará a el primer disco duro que encuentra y aceptar todas las opciones por defecto. Se mostrará un cuadro de diálogo de confirmación.
Presiona OK para continuar o Cancelar para regresar al menú anterior. La instalación continuará y sólo parar para solicitar que se debe instalar el kernel.

Si decide utilizar la opción Instalar Quick / Easy, vaya a la Tabla 4.1, "Opciones del Kernel" para el núcleo opciones. De lo contrario, elija la primera opción: Instalar pfSense para realizar una instalación personalizada y continuar en el resto de esta sección.

Ahora coge el disco duro a la que se instalará pfSense. Cada disco duro conectado al sistema debe ser demostrado, junto con cualquier RAID admitido o volúmenes gmirror. Seleccione la unidad con el arriba y flechas hacia abajo, luego presione Intro. Si no se encuentra ninguna unidad o las unidades incorrectas se muestran, es posible
que la unidad deseada está conectado a un controlador compatible o un conjunto controlador para un sin apoyo el modo en el BIOS. Consulte la sección "Solución de problemas de instalación" para obtener ayuda.

El siguiente paso es formatear la unidad que acaba de ser elegido. A menos que se sabe con certeza que la unidad contiene una partición de FreeBSD utilizable, seleccione Formato Este disco y pulse Enter. De lo contrario, seleccione Omitir
este paso. Cuando se presenta la pantalla de disco Geometría, lo mejor es elegir Utilice esta geometría. Es posible sobrescribirlo si se conocen los valores más adecuados, pero en la mayoría de los casos, los valores predeterminados son correctos.
Se mostrará una pantalla de confirmación, en cuyo punto se debe elegir la opción de <nombre unidad> Formato para continuar.

Nota

Este es un buen lugar para parar y asegurarse de que la unidad se ha elegido correctamente, ya que no es vuelta atrás una vez que se ha efectuado la grabación. Todo en el disco será destruida.

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

Particiones que sigue, y debería simplemente aceptar los valores predeterminados seleccionando Aceptar y crear, a continuación,
eligiendo Sí, la partición en la siguiente pantalla.
Un mensaje se muestra a continuación para instalar los bloques de arranque. Esto es lo que va a permitir que la unidad de disco duro para arrancar. Instalar
Bloques de arranque ya estará seleccionado (aparece una X en esa columna al lado de la unidad que se está configurado). Puede o puede no ser necesario en modo de paquetes, dependiendo de la combinación de hardware en uso. Algunos más nueva
unidades de hardware y más grandes funcionan mejor con el modo de paquetes habilitada y hardware antiguo puede que prefieran
modo paquete deshabilitado. Deje los valores predeterminados seleccionados a menos que no funcionan en su sistema por algún
razón. Acepte la opción, seleccione Aceptar e instalar bloques de arranque y pulse Intro. Aparecerá un cuadro de confirmación
como se sugiere, es posible que haya una sola opción. Si aparecen varias opciones, escoger el que fue creado para pfSense. Otra ventana de confirmación aparecerá informando del éxito del formato
proceso.

Subparticiones pueden ahora ser creados, pero de nuevo los valores por defecto de esta pantalla serán aceptables para casi todos los usos. Algunas personas prefieren tener subparticiones separadas para `/ Var, / tmp,` y así sucesivamente, pero esto es
no es necesario, y no debería hacerlo a menos que usted tenga una comprensión considerable del espacio requisitos específicos para su instalación. Si va a realizar una instalación completa de los medios de comunicación basados en flash como
una tarjeta CF o USB pulgar unidad, asegúrese de retirar la `intercambio` partición. Realice los cambios deseados, y a continuación, seleccione Aceptar y Crear.
Ahora siéntese y espere, espere, y tienen unos pocos sorbos de café mientras los proceso de instalación copia pfSense para la
Ubicación de destino. Después de que el proceso de instalación ha finalizado su trabajo, no es un indicador definitivo para seleccionar
qué kernel para instalar en el sistema de destino. Hay dos opciones disponibles, cada uno con su propio objetivo:

Cuadro 4.1. Opciones del Kernel

Tipo Kernel	Objetivo / Descripción
Multiprocesamiento simétrico Kernel	Se utiliza para los sistemas que tienen múltiples núcleos o procesadores.
Kernel Embedded	Desactiva la consola VGA y el teclado, usa serial consola.

El multiprocesamiento simétrico Kernel (SMP) funcionará independientemente del número de procesadores disponibles, y es el que recomendamos actual. Anteriormente se había producido un núcleo monoprocesador elección, pero gracias a los avances en FreeBSD, ya no es un beneficio para excluir de la ayuda a partir de leche desnatada en polvo
el kernel por defecto. También solía ser un desarrollador del kernel, sino que es también ya no es necesario en casi todos los casos, por lo que se ha eliminado.

Nota

Una de las razones ya no se necesita un núcleo de depuración se debe a que ahora podemos automáticamente recopilar información sobre los accidentes que usen un núcleo regular. El núcleo de depuración estaba ocupando

más espacio, y poco beneficio ofrecido. En las instalaciones nuevas, con el espacio de intercambio configurados, en caso de un
Kernel Panic o accidente parecido sucedería, el firewall ahora recopilar automáticamente información sobre el accidente y luego reiniciar el sistema. Una vez que el sistema se ha recuperado, se encuentra el símbolo en el tablero de instrumentos para ver y enviar el informe de errores a nuestros servidores o eliminar el accidente
datos sin enviarla. Al comunicarse con el apoyo o el uso de la lista de foro / correo, el información que contiene este informe de errores puede ser útil en el diagnóstico del problema.

Cuando se complete la instalación, seleccione Reiniciar, y luego una vez que el sistema se haya reiniciado, retire el CD antes de que comience el proceso de arranque.

Felicitaciones, pfSense es ahora completamente instaladas!

Instalación de Embedded

La versión incorporada se libera como una imagen de disco, que debe ser escrito a una Compact Flash (CF), utilizando physdiskwrite o dd. Después de la imagen se escribe, se coloca entonces en el dispositivo de destino y configurado.

Nota

Ser muy cuidadoso al hacer esto! Si se ejecuta este en una máquina que contiene otros discos duros es posible seleccionar la unidad incorrecta y sobrescribir una parte de esa unidad con pfSense. Esto hace que el disco completamente ilegible excepto para ciertos programas de recuperación de disco y que es inconsistente en el mejor. physdiskwrite para Windows contiene un control de seguridad que se No permitir sobrescribir una unidad más grande de 800 MB sin una opción específica en el comando line. La manera más segura de instalar pfSense a un CF es a través de la redirección de USB con VMware, más adelante en este capítulo en la sección Técnicas de instalación alternativo (la sección denominado "Técnicas de instalación alternativos").

Una vez más, tener mucho cuidado al hacer esto! Hago hincapié en esto porque sé de varias personas que han escrito mal un disco y sobrescrito un disco duro. Esto puede ocurrir a cualquiera, incluyendo el otro fundador de pfSense, que sobrescribió accidentalmente a su unidad de datos de 1 TB en lugar de su CF imagen de pfSense con.

Instalación en Windows Embedded

La physdiskwrite programa por Manuel Kasper, autor de m0n0wall, es el medio preferido de la escritura la imagen pfSense a CF en Windows. Se puede descargar desde el sitio web m0n0wall [http://m0n0.ch/wall/physdiskwrite.php]. Guárdalo en algún lugar del ordenador que esté utilizando, por ejemplo, `C: \ Herramientas` o
otra ubicación conveniente. Si se elige otra ubicación, sustituto `C: \ Herramientas` en el ejemplo con el directorio en el `physdiskwrite.exe` ha sido colocado.

Nota

También hay una interfaz gráfica de usuario disponible para physdiskwrite llamado PhysGUI, pero la única disponible
la versión de este escrito era en alemán. Dicho esto, la interfaz gráfica de usuario es bastante simple de usar 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 está en Inglés. Por ejemplo, la identificación de la dispositivo adecuado es una tarea mucho más sencilla. También está disponible desde el sitio web m0n0wall. Hay
otras herramientas de la GUI impulsado para unidades de imagen como Image Writer para Windows [https://launchpad.net/win32-image-writer]. Si se siente más cómodo usando una interfaz gráfica de usuario, no dude en
seguir otros métodos por imágenes. Tenga en cuenta que algunas otras herramientas pueden esperar lo descargado
imagen para ser descomprimido antes de escribir.

En Windows Vista o Windows 7, physdiskwrite debe ser lanzado desde un símbolo del sistema de ejecución como administrador. Basta con tener derechos de administrador no es suficiente. La forma más sencilla de hacerlo es hacer clic en
el botón Inicio, a continuación, escriba cmd en el cuadro de búsqueda. Haga clic en `cmd.exe` cuando aparezca y elija

Ejecutar como administrador. La physdiskwrite programa puede entonces ser ejecutado desde que el símbolo del sistema sin ningún problema. Si lo ejecuta desde un símbolo del sistema que no ha sido ejecutar como administrador resultará en ningún disco se encuentran.

Para utilizar physdiskwrite, primero iniciar un símbolo del sistema.

A continuación, cambie al directorio que contiene `physdiskwrite.exe` y ejecutarlo seguido por el camino de la el pfSense `.Img.gz` archivo descargado antes. Después de ejecutar el comando, aparecerá un mensaje con una lista de
aparecerán las unidades conectadas al sistema. Se elige la forma más segura de garantizar la unidad correcta haría ser para ejecutar physdiskwrite antes de insertar el CF, grabar la salida, a continuación, pulse Ctrl + C para salir. Insertar la CF y correr physdiskwrite de nuevo, la comparación de la salida para la ejecución anterior. El disco muestra ahora que no se había demostrado es la CF. El número de cilindros ("cilindros" en physdiskwrite de salida)
También pueden ser utilizados para ayudar a indicar la unidad apropiada. El 512 MB CF utilizado en el ejemplo siguiente tiene 63 cilindros, mientras que los discos duros tienen más de 30.000. Asimismo, recuerda que physdiskwrite tiene un mecanismo de seguridad que no sobrescribirá un disco de más de 2 GB sin especificar `-U` después de la physdiskwrite comando.

Después de seleccionar el disco para escribir, physdiskwrite escribirá la imagen. Esto tomará entre dos a diez minutos en una máquina rápida con USB 2.0 y un 2.0 escritor CF USB. Si el sistema o escritor CF sólo es USB 1.1, esperamos que tome varias veces más larga debido a la muy baja velocidad de USB 1.1. Ampliar imágenes, tales como la imagen de 4 GB, puede tardar bastante más en algunos sistemas.

El siguiente es un ejemplo práctico de utilizar physdiskwrite para escribir una imagen de 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-2.1-RELEASE-2g-i386-nanobsd.img.gz

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

Búsqueda de unidades físicas ...

Información para \ \ \ PhysicalDrive0.:
   Ventanas: cil: 36481
                  tpc: 255
                  spt: 63


Información para \ \ \ PhysicalDrive1.:
   Ventanas: cil: 30401
                  tpc: 255
                  spt: 63


Información para \ \ \ PhysicalDrive2.:
   Ventanas: cil: 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.:
   Ventanas: cil: 30515
                  tpc: 255
                  spt: 63


Información para \ \ \ PhysicalDrive7.:
   Ventanas: cil: 0
                  tpc: 0
                  spt: 0


¿Qué disco que desea escribir? (0 .. 7) 2
A punto de sobrescribir el contenido de disco 2 con nuevos datos. Proceda? (Y / n) y
Encontrado archivo de imagen comprimido
122441728/122441728 bytes escritos en total


C: \
Herramientas>
```

Después physdiskwrite ha completado, el CF puede ser removido de la escritora y se coloca en el blanco de hardware.

Nota

El CF escrito contiene los sistemas de ficheros BSD particiones formateadas que no son legibles en Ventanas. Windows reclamar la unidad necesita ser formateado en caso de intentar acceder a él. Hacer No hacerlo, sólo tiene que mover el CF para el hardware de destino. No hay manera para ver el contenido del CF escrita en Windows.

Instalación en Linux Embedded

Montaje rasante en Linux se logra mediante la canalización de la gunzip de salida de la imagen a dd.

#gunzip-c pfSense-2.1-RELEASE-2g-i386-nanobsd.img.gz | dd of = / dev / hdX bs = 16k

donde Xespecifica el nombre del dispositivo IDE de la tarjeta CF o disco IDE (consulte con hdparm-i / dev / hdX) - Algunos adaptadores USB, en particular, pueden aparecer bajo emulación SCSI que `/ Dev / sdX.`

Ignore la advertencia sobre la fuga de basura - es a causa de la firma digital.

Instalación Incrustado en FreeBSD

gzip canalizado a dd escribirá la imagen a CF en FreeBSD. Antes de empezar, tendrá que saber el nombre del dispositivo que corresponde a la tarjeta CF en uso. Si un disco duro o el adaptador CF-a-IDE está siendo utilizado, puede ser un `anuncio` dispositivo tal como `ad0.` Compruebe la salida de dmesg o `/ Var / log / messages.` Si se está utilizando un lector de USB CF, puede ser un `da` dispositivo tal como `da0,` comprobar `/ Var / log / messages` después de conectar el lector de tarjetas, se debe informar de qué dispositivo se agregó.
Para la imagen de la tarjeta, usted debe ser capaz de descomprimir la imagen y copiarlo a la tarjeta en un solo paso:

#gzip-dc pfSense-2.1-RELEASE-2g-i386-nanobsd.img.gz | dd of = / dev / ADX obs = 64k

Ignore la advertencia sobre la fuga de basura - es a causa de la firma digital.

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

#gunzip pfSense-2.1-RELEASE-2g-i386-nanobsd.img.gz
#dd if = pfSense-2.1-RELEASE-2g-i386-nanobsd.img of = / dev / ADX obs = 64k

Instalación Incrustado en Mac OS X

Este proceso ha sido probado en Mac OS X 10.3.9 y versiones posteriores, hasta e incluyendo Snow Leopard/10.6. Se recomienda que desconecte todos los discos excepto por el disco de arranque antes de llevar a cabo esta procedimiento, como un error en la especificación de la unidad que se escriben en podría causar la pérdida de datos.

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

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

• Abre la Utilidad de Discos.

• Seleccione las particiones de su tarjeta CF que se montan, y haga clic en el botón Desmontar. Las particiones Ahora debería aparecer 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 'Disco identificador': por ejemplo, "Disk1".

• Abrir terminal.

• Cambie al directorio que contiene la imagen de pfSense.

• Utilice este comando, reemplazando disco [n] con el identificador de disco encontrado anteriormente:

#gzcat pfSense-2.1-RELEASE-2g-i386-nanobsd.img.gz | dd of = / dev / disk [n] bs = 16k

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

```
$lista diskutil
/ Dev/disk0
   #: TIPO                                  NOMBRE                  TAMAÑO       IDENTIFICADOR
   0: GUID_partition_scheme                                        * 298.1 Gi    disk0
   1: EFI                                                           200.0 Mi     disk0s1
   2: Apple_HFS                                                     297.8 Gi     disk0s2
/ Dev/disk1                                 Macintosh HD
   #: TIPO
   0: CD_partition_scheme                   NAMESIZEIDENTIFIER
   1: CD_DA                                 30 días para Great French * 521.4 Midisk1
   2: CD_DA                                                        7.8 Midisk1s1
   3: CD_DA                                                        7.8 Midisk1s2
   4: CD_DA                                                       18.2 Midisk1s3
   5: CD_DA                                                       13.8 Midisk1s4
   6: CD_DA                                                       14.0 Midisk1s5
   7: CD_DA                                                       12.1 Midisk1s6
   8: CD_DA                                                       14.2 Midisk1s7
   9: CD_DA                                                       21.5 Midisk1s8
  10: CD_DA                                                       16.6 Midisk1s9
  11: CD_DA                                                       14.7 Midisk1s10
  12: CD_DA                                                       24.3 Midisk1s11
  13: CD_DA                                                       16.6 Midisk1s12
  14: CD_DA                                                       22.4 Midisk1s13
  15: CD_DA                                                       14.7 Midisk1s14
  16: CD_DA                                                       20.5 Midisk1s15
  17: CD_DA                                                       19.4 Midisk1s16
  18: CD_DA                                                       15.3 Midisk1s17
  19: CD_DA                                                       17.9 Midisk1s18
  20: CD_DA                                                       18.2 Midisk1s19
  21: CD_DA                                                       16.0 Midisk1s20
                                                                  26.8 Midisk1s21
```

```
 22: CD_DA18.8 Midisk1s22
 23: CD_DA21.7 Midisk1s23
 24: CD_DA14.5 Midisk1s24
 25: CD_DA22.2 Midisk1s25
 26: CD_DA16.7 Midisk1s26
 27: CD_DA20.9 Midisk1s27
 28: CD_DA16.0 Midisk1s28
 29: CD_DA20.8 Midisk1s29
 30: CD_DA17.1 Midisk1s30
/ Dev/disk2
  #: TIPO NAMESIZEIDENTIFIER
  0: GUID_partition_scheme * 90,0 Midisk2
  1: Apple_HFS Processing90.0 Midisk2s1
/ Dev/disk3
  #: TIPO NAMESIZEIDENTIFIER
  0: FDisk_partition_scheme * 978.5 Midisk3
  1: DOS_FAT_32 UNTITLED978.4 Midisk3s1
$diskutil umount disk3s1
$gzcat pfSense-2.1-RELEASE-2g-i386-nanobsd.img.gz | dd of = / dev/disk3 bs = 16k
7665 1 registros en
7665 1 registros fuera
125587456 bytes transferidos en 188.525272 secs (666157 bytes / seg)
```

Finalización de la instalación Embedded

Ahora que el CF contiene una imagen de pfSense, que se puede colocar en el dispositivo de destino, pero es posible que aún
necesita algo de configuración. Los usuarios de ALIX y Soekris 5501 hardware pueden saltarse esta sección, ya que utilizan
vr (4)-basado controladores de red y la instalación por defecto integrado supone que vr0 es LAN y
VR1 es la WAN. Estos puertos deben estar etiquetados en el hardware. Si desea volver a asignar estas interfaces
desde la consola en lugar de la WebGUI, seguir adelante.

Conecte un cable serie

En primer lugar, un cable serie de módem nulo [http://en.wikipedia.org/wiki/Null_modem] debe conectarse
entre el dispositivo y un PC. Dependiendo del puerto serie y el cable que se utiliza, un cable serie de género
cambiador [http://en.wikipedia.org/wiki/Gender_changer] también puede ser necesario para que coincida con la disposición
puertos. Si un cable serie de módem nulo real no está disponible, también hay adaptadores de módem nulo que se
convertir un cable serie estándar en un cable de módem nulo.

Iniciar un Serial Client

En el PC se utiliza para configurar el dispositivo integrado, un programa cliente de serie debe ser utilizado. Algunos
clientes más populares para Windows son Hyperterminal, que debe estar en casi cualquier instalación de XP, y
PuTTY [http://www.chiark.greenend.org.uk/ ~ sgtatham / putty /], que es gratuito y mucho más fiable.
En Linux, `minicom` debe estar presente en la mayoría de los sistemas de paquetes de distribución. En FreeBSD, simplemente
utilizar el programa integrado `punta`. Mecanografía com1 punta (O inclinar ucom1 si está utilizando una serie USB
adaptador) se conectará al primer puerto serie. Desconecte escribiendo "~". en el comienzo de una línea.

Cualquiera que sea el cliente se utiliza en serie, asegúrese de que está configurado para la velocidad adecuada (9600), Bits de datos (8), de paridad
(No), y los bits de parada (1). Normalmente, esto se escribe como 9600/8/N/1. Algunas unidades incorporado por defecto a un
velocidad más rápida. Motores PC WRAP y ALIX defecto para 38400/8/N/1 y hardware Soekris impagos
a 19200/8/N/1. Muchos clientes de serie por defecto a 9600/8/N/1, por lo que estos ajustes pueden no ser
necesario. Usted tendrá que utilizar 9600/8/N/1 con pfSense independientemente de la configuración de su hardware.
Para el hardware utilizando velocidades diferentes a 9600, es probable que desee para cambiar la velocidad de transmisión de 9600 en el
Configuración de la BIOS para que el BIOS y pfSense son accesibles con los mismos ajustes. Consulte el manual de
para su hardware para obtener información sobre la configuración de su velocidad de transmisión. 9600 es sólo la velocidad por defecto de la caja,
posteriormente puede aumentar la velocidad de serie utilizado por pfSense, consulte la sección llamada "serie Velocidad de consola".

Asigne las interfaces de red

Después de que el dispositivo está encendido y el proceso de arranque se ha iniciado, el símbolo se mostrará para las VLAN
y la asignación de las interfaces de red. Este paso fue cubierto anteriormente bajo la sección denominada "Asignación Interfaces "para la detección automática, y más adelante en la sección titulada" Interfaces de asignación manual " para asignar manualmente las interfaces.

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

Técnicas de instalación alternativos

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

Instalación con unidad en un equipo diferente

Si es difícil o imposible para agregar una unidad de CD-ROM para el hardware de destino, y el sistema no puede arranque desde USB, otro sistema se puede utilizar para instalar pfSense en el disco duro de destino. La unidad puede entonces ser movido a la máquina original.

Cuando aparezca `Asigne Interfaces` durante el arranque del CD Vivo, escoja npara VLANs y
tipo salida en el símbolo del interface LAN asignación para saltar asignación interfaz. A continuación, proceder a través de
la instalación normalmente. Aparecerá un mensaje en el instalador para configurar los ajustes de red y esto puede ser omitido también. Después de la instalación, deje que la máquina se reinicie y apagarlo una vez que vuelve a la pantalla de la BIOS. Retire el disco duro de la máquina de la instalación y colóquelo en el sistema de destino. Después del arranque, se le pedirá para la asignación de la interfaz y luego el resto de la configuración puede llevarse a cabo como de costumbre.

Los errores de inicio después de la unidad en movimiento para apuntar máquina

Si el equipo utiliza para realizar la instalación de la unidad asignada con un nombre de dispositivo diferente del dispositivo de destino, el sistema se detendrá el arranque en una `mountroot>` pedirá. Esto puede suceder si la instalación
se lleva a cabo con la unidad en el puerto IDE secundario y en el hardware de destino reside en el puerto IDE primario. En el caso de VMware, el adaptador USB puede ser detectado como un dispositivo SCSI mientras el hardware de destino utiliza IDE.

Si se produce este problema, el sistema dejará de arrancar y sentarte en una `mountroot>` pronta, como en este ejemplo:

```
TimeCounter frecuencia "TSC" calidad 431646144 Hz 800
Timecounters marque cada 10.000 ms
Fast IPsec: Inicializado Procesamiento de Seguridad de la Asociación.
ad0: 3906MB <HMS360404D5CF00 DN4OCA2A> en UDMA33 ata0-master
Tratar de montar raíz de ufs :/ dev/ad2s1a


Manual de especificación del sistema de archivos raíz:
  <fstype>: <device> Monte <device> utilizando el sistema de archivos
<fstype>
                       por ejemplo. ufs: da0s1a
  ? Lista de dispositivos de arranque del disco válidos
  vacía> line> Abortar entrada manual

mountroot> ufs: ad0s1a
Tratar de montar raíz de ufs: ad0s1a


    ___
 ___ / F \
/ P \ ___ / Sense
\ ___ / \
```

```
      \ ___ /
```

El sistema está tratando de montar la unidad con el nombre de dispositivo equivocado, como `ad2`. Una línea justo por encima
la `mountroot` prompt debe enumerar la ubicación real de la ofensiva, como `ad0`. Para proseguir con el arranque proceso, escriba el nombre de dispositivo correcto. En este caso, ufs: ad0s1a. Basta con sustituir ad0 en esa línea con el nombre de dispositivo de la unidad de disco duro como se muestra por encima de este indicador. Tome nota de que el dispositivo adecuado
nombrar, ya que será necesaria para el siguiente paso.
Ahora que el sistema ha arrancado, se necesita un cambio más. La tabla de sistema de archivos en `/ Etc / fstab` necesita ser actualizado con el dispositivo adecuado. Para cambiar esto en el WebGUI, vaya a Diagnósticos

 Editar el archivo, y abierto `/ Etc / fstab`. Reemplace cada instancia del nombre del dispositivo en ese archivo y guardarlo
sus cambios. Reinicie para verificar el cambio.

Para aquellos familiarizados con las operaciones de línea de comandos, para cambiar esto en la línea de comandos opción de elegir
8una vez que se cargue el menú de la consola para entrar a iniciar un shell. En este ejemplo se utiliza el vi editor. Si vi no es un
opción deseable, ee También está disponible y tiene la ayuda en pantalla.
Introduzca ahora el comando para editar el `fstab` presentar:

```
#vi / etc / fstab
```

Aparecerán los contenidos del archivo. Se verá algo como esto:

```
# Dispositivo           Punto de montaje FsType   Opciones         VertederoPase #
/ Dev/ad2s1a            /                ufs      rw                1       1
```

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

```
# Dispositivo           Punto de montaje FsType   Opciones         VertederoPase #
/ Dev/ad0s1a            /                ufs      rw               1        1
```

Ahora, guarde el archivo y salga del editor. (Esc, luego : Wq! si vi se utilizó.)

Instalación completa de VMware con redirección USB

Puede utilizar la redirección de USB en VMware Player y la estación de trabajo para instalar un disco duro. Más cualquier USB a IDE o SFF (Small Form Factor) Adaptador IDE funciona para este propósito. La siguiente instrucciones son específicas de VMware Workstation 6.0 y anteriores.

• Crear una máquina virtual con redireccionamiento
USB.
• Desconecte el escritor CF desde su PC.

• Enchufe el CF / Microdrive en su escritor CF.

• Inicie la máquina virtual y haga clic en el interior de la máquina virtual para que tenga el foco.
• Enchufe el escritor CF en el PC. El VM recogerá el dispositivo USB, y el instalador pfSense CD reconocerá el CF / Microdrive como un disco duro.

• Continuar con la instalación de la misma como una completa normalidad en Instalar.

En VMware Workstation 6.5 y posteriores, verá un icono para cada dispositivo USB en la máquina a lo largo de la parte inferior de la ventana de VMware. Haga clic en el dispositivo y haga clic en Conecte (Desconectar de host) utilizarlo dentro de su máquina virtual. Consulte la documentación de VMware para más información sobre USB redirección.

Instalación Incrustado en VMware con USB Redirección

La imagen incrustada también puede escribirse en VMware utilizando su redirección USB. Esta es una opción más segura
ya que hace que sea imposible para sobrescribir los discos en el host, lo que limita el daño potencial a lo que está en su máquina virtual. Para ello, basta con conectar el escritor CF a la máquina virtual y realizar la instalación como lo haría en el mismo sistema operativo en una máquina física. Consulte la documentación de VMware para más información sobre la redirección de USB.

On-the-fly imagen de NanoBSD durante el arranque del LiveCD o memstick

Si puede arrancar el LiveCD o memory stick, pero no se puede mover con facilidad la unidad de destino a otra máquina a la imagen de disco, no hay otra manera. Puede buscar y escribir la imagen de NanoBSD en una sola pasada, pero al hacerlo no se recomienda generalmente como no hay manera de verificar la descarga antes de escribir el imagen. Sin embargo, si las circunstancias le obligan a utilizar este método, puede ser eficaz.

En primer lugar, arrancar el LiveCD o memory stick hasta el final, y configurarlo de manera que tenga conectividad externa.
Normalmente, la configuración por defecto está bien si estás en un entorno DHCP. Una vez que haya confirmado conectividad externa, ir a un intérprete de comandos (8 en el menú de la consola) y escriba el siguiente comando:

```
# Fetch-o - http://files.pfsense.org/mirror/downloads/pfSense-2.1-RELEASE-4g-i3
  gzip-dc | dd of = / dev/ad0 obs = 64k
```

Ese comando fue a buscar la imagen, y en lugar de almacenarlo en cualquier lugar, salidas directamente en el descompresión y proceso de imágenes de disco. Al igual que con las las instrucciones de imágenes anteriores nanobsd sobre
FreeBSD (Consulte la sección "Instalación de Embedded en FreeBSD"), también puede sustituir a la NanoBSD tamaño de la imagen, la arquitectura, y si es necesario, utilizar las imágenes VGA nanobsd, ajustando el comandar apropiadamente.

Nota

Este método sólo funciona si el disco duro es ad0, de lo contrario algunos cambios manuales en el Se requerirían etiquetas del sistema de archivos.

Solución de problemas de instalación

La gran mayoría de las veces, instalaciones terminará sin problemas. Si los problemas de pop-up, el siguiente secciones se describen los problemas más comunes y las medidas adoptadas para resolverlos.

Arrancar desde Live CD falla

Debido a la amplia gama de combinaciones de hardware en uso, no es raro que un CD para arrancar incorrectamente (O en absoluto). Los problemas y soluciones más comunes son:

Dirty Drive CD-ROM	Limpie la unidad con un disco de limpieza o una lata de aire comprimido, o tratar otra unidad.
Bad CD-R Medios	Grabe otro disco y / o grabar el disco a una velocidad más baja. Tal vez pruebe otra marca de medios de comunicación.
Cuestiones BIOS	Actualizar a la última BIOS y desactive todos los dispositivos periféricos que no sean necesarios tales como Firewire, unidades de disquete y de audio.
IDE Cuestiones Cable	Pruebe con un cable IDE diferente entre la unidad de CD-ROM y el IDE Controlador o placa base

Problemas de arranque de la cargadora	Ha habido casos en los que las versiones específicas de arranque del CD de FreeBSD cargador no funcionará en algunos sistemas. En este caso, consulte la sección anterior acerca de cómo realizar la instalación desde el disco duro en un PC independiente y luego moviéndolo al sistema de destino.

Hay más técnicas de solución de problemas enumerados en el Wiki de documentación pfSense con Boot Solución de problemas [http://doc.pfsense.org/index.php/Boot_Troubleshooting].

Arrancar desde el disco duro después de la instalación del CD no

Después de la instalación del CD se completa y se reinicia el sistema, hay algunas condiciones que pueden prevenir pfSense desde el arranque plenamente. Las razones más comunes son típicamente BIOS o disco duro relacionados controlador. Algunos de estos pueden ser trabajados en torno a la elección de diferentes opciones para el arranque cargador durante el proceso de instalación, la activación / desactivación del modo de paquetes, o mediante la instalación de un tercero gestor de arranque como GRUB1. Actualización de la BIOS a la última versión disponible también puede ayudar en este caso.

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

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

Interface Link Up no se detecta

Si el sistema se queja de que no se detecte enlace de interfaz, primero asegúrese de que el cable está desconectado y que la interfaz no tiene una luz de enlace antes de elegir la opción de detección de enlace. Usted puede también quieren probar o reemplazar el cable en cuestión. Después de seleccionar la opción, conecte el cable de nuevo en la interfaz y asegurarse de que tiene una luz de enlace antes de pulsar Intro.

Si un cable de red está conectado directamente entre dos sistemas y no a un interruptor, asegúrese de que un cable cruzado se utiliza [http://en.wikipedia.org/wiki/Ethernet_crossover_cable]. Algunos más nueva adaptadores pueden apoyar Auto-MDIX [http://en.wikipedia.org/wiki/Auto-MDIX] y se encargará de esta internamente, pero muchos adaptadores más antiguos no lo hacen. Del mismo modo, si la conexión de un sistema de pfSense a un conmutador que no es compatible con Auto-MDIX, utilice un cable de conexión directa.

Si la interfaz está conectado correctamente pero pfSense aún no detecta el enlace de arriba, la red las interfaces que se utilizan pueden no detectar correctamente enlace por alguna razón. En este caso, la asignación manual las interfaces es necesario.

Asignación manual de interfaces

Si la función de detección automática no funciona, todavía hay esperanza de decir la diferencia entre la red tarjetas antes de la instalación. Una forma es mediante la dirección MAC, la cual debe ser comparadas con la interfaz nombres en la pantalla de asignación:

```
le0     08:00:27:26: a4: 04
LE1     08:00:27:32: ec: 2f
```

La dirección MAC a veces se aparece en una pegatina en alguna parte física de la tarjeta de red. MAC direcciones también son asignados por el fabricante, y hay varias bases de datos en línea que le permitirá hacer una búsqueda inversa en una dirección MAC con el fin de encontrar la compañía que hizo el card.2

Las tarjetas de red de diferentes marcas, modelos, oa veces chipsets pueden detectarse con diferente conductores. Puede ser posible contar una tarjeta basada en Intel utilizando el `fxp` conductor, aparte de una tarjeta Realtek

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

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

usando el `rl` conductor mirando las tarjetas ellos mismos y la comparación de los nombres impresos en la circuitos.

Una vez que se determina que la tarjeta de red se utilizará para una determinada función, escríbalo en la interfaz pantalla de asignación cuando se le solicite. En el ejemplo anterior, `le0` será WAN y `LE1` será LAN. Cuando se le solicite por primera vez para la dirección de WAN, se podría escribir le0 y pulse enter. Luego, cuando se le solicite para LAN, tipo LE1, y pulse enter. Dado que no existen interfaces opcionales, una pulsación más entrar, entonces ycompletará la tarea. En casi todos los PC de torre, la ranura PCI más alta será la primera NIC, ordenó secuencialmente en orden de arriba hacia abajo. Cuando usted tiene tres Intel `fxp` tarjetas en un sistema, el top NIC es normalmente `fxp0,` la de abajo que `fxp1,` y el más bajo `fxp2.` Esto depende en la placa base, pero casi siempre es válido. Si usted tiene una NIC a bordo que es de la misma marca como un complemento NIC, tenga en cuenta que algunos sistemas, aparecerá una lista de la NIC a bordo primero, y otros no.

Solución de problemas de hardware

Si se encuentra con problemas con el hardware que está intentando usar, las siguientes sugerencias le ayudar a resolverlos en muchos casos.

Retirar hardware innecesario

Si el sistema contiene todo el hardware que no se va a utilizar, retírelo. Por ejemplo, si usted tiene redistribuido un viejo escritorio 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 extraíble y usted no lo necesita, se lo quita.

Desactivar PNP OS en su BIOS

Esta es la solución más común para los problemas de hardware. Muchas pantallas de configuración del BIOS tendrán un ajuste de PNP OS o Plug and Play del sistema operativo, que debe ajustarse a inhabilitar o No. Algunos tienen un ajuste para el sistema operativo, el cual por lo general se debe establecer en otra.

Actualice su BIOS

La segunda solución más común para los problemas de hardware está actualizando el BIOS a la última revisión. La gente parece tener dificultades para creer esto, pero confía en mí, sólo hazlo. Actualizaciones de BIOS comúnmente corregir errores en el hardware. No es raro para golpear los problemas inducidos por errores de hardware en sistemas que de forma estable han de ejecutar Windows desde hace años. Supongo tanto en Windows no se activa el error, o tiene una evitar, como lo he visto personalmente este en múltiples ocasiones. Cosas que las actualizaciones de BIOS pueden arreglar incluir en su defecto para arrancar, el tiempo de mantenimiento de los problemas y la inestabilidad general, entre otros.

Cambiar la configuración del BIOS a los valores predeterminados de fábrica

Algunos sistemas de reciclados pueden tener una configuración BIOS atípica de su uso anterior. La mayoría contienen una opción que le permite restablecer todos los ajustes a los valores predeterminados de fábrica. Trate de hacer esto. También puedes ver la sección llamada "Disable PNP OS en tu BIOS" de nuevo después de hacer esto.

Desactivar el hardware no utilizado en el BIOS

Si la placa se ha construido ninguna en los componentes que no se va a utilizar, pruebe a desactivar ellos. Común ejemplos incluyen el puerto paralelo, módems de a bordo, dispositivos de audio, Firewire, USB, posiblemente, y la puertos serie a menos que usted planea usar una consola serie.

Otros parámetros de la BIOS

Si su BIOS permite la configuración de administración de energía, trate de apagarlo o encendido. Puedes buscar cualquier otra cosa que parece relevante y tratar de cambiar algunas cosas. Si se llega a este punto, el hardware es probablemente una causa perdida y usted debe buscar hardware alternativo. También revise si su BIOS tiene un registro de eventos que puede enumerar los errores de hardware, tales como fallos en las pruebas de memoria.

Otros Problemas de hardware

También podría haber un problema con el hardware de destino, que las pruebas con el software de diagnóstico puede revelar. Se debe probar el disco duro con el software de diagnóstico del fabricante, y probar el memoria con un programa como memtest86 +. Estos y más herramientas están disponibles en el "Ultimate Boot CD [http://www.ultimatebootcd.com/] ", que está precargado con muchas herramientas de diagnóstico de hardware libre.

Asegúrese también de que todos los fans están girando a gran velocidad, y que el suministro está sobrecalentando. Si este es el hardware más antiguo reutilizado, un poco de limpieza comprimido / lata de aire de los ventiladores y disipadores de calor puede trabajar
maravillas.

Problemas de arranque integrados en ALIX Hardware

Si un sistema embebido no arranca correctamente, conecte un cable serie al dispositivo y supervisar el arranque proceso en busca de pistas sobre la manera de proceder. El problema más común será para los usuarios de hardware ALIX.
Si está utilizando una tarjeta del ALIX, usted tendrá que asegurarse de que el BIOS más reciente disponible en el momento de
este escrito, 0.99h, se carga en el tablero para poder arrancar correctamente las imágenes nanobsd de ambos sectores.
Un ALIX en necesidad de una actualización de la BIOS se exhiben típicamente los siguientes síntomas en el arranque:

```
V0.99 PC Engines ALIX.2
640 KB de memoria Base
261,120 KB de memoria extendida


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


1    FreeBSD
2    FreeBSD


Boot:    1 # # # # # # # # # #
         # #
```

El número de marcas de hash (#) crecerá lentamente en el tiempo como la bota intenta continuar. Si este comportamiento se ve, siga los procedimientos de actualización de la BIOS de su proveedor para al menos la versión 0.99h
Además de necesitar la versión del BIOS 0.99h, el BIOS también debe estar configurado para el modo CHS (cilindro / cabeza /
Sector de modo para el direccionamiento de datos en un disco), como en el siguiente ejemplo:

```
V0.99h Motores PC ALIX.2
640 KB de memoria Base
261,120 KB de memoria extendida


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


Configuración del
BIOS:
* 9 * 9600 (2) 19.200 baudios (3) 38.400 baudios (5) 57.600 baudios (1) 115 200 baudios
* C * Modo CHS (L) el modo LBA (W) HDD esperar esclavo (V) HDD (U) UDMA permiten
(M) MFGPT solución
(P) init PCI tarde
* R * Consola de serie permiten
(E) Arranque PXE permite
(X) Xmodem carga
(Q) Dejar de
```

Para llegar a esta pantalla, pulse Smientras se muestra la prueba de la memoria durante la consola serie. Luego presione Cpara cambiar al modo de CHS, a continuación, pulse Qdejar de fumar.

En este punto el ALIX deberían adecuadamente arranque de cualquiera porción de una imagen de NanoBSD.

Instalación de Recuperación

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 vuelva a instalar rápida con que se necesita una configuración de copia de seguridad. En el
segundo caso, la configuración sigue estando presente en el disco duro, pero algunos de los contenidos del sistema de archivos
puede estar dañado. pfSense ofrece un proceso fácil y relativamente sin dolor para recuperarse rápidamente de este tipo de problemas, y si ninguno de estos escenarios se aplica entonces no es siempre el método tradicional de restaurar una configuración desde dentro de la WebGUI.

Pre-Flight Recuperación de la configuración del instalador

pfSense tiene, como parte de la rutina de instalación, "Instalación Pre-Flight" una o PFI. PFI investigará si existe otra configuración existente en una unidad USB y usarlo en lugar de pedir una nueva configuración. ¿Cuándo la instalación de un disco duro, el programa de instalación copiará esta configuración. Cuando el proceso se completa, se reiniciará con el archivo de configuración restaurada.

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

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 vino de la pfSense WebGUI, es probable nombrado como el siguiente: `config-routerhostname.example.com-20111018142139.xml`. Cambiar el nombre de este archivo a `config.xml`. Para obtener más información sobre cómo realizar copias de seguridad, consulte el Capítulo 9, Reserva
y recuperación.

La unidad ya debe estar lista para su uso. Para comprobar que la configuración está en el lugar correcto, el archivo debe estar en E: \ conf \ config.xml si la unidad USB es E:. Sustituya la letra de unidad correspondiente para el sistema que está siendo utilizado.

Extraiga la unidad USB de la estación de trabajo, y luego conectarlo al sistema de pfSense siendo restaurado. Ponga el CD en vivo en su unidad de CD-ROM e inicie el sistema hasta el final hasta que el indicador del menú, no pulse 'i' durante el proceso de arranque para invocar la instalación inicial. Una vez que haya iniciado por completo, debe ser notable
que el sistema utiliza la configuración desde el USB y no solicita para configurar las interfaces. La único que queda por hacer es seguir los pasos descritos en la sección titulada "Instalación de la unidad de disco duro" para realizar una instalación normal de un disco duro.

Cuando la instalación haya finalizado, apague el sistema, desenchufe la unidad USB y retire el CD de instalación. Encienda el sistema de nuevo, y debería arrancar normalmente y sea plenamente operativa. Si cualquiera
paquetes estaban en uso, visite el WebGUI y después de inicio de sesión que se vuelven a instalar automáticamente.

Nota

Tenga cuidado al extraer una unidad USB desde un sistema de pfSense. Siempre es más seguro para hacerlo cuando la alimentación está apagada. Si la unidad USB se monta un sistema de pfSense correr y eliminado sin desmontar, el sistema voluntad accidente y reiniciar con posiblemente impredecible resultados. FreeBSD es incapaz de perder los sistemas de ficheros montados actualmente sin inducir una pánico. Esto ya no será un problema en FreeBSD 8.0.

Recuperación de la configuración instalada

Si partes de la instalación en el disco duro no están funcionando (como resultado de un error de actualización u otro causar), la configuración puede ser retenido mientras se limpian a cabo el resto de los archivos instalados.

Durante el proceso de instalación, antes de elegir Instalar pfSense hay una opción de menú denominado Rescate config.xml. Cuando se elige esta opción, una configuración puede ser seleccionado de cualquiera de almacenamiento masivo
medios conectados al sistema. El proceso de instalación se carga esta configuración, y una vez que el reinstalación es completa, el sistema se ejecuta con la configuración rescatados.

WebGUI Recuperación

Si todo lo demás falla, procederá a efectuar una instalación normal, como se describe anteriormente en este capítulo a continuación, restablezca
la configuración antigua visitando Diagnóstico Backup / Restore en el WebGUI vez de red
conectividad ha sido restaurada. En la sección Restaurar configuración de la página, haga clic en Examinar, busque el archivo de copia de seguridad de configuración. Una vez localizado, haga clic en Abrir y, a continuación, finalmente, haga clic en Restaurar configuración.
La configuración se restaurará y el sistema se reiniciará automáticamente. Después de reiniciar, el configuración completa debería estar presente. Este proceso se describe con mayor detalle en la sección llamada "Restauración de copias de seguridad".

Actualizar una instalación existente

Los medios compatibles de actualizar de una versión pfSense a otro dependen de la plataforma es utilizado. En la mayoría de los casos, pfSense se puede actualizar de manera fiable a cualquier otra versión al tiempo que conserva la existente
configuración.

Al mantener un sistema pfSense actualizado con una versión actual con el apoyo, que nunca será obsoleto. Nuevo versiones se liberan periódicamente que contener nuevas funciones, actualizaciones, correcciones de errores, y varios otros
cambios. En la mayoría de los casos, la actualización de una instalación pfSense es muy fácil. Si la actualización a una nueva versión que
es un sólo un punto de desenganche (por ejemplo, 2.0.1 a 2.0.2), la actualización debe ser mínimamente invasiva y es improbable que
causará ningún problema. El problema más común es regresiones específicas del hardware de un FreeBSD versión a otra, aunque esto sea muy poco frecuente. Comunicados Actualizado fijan más hardware que se rompen, pero regresiones son siempre posibles. Saltos más grandes, como de 1.2.3 a 2.0 en el futuro deben ser manejados con cuidado, e idealmente probado en hardware idéntico en un entorno de prueba antes de su uso en la producción.
A menudo poste de Notas de actualización junto con los lanzamientos para ayudar a guiar a través de cualquier peligros potenciales que se podría
encontrarse con ocasión de tal esfuerzo. Estas notas varían de una versión a otra, la versión más actual se puede encontrar en el wiki de documentación [http://doc.pfsense.org/index.php/Upgrade_Guide].

Haga una copia de seguridad ... y un plan de copia de seguridad

Lo primero es lo primero, antes de hacer cualquier modificación a un sistema de pfSense, que es una buena idea hacer una
copia de seguridad. En la WebGUI, visite Diagnóstico Backup / Restore. En la sección de configuración de copia de seguridad
de la página, asegúrese de que el Área de copia de seguridad está establecido en TODOS, a continuación, haga clic en Descargar Configuración. Guardar este archivo
en un lugar seguro, y no estaría de más hacer varias copias. Las personas con un pfSense Portal [https://portal.pfsense.org /] suscripción debería considerar el uso del paquete de copia de seguridad automática de configuración y hacer
una copia de seguridad manual señalando la razón que antes de la actualización.
También puede ser una buena idea tener a mano el medio de instalación para la versión que se está ejecutando actualmente, en caso de
algo va mal y se requiere una reinstalación. Si eso ocurre, tiene el archivo de copia de seguridad a mano y se refieren a la anterior la sección "Instalación de Recuperación". También consulte el Capítulo 9, Reserva y recuperación.

Actualización de una Instalación de Embedded

Antes de la versión 1.2.3, el único 100% garantizado forma fiable de actualizar incrustado se re-flash la CF y restaurar una copia de seguridad de configuración anterior después. Ese método todavía puede ser utilizado, pero gracias a la nueva versión integrada con sede en NanoBSD en uso desde 1.2.3 adelante, actualizaciones fiables se puede realizar como una instalación completa. Continuar en la Instalación completa en las instrucciones de actualización si
Ya se están ejecutando pfSense versión 1.2.3 o posterior.

Nota

Si está actualizando desde una versión anterior de pfSense hasta la versión 1.2.3 o posterior, se quiere todavía tendrá que volver a actualizar la tarjeta por una nueva imagen basada en NanoBSD. A partir de entonces se puede actualizar
como de costumbre.

Instalar actualización de un completo o instalar NanoBSD

Hay varios métodos disponibles para actualizar una instalación completa o una instalación de NanoBSD pfSense. O bien el WebGUI o la consola se pueden utilizar, y cualquiera de los métodos tiene un medio de suministrar un archivo de actualización descargado o descontar automáticamente de Internet.

Actualizando usando el WebGUI

Hay dos opciones para la actualización mediante la interfaz web, con la actualización manual y automático. Las secciones siguientes describen estos métodos de actualización.

Manual de actualización de firmware

Con el fin de realizar una actualización manual del firmware, tendrá que ser descargado por primera vez un archivo de actualización.
Busque http://www.pfsense.org y haga clic en el enlace de descarga. En la página Descargas, haga clic en el vincular las actualizaciones. Esto le llevará a la página de selección de espejo. Elija un servidor geográficamente cerca su ubicación para un mejor rendimiento. Una vez que el espejo ha sido seleccionada, aparecerá una lista de directorios con los archivos de actualización para la versión pfSense actual. Descargue la `. Tgz` archivo, (por ejemplo, `pfSense-Full-Update-2.1-RELEASE.tgz)` y el acompañante `. Md5` presentar para verificar la descarga. Consulte la sección llamada "Verificación de la integridad de la descarga" en MD5 para obtener detalles sobre cómo utilizar un `. Md5` presentar.
Para instalar el archivo de actualización, visite el pfSense WebGUI. Haga clic en Sistema Firmware. Haga clic en Activar
Firmware Upload. Haga clic en el botón Examinar situado junto al archivo de imagen del firmware. Busque el archivo de actualización
descargado en el paso anterior y haga clic en Abrir. Por último, haga clic en el botón de actualización del firmware. La actualización tardará unos minutos para cargar y aplicar, en función de la velocidad de la conexión es
utilizado para la actualización y la velocidad del sistema de destino. El cortafuegos se reiniciará automáticamente cuando terminado.

Actualización automática

Actualización automática es una nueva función que va a ponerse en contacto con un servidor pfSense.com y determinar si hay
una nueva versión liberada del que se ejecuta actualmente. Esta comprobación se realiza cuando visita la página de actualizaciones automáticas se encuentra en Sistema Firmware, a continuación, haga clic en la pestaña de actualización automática en el
WebGUI. Si hay una nueva actualización disponible, aparecerá en la lista. Haga clic en el botón para instalar la actualización. La actualización
tomará unos minutos para descargar y aplicar, en función de la velocidad de la conexión a Internet
siendo utilizado y la velocidad del sistema de destino. El cortafuegos se reiniciará automáticamente cuando haya terminado.
Por defecto, la búsqueda de actualizaciones sólo se refiere a conocer oficialmente las versiones de pfSense, pero también es
posible utilizar este método para el seguimiento de instantáneas también. La ubicación de actualización se puede cambiar por visitar
en la pestaña Ajustes del Actualizador, situada inmediatamente a la derecha de la pestaña de actualización automática. Es más seguro utilizar
las versiones publicadas, ya que ven la mayoría de las pruebas y deben ser razonablemente seguro y libre de problemas.
Sin embargo, como con cualquier actualización, primero debe visitar la página web de pfSense y leer las notas de la actualización
para esa versión. Al seleccionar una dirección URL de actualización de la lista, asegúrese de elegir la arquitectura adecuada
(I386 o amd64). Si no está seguro de la arquitectura, compruebe la información del sistema widget en la salpicadero.
A partir de pfSense 2.0, actualización automática funciona en NanoBSD, así como instalación de (todo).

Actualización de uso de la Consola

Una actualización también se puede ejecutar desde la consola. La opción de la consola está disponible en cualquier medio disponible
de acceso a la consola: Video / teclado, consola serie o SSH. Una vez conectado a la consola de la sistema pfSense ser modernizado, iniciar el proceso de actualización por la elección de la opción de menú 13.

Actualizar desde una URL

Si se conoce la dirección URL completa en un archivo de actualización de pfSense, esta es una buena opción. Se evitará tener que primero
descargar el archivo de actualización sólo para subirlo de nuevo, ya diferencia de la función de actualización automática en el
WebGUI también permite que un archivo de actualización personalizada ubicación que se utilizará.

Desde el menú de actualización de la consola, la opción de elegir 1Actualizar desde una URL. Introduzca el URL completo al
archivo de actualización, tales como:

```
http://files.pfsense.org/mirror/updates/pfSense-Full-Update-2.1-
RELEASE-i386.tgz
```

Confirme que la actualización se debe aplicar, y entonces debe ser descargada de forma automática y instalado. Después de la instalación se haya completado, el router se reiniciará automáticamente.

Cuando se le pida una URL para actualizar, también puede escribir auto que utilizará la configuración de actualización automática
para determinar la dirección URL del firmware, en lugar de introducir manualmente la ruta completa a la imagen.

Actualizar desde un archivo local

Un archivo de actualización se puede descargar, como en la actualización manual del firmware anterior, y luego se copia en el
sistema pfSense través scp o Diagnóstico Comando. Para instalar un archivo de este tipo, a la actualización de la consola
menú, elija la opción 2Actualizar desde un archivo local y, a continuación, introduzca la ruta completa al archivo que fue cargado, como `/ Root/pfSense-Full-Update-2.1-RELEASE-i386.tgz.` Confirme que
la actualización se debe aplicar, y entonces debe ser instalado de forma automática. Después de la instalación completa, el router se reiniciará automáticamente.

Actualización de instalar un CD en vivo

En un sistema separado, descargar y grabar un CD con la última versión. Asegúrese de que tiene
movido la configuración en un medio extraíble (USB o disquete) desde el menú de la consola (vea el
sección llamada "Archivo de configuración Mover a dispositivo extraíble"). A continuación, reinicie el router pfSense y arrancar con el nuevo CD. Cuando las botas pfSense en el nuevo CD, el soporte de almacenamiento existente que contiene
su configuración se encuentra y utiliza.

Capítulo 5. Configuración

Después de la instalación, el router pfSense está listo para la configuración. La mayor parte de la configuración se realiza mediante la GUI configurador basado en la web (webConfigurator) o WebGUI para abreviar. Hay algunas tareas que también pueden llevar a cabo fácilmente desde la consola, ya sea un monitor y un teclado, a través de una serie puerto, o por medio de SSH. Algunos de estos pueden ser necesarios antes de que usted será capaz de acceder a la WebGUI, tales
como si desea que aparezca la LAN en una red LAN existente con una dirección IP diferente.

Conexión a la WebGUI

Con el fin de llegar a la WebGUI, debe conectar desde otro PC. Este PC puede conectarse directamente con un cable cruzado, o conectado al mismo conmutador. Por defecto, la IP LAN de un nuevo pfSense sistema es 192.168.1.1 con una máscara / 24 (255.255.255.0), y también hay un servidor DHCP en funcionamiento. Si el ordenador que esté utilizando para conectar está configurado para obtener su dirección IP por DHCP, sólo debería ser una cuestión de
señalando su navegador web favorito para https://192.168.1.1. El sistema utiliza la dirección local de vínculo IPv6 de fe80 :: 01:01 de forma predeterminada en LAN, así que si usted necesita para llegar a la WebGUI sobre IPv6 en un principio, es posible que
hacerlo a través de esa dirección, como https:// [fe80 :: 01:01].

> **Nota**
>
> Algunos navegadores, especialmente Firefox, tienen un error por el que no van a aceptar una firma automática certificado para el acceso HTTPS a través de IPv6 utilizando la IP en la dirección en lugar de un nombre de host. En
> tal caso, otro navegador como Chrome funcionaría, acceso el servidor de seguridad sobre IPv4, o si DNS es funcional, acceder a ella utilizando el nombre de host.

Si usted necesita cambiar la dirección IP de la LAN o desactivar DHCP, esto se puede hacer desde la consola opción 2, a continuación, introduzca la nueva IP LAN, máscara de subred y especifique si se activa o no DHCP. Si decide habilitar DHCP, también se le pedirá que introduzca la dirección de inicio y finalización de la piscina de DHCP, que podría ser cualquier rango que desea dentro de la subred determinada.

Al deshabilitar el servidor DHCP, debe asignar una dirección IP estática en el sistema de pfSense Subred LAN de la PC que se utiliza para la configuración, 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. Comenzando con pfSense 2.0, la interfaz gráfica de usuario escucha en HTTPS por defecto, pero si intenta explorar usando la
HTTP, se le redirigirá al puerto HTTPS en lugar. Si desea acceder a la interfaz gráfica de usuario directamente sin la redirección, utilice https://192.168.1.1.

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

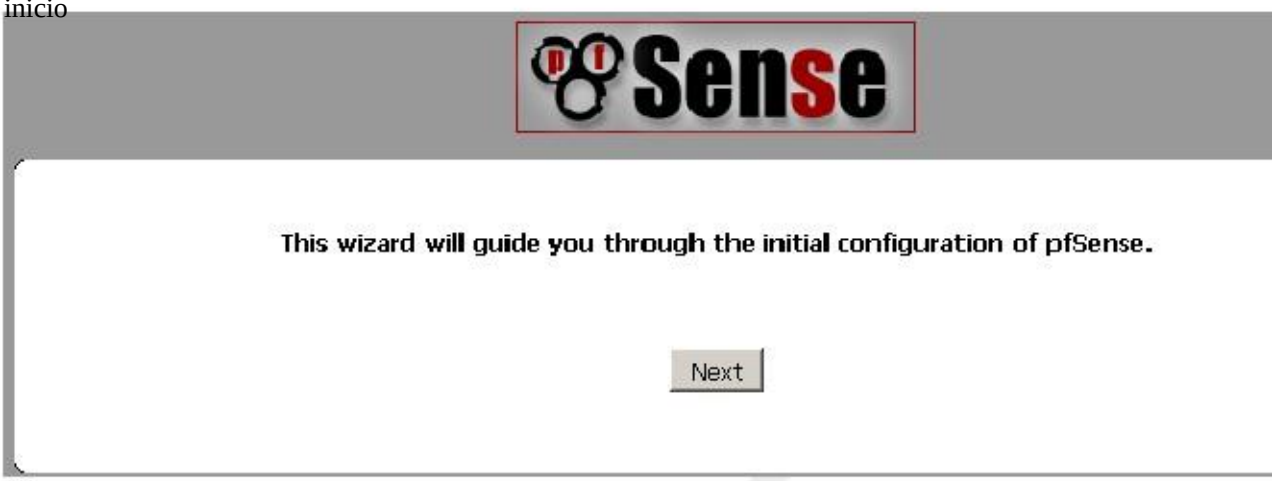
Asistente de configuración

Al navegar a la WebGUI, primero será recibido por una pantalla de inicio de sesión. Para introducir el nombre de usuario administración y la contraseña, introduzca pfSense.

Dado que esta es la primera vez que visita la WebGUI, el Asistente de instalación se iniciará de forma automática, y la voluntad
verse como la Figura 5.1, "Asistente de configuración de inicio de la pantalla". Haga clic en Siguiente para iniciar el proceso de configuración.

> **Nota**
>
> Utilizando el asistente de configuración es opcional. Si necesita crear una configuración más compleja o si los valores por defecto son aceptables, es posible que simplemente clic en el logotipo en la parte superior del asistente
> para volver a la configuración del firewall. Una vez fuera del asistente, a continuación, puede hacer cualquier los ajustes necesarios de forma manual a partir de ahí.

Figura 5.1. Asistente de configuración de la pantalla de inicio

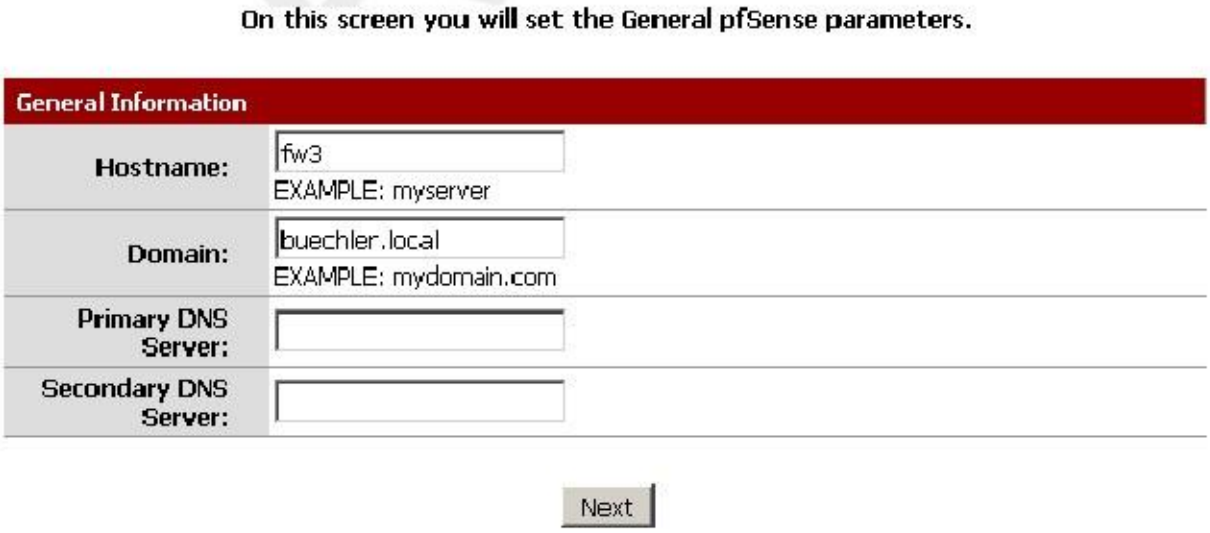


Información general de la pantalla

La siguiente pantalla (Figura 5.2, "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 quiera, pero debe comenzar con una letra, y entonces puede contener sólo letras, números o un guión. Después de que el nombre de host, introduzca un
Dominio, por ejemplo, example.com. Si usted no tiene un dominio, puede utilizar <algo>. locales, donde <algo> es todo lo que quieras: un nombre de la empresa, su apellido, apodo, y así en. El nombre de host y de dominio se combinan para hacer que el nombre de dominio completo el router.

El servidor DNS primario y Servidor DNS secundario podrán rellenarse, si se conoce. Si está utilizando un dinámica del tipo de WAN como las conexiones DHCP, PPTP o PPPoE, éstas por lo general será automáticamente asignada por su proveedor de Internet y se puede dejar en blanco. Estos tipos WAN se explican con más detalle más adelante en
el asistente de configuración. Haga clic en Siguiente cuando haya terminado.

Figura 5.2. Información general de la pantalla



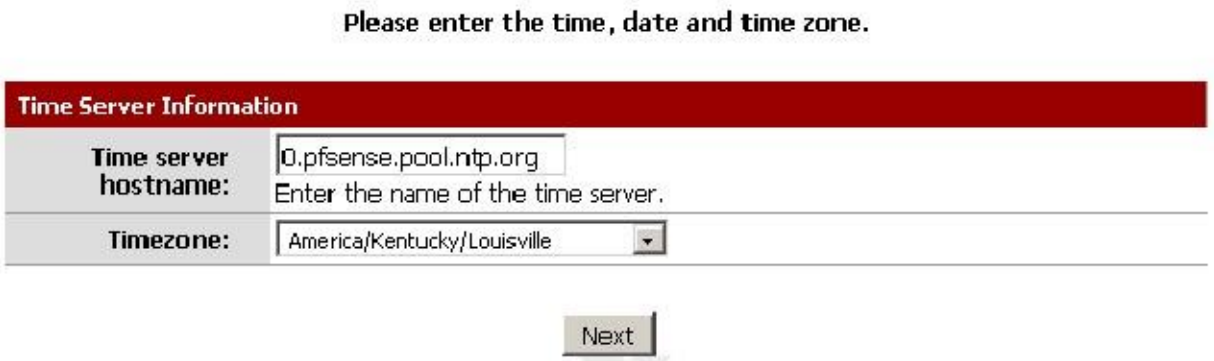
NTP y Configuración del huso horario

La siguiente pantalla (Figura 5.3, "NTP y la zona horaria Configuración de pantalla") tiene un lugar para una Red Time Protocol (NTP) del servidor, y la zona horaria en la que reside el servidor. A menos que tenga una preferencia específica por un servidor NTP, tales como uno dentro de su LAN, lo mejor es dejar el nombre de host del servidor del período predeterminado 0.pfsense.pool.ntp.org, que elegir un

servidor aleatorio de un grupo de conocidos buenos anfitriones NTP. Si se desean los servidores de tiempo múltiple, se pueden añadir en la misma caja, la separación de cada servidor por un espacio. Por ejemplo, si usted quiero cuatro servidores NTP, introduzca 0.pfsense.pool.ntp.org 1.pfsense.pool.ntp.org 2.pfsense.pool.ntp.org 3.pfsense.pool.ntp.org. La numeración es específico de cómo *. Pool.ntp.org opera y garantiza que cada dirección se extrae de una piscina única de IPs por lo que el mismo servidor no se acostumbra dos veces.

Para la selección de zona horaria, seleccione una zona geográficamente llamado que mejor se adapte a la pfSense la ubicación del sistema. No utilice el GMT (Greenwich Mean Time) compensar zonas de estilo. Para obtener más información, consulte la sección denominada "zonas horarias" más adelante en este capítulo. Cuando haya terminado, haga clic en Siguiente para continuar.

Figura 5.3. NTP y la zona horaria Configuración de la pantalla



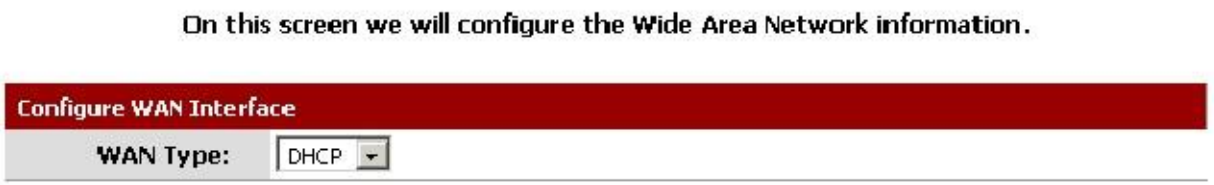
Configuración WAN

Estos párrafos siguientes, y sus imágenes asociadas le servirán de guía a través de la creación de la Interfaz WAN en el sistema pfSense. Dado que este es el lado que da a su proveedor de Internet o router aguas arriba, hay son opciones de configuración para apoyar varios tipos de conexión ISP común. La primera elección es para el WAN Type (Figura 5.4, "Configuración de WAN"). Debe coincidir con lo que su ISP admite, o cualquiera que sea su router anterior se configuró para usar. Las opciones posibles son estáticas, DHCP, PPPoE, y PPTP. La opción por defecto es DHCP, ya que es muy común, y en la mayoría de los casos permitirá que un router "Sólo el trabajo" sin necesidad de configuración adicional. Si no está seguro de qué tipo de WAN para utilizar, o que campos para configurar, tendrá que obtener esta información de su ISP. Si el tipo de WAN no está disponibles en el asistente, o si necesita más información acerca de los tipos de WAN que se encuentran aquí, se encuentra mucha más información detallada en el capítulo 6, Tipos de interfaz y configuración.

Nota

Si usted tiene una interfaz inalámbrica para la interfaz WAN, pueden aparecer algunas opciones adicionales que no están cubiertas en este tutorial del Asistente para la instalación estándar. Puede hacer referencia del capítulo 22, Wireless, que tiene una sección sobre WAN inalámbrica para obtener información adicional. Es posible que deba omitir la configuración WAN por ahora y, a continuación, realizar la configuración inalámbrica después.

Figura 5.4. Configuración WAN



El campo de dirección MAC en la sección siguiente (Figura 5.5, "Configuración general de la WAN") es útil para la sustitución de un router existente con complicaciones mínimas. Algunos ISP, principalmente los dirigidos por Cable proveedores, no funcionará correctamente si se produce una nueva dirección MAC. Algunos requieren ciclos de encendido

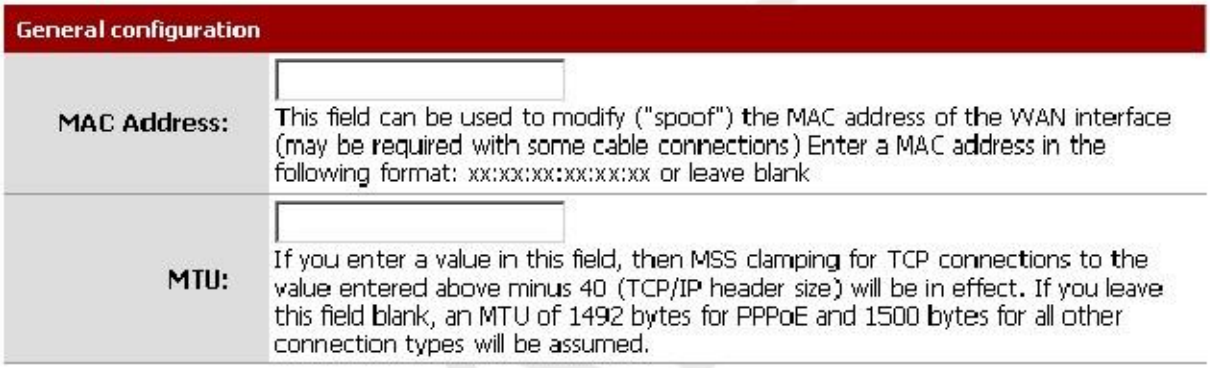
los módem, otros requieren el registro de la nueva dirección con ellos por teléfono. Si este WAN
conexión está en un segmento de red con otros sistemas que lo ubican a través de ARP, el cambio de la MAC para
partido y más viejo pedazo de equipo también pueden ayudar a facilitar la transición, en lugar de tener que borrar ARP
caches o actualizar las entradas ARP estáticas.

Nota

Si alguna vez la intención de utilizar este servidor de seguridad como parte de un clúster de alta disponibilidad (Consulte el Capítulo 24,
Firewall de redundancia / alta disponibilidad), no suplantar la dirección MAC.

La unidad de transmisión máxima (MTU) campo de tamaño se observa en la Figura 5.5, "Configuración general de la WAN"
normalmente se puede dejar en blanco, pero se puede cambiar si se desea. Algunas situaciones pueden requerir un MTU inferior a
asegurar los paquetes son del tamaño adecuado para su conexión a Internet. En la mayoría de los casos, el defecto asume valores para el tipo de conexión WAN funcionarán correctamente.

Figura 5.5. Configuración general de la WAN



Si se elige la opción "Static" para el tipo de WAN, la dirección IP, la máscara de subred en CIDR y Gateway
todos deben ser llenados en la (Figura 5.6, "Configuración de IP estática"). Esta información se debe obtener de su
ISP o quien controla la red en el lado WAN del router pfSense. La dirección IP y
Gateway debe tanto a residir en la misma subred.

Figura 5.6. Configuración de IP estática

Algunos ISP requieren un cierto nombre de host DHCP (Figura 5.7, "Nombre de host DHCP Setting") para ser enviado
con la solicitud de DHCP para obtener una dirección IP WAN. Si no está seguro de qué poner en este campo, tratar de salir
en blanco a menos que se lo indique su proveedor de Internet.

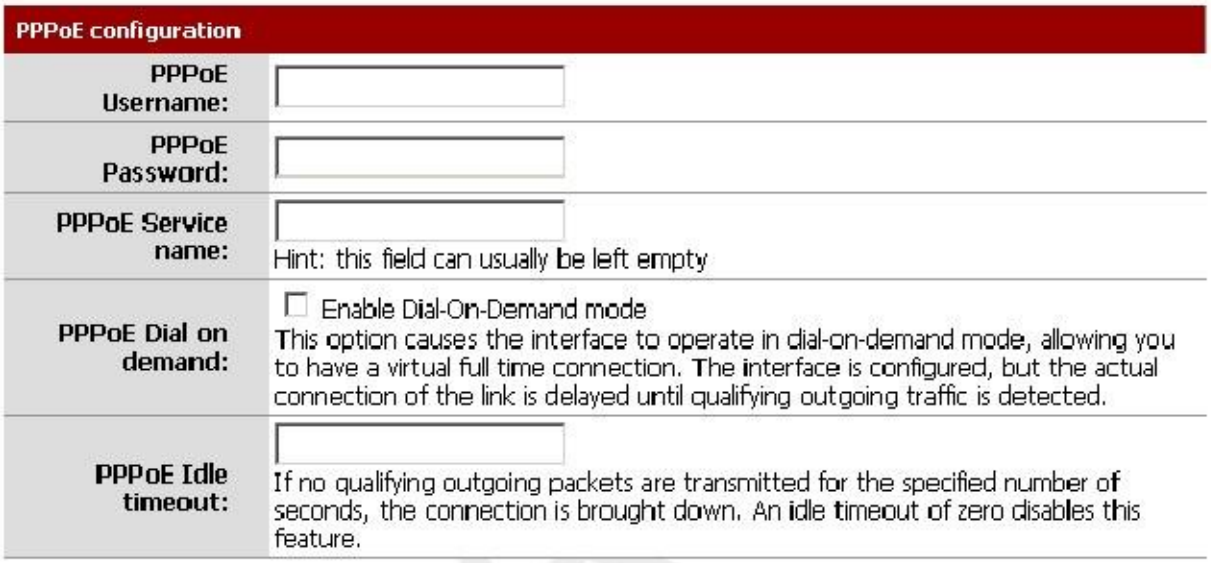
Figura 5.7. DHCP Hostname Ajuste

Cuando se usa el PPPoE (Point-to-Point Protocol sobre Ethernet) WAN tipo (Figura 5.8 ", PPPoE
Configuración "), usted debe, al menos, rellene los campos para PPPoE nombre de usuario y contraseña PPPoE.
Estos serán proporcionados por su proveedor de Internet, y por lo general están en la forma de una dirección de correo electrónico, tales como
mycompany@ispexample.com. El nombre del servicio PPPoE puede ser requerido por algunos proveedores de Internet, pero es
a menudo se deja en blanco. Si usted está en duda, dejarlo en blanco o póngase en contacto con su ISP y preguntar si es necesario.

PPPoE de acceso telefónico en la demanda hará que pfSense para dejar la conexión abajo / fuera de línea hasta que se soliciten datos
que necesitaría la conexión a Internet. Conexiones PPPoE suceden muy rápido, por lo que en la mayoría de los casos, el retrasar mientras que la conexión se configura sería insignificante. Si planea ejecutar cualquier servicio detrás el cuadro de pfSense, ¿no comprobarlo, ya que querrá mantener una conexión en línea tanto como posible en este caso. También tenga en cuenta que esta opción no se caiga la conexión existente.

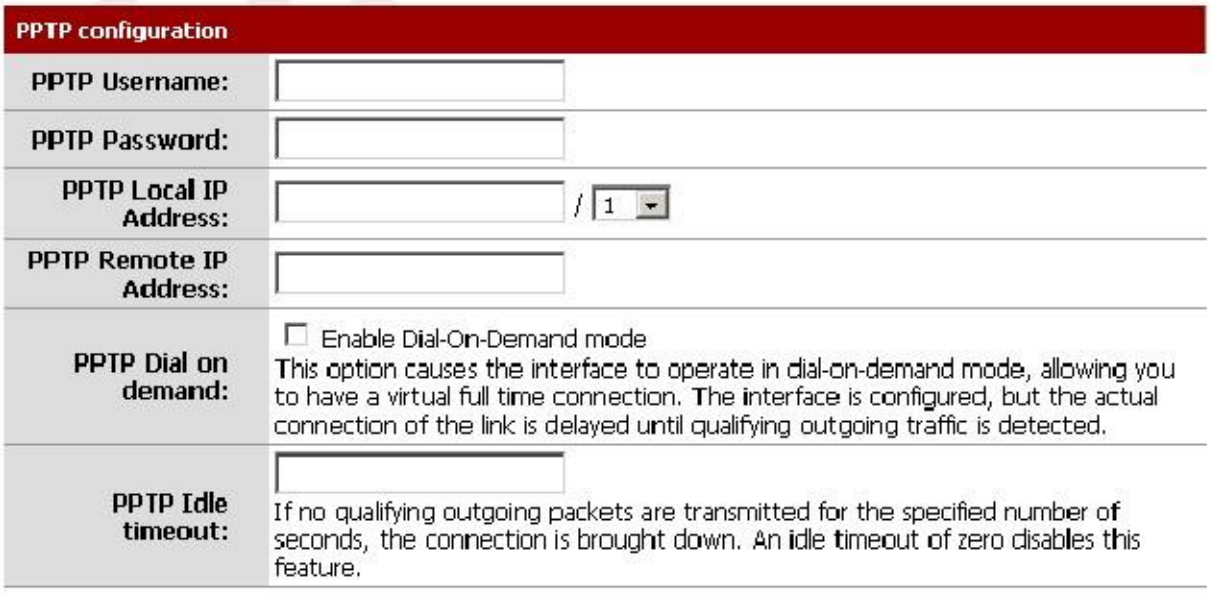
El tiempo de espera de inactividad PPPoE especifica cuánto tiempo pfSense le permitirá la conexión PPPoE ir sin la transmisión de datos antes de desconectar. Esto sólo es realmente útil cuando se combina con el dial de la demanda, y queda por lo general en blanco (desactivado).

Figura 5.8. Configuración PPPoE



El PPTP (Point-to-Point Protocolo de túnel) tipo de WAN (Figura 5.9, "Configuración de WAN PPTP") es la fuente de cierta confusión. Esta opción es para los ISP que requieren un inicio de sesión PPTP, y no para la conexión a una VPN de PPTP a distancia. Estos valores, al igual que la configuración PPPoE, se proporcionarán por su ISP. A diferencia de PPPoE, sin embargo, con una WAN PPTP también debe especificar una dirección IP local, Máscara de subred CIDR, y la dirección IP remota para establecer la conexión.

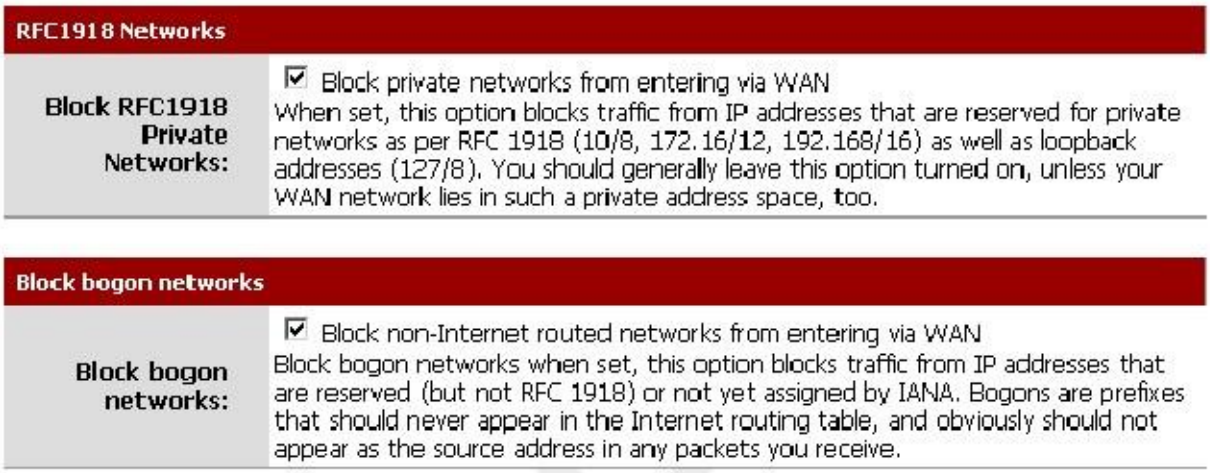
Figura 5.9. Configuración WAN PPTP



Estas dos últimas opciones, visto en la figura 5.10, "Built-in Ingress Opciones de filtro", son útiles para prevenir el tráfico no válido entren en su red, también conocido como "El filtrado de entrada". Habilitación

Bloquear RFC 1918 redes privadas bloquearán redes privadas registradas como 192.168.xx y 10.xxx de realizar las conexiones a su dirección WAN. Una lista completa de estas redes se encuentra en la sección llamados "Direcciones IP privadas". La opción de las redes bogon Bloquear detendrá el tráfico de venir en ese proviene de un espacio IP reservado o asignado que no debe estar en uso. La lista de redes bogon se actualiza periódicamente en el fondo, y no requiere mantenimiento manual. Redes Bogon son explica con más detalle en la sección llamada "Block Bogon Redes". Haga clic en Siguiente para continuar cuando haya terminado.

Figura 5.10. Built-in Ingress opciones de filtrado

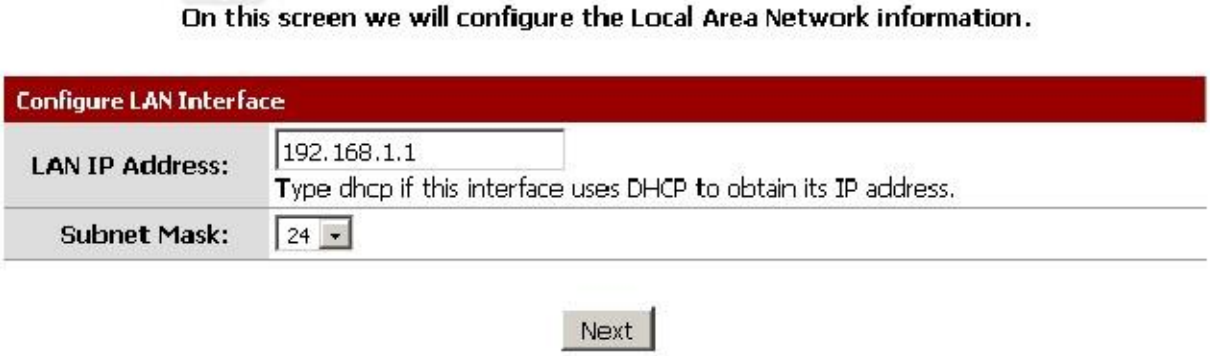


Configuración de la interfaz LAN

Aquí se le da la oportunidad de cambiar la dirección IP de la LAN y la máscara de subred (Figura 5.11, "Configuración de LAN"). Si no tiene pensado alguna vez acerca de la conexión de red a cualquier otra red a través de VPN, por defecto está bien. Si usted quiere ser capaz de conectarse a la red mediante VPN de forma remota ubicaciones, usted debe elegir un rango de direcciones IP privadas mucho más oscura que la muy común 192.168.1.0/24. Espacio en el 172.16.0.0/12 RFC 1918 bloque de direcciones privada parece ser la menos utilizado con frecuencia, así que elige algo entre 172.16.xx y 172.31.xx para menos 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), usted no será capaz de 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 LAN que hay que cambiar, ingrese aquí junto con una nueva máscara de subred. Tenga en cuenta que si usted cambiar estos valores, también tendrá que ajustar la dirección IP de su PC, la liberación / renovar su concesión DHCP, o realizar una "reparación" o "Diagnóstico" en la interfaz de red cuando haya terminado con el asistente de configuración.

Figura 5.11. Configuración de LAN

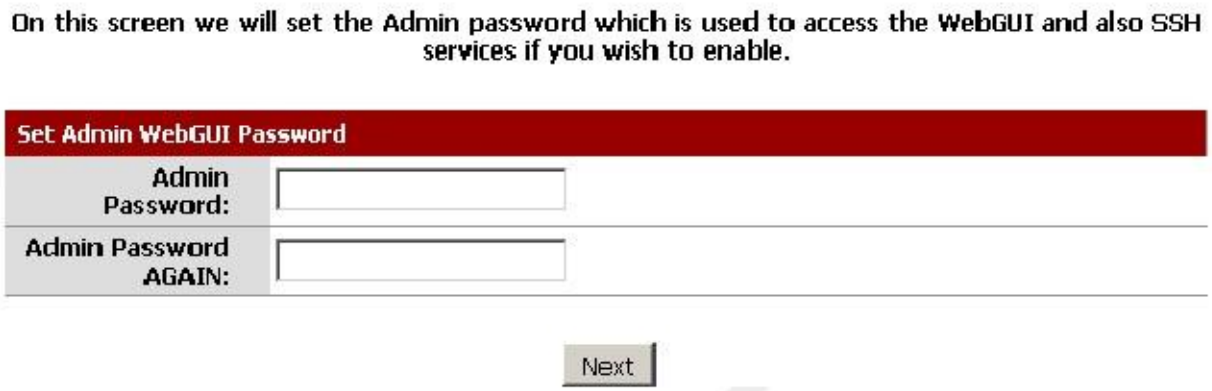


Establezca la contraseña de administrador

A continuación, debe cambiar la contraseña administrativa para la WebGUI como se muestra en la Figura 5.12, "Cambio Contraseña administrativa ". Esta contraseña debe ser algo fuerte y seguro, pero no hay restricciones

se hacen cumplir de forma automática. Introduzca la contraseña dos veces para asegurarse de que se ha introducido correctamente, a continuación,
haga clic en Siguiente.

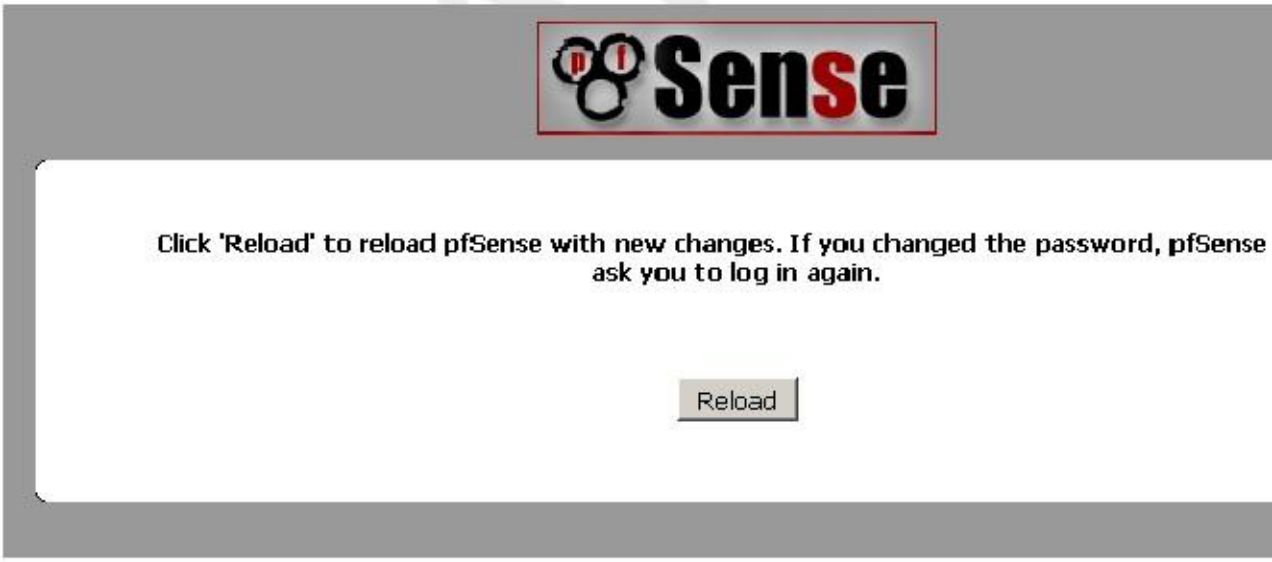
Figura 5.12. Cambiar contraseña administrativa



Completando el Asistente de configuración

Ese es el final del asistente de configuración, haga clic en Actualizar (Figura 5.13, "Reload pfSense WebGUI") y el WebGUI volverá a cargar. Si ha cambiado la IP LAN, ajuste la dirección IP de su PC en consecuencia. Lo harás También se le solicite la contraseña nueva. El nombre de usuario es todavía administrador.

Figura 5.13. Actualizar pfSense WebGUI



En este punto, usted debe tener la conectividad básica a Internet o la red en el lado WAN.
Los clientes de la LAN debe ser capaz de llegar a los sitios a través del router pfSense. Si en algún momento usted que tenga que repetir esta configuración inicial, puede hacerlo dirigiéndose al Sistema Asistente de configuración desde
dentro de la WebGUI.

Configuración de la interfaz

Como se ha visto, alguna configuración de la interfaz se puede realizar en la consola y en el asistente de configuración para comenzar las cosas, pero los cambios también pueden ser realizados después de la instalación inicial visitando la adecuada
lugares bajo el menú Interfaces. Algunas nociones básicas aquí, los detalles se pueden encontrar en el capítulo 6, Tipos de interfaz y configuración.

Asigne las interfaces

Si interfaces adicionales se agregan después de la configuración, entonces pueden ser asignados papeles visitando Interfaces (Asignar). Hay muchas pestañas aquí para assignig y la creación de diversos tipos de interfaces. Los dos pestañas más utilizadas son las tareas y las VLAN de la interfaz. (Configuración de VLAN está cubierto más adelante en el capítulo 14, LAN virtuales (VLAN).) La ficha asignaciones de interfaz muestra una lista de todos los actualmente
las interfaces asignadas: WAN, LAN, y cualquier OPTX que están configurados. Al lado de cada interfaz es una gota-la lista desplegable de todas las interfaces de red / puertos que se encuentran en el sistema, incluidas las interfaces de hardware reales como
así como las interfaces de VLAN y otros tipos de interfaces virtuales. La dirección MAC o VLAN tag mostrará al lado del nombre de la interfaz para ayudar a identificarlo. Las otras fichas (de grupos de interfaces, Wireless, QinQs, las APP, GRE, GIF, Puentes y LAGG), al igual que en la ficha VLAN, están ahí para crear adicional las interfaces que pueden ser asignadas. Todos estos tipos de interfaz se tratan en el capítulo 6, Interfaz Tipos y configuración.

Puede cambiar las interfaces asignadas actualmente escogiendo un nuevo puerto de red o agregar un adicional

Interfaz OPTX haciendo clic. Esto añadirá otra línea, con una nueva interfaz OPT, el número más alto que cualquier interfaz OPT existente, o si no los hay, OPT1. Por defecto, se seleccionará automáticamente la próxima interfaz disponible que no esté asignado. Por ejemplo, si el sistema de destino tiene `fxp0, fxp1,` y `fxp2,` y ha WAN establece en `fxp0,` y LAN establece para `fxp1,` elegir agregar otra interfaz asumirá automáticamente OPT1 será `fxp2.` Si dispone de interfaces adicionales y esto no es la ajuste deseado, y puede ser modificada. Si se realiza algún cambio, asegúrese de hacer clic en Guardar.

Conceptos básicos de configuración de interfaz

Las interfaces se configuran seleccionando su entrada desde en el menú Interfaces. Por ejemplo, a configurar la interfaz WAN, seleccione Interfaces WAN. Casi la totalidad de las opciones que se encuentran bajo

Interfaces WAN son idénticos a los mencionados en la parte WAN del asistente de configuración. El IPv4 Tipo de configuración se puede cambiar entre IPv4 estático, DHCP, PPPoE, PPP, PPTP, L2TP, o ninguno para salir de la interfaz sin una dirección IPv4. Si se elige estática IPv4, una dirección IPv4, la máscara de subred, y la puerta de enlace se puede ajustar. Si se eligen las otras opciones, a continuación, los campos específicos de tipo parecen configurar
cada tipo. El tipo de configuración de IPv6 también se puede cambiar a cualquiera de IPv6 estática, DHCP6, SLAAC, 6rd túnel, túnel 6to4, o ninguno de dejar IPv6 no configurada de la interfaz. Al elegir estático IPv6, es posible establecer una dirección IPv6, la longitud de prefijo y puerta de enlace. Si esta una interfaz inalámbrica, muchos
más opciones aparecerá para configurar la parte inalámbrica de la interfaz, así como la norma elementos de configuración.

En versiones anteriores de pfSense (1.2.x y anteriores), la WAN, LAN, y configuraciones de interfaz OPT diferido. Comenzando con pfSense 2.0, cada interfaz está configurada de forma idéntica. Cualquier interfaz puede ser configurado como cualquier tipo de interfaz (estático, DHCP, PPPoE, y así sucesivamente). Además, el bloqueo de los redes privadas y redes bogon se pueden realizar en cualquier interfaz. Cada interfaz ahora puede ser renombrado, así, como WAN y LAN, a un nombre personalizado de su preferencia. Además, todos los interfaz puede ser activado y desactivado según se desee, siempre y cuando una interfaz permanece activado.

Para obtener más información sobre las opciones de interfaz, consulte la sección titulada "Configuración de la interfaz".

Nota

Selección de una puerta de enlace de la lista desplegable, o la adición de una nueva puerta de entrada y la selecciona, se
hacer pfSense tratar esa interfaz como una interfaz de tipo WAN para NAT y las funciones relacionadas. Esto no es deseable para las interfaces-el revestimiento interior, como LAN o una DMZ. Usted puede todavía utilizar puertas de enlace en esas interfaces con el propósito de rutas estáticas sin seleccionar una puerta de enlace
aquí en la pantalla de las interfaces.

Administración de listas en la GUI

La GUI pfSense tiene un conjunto común de iconos que se utilizan para la gestión de listas y colecciones de objetos en todo el sistema. No todos los icono se utiliza en todas las páginas, pero sus significados son típicamente

coherente basado en el contexto en el que se ven. Ejemplos de tales listas incluyen las reglas del cortafuegos, Reglas NAT, instancias de IPsec o OpenVPN y certificados.

- (+) Icono - Añadir un elemento a una lista. En la parte superior de una lista de los artículos pedidos, el + añadirá un elemento
  al principio de la lista; en la parte inferior, el + se sumará a la final. En las listas no ordenadas la parte superior e inferior + simplemente añadirá un nuevo elemento.
- (E) Icono - Editar una entrada.
- (X) Icono - Eliminar una entrada.
- (Hasta) Icono - Mueve un elemento hacia arriba una fila en una lista ordenada. También se utiliza para indicar una carga o
  función de importación en algunos lugares.
- (Abajo) Icono - Bajar un elemento de una fila en una lista ordenada. También se utiliza para indicar una descarga o la función de exportación en algunos lugares.
- (Izquierda) Icono - Se utiliza para mover elementos. Cuando se trabaja con una lista ordenada, los elementos seleccionados serán
  trasladado a la fila por encima de la flecha cuando se hace clic, como se indica en la interfaz gráfica de usuario con una barra horizontal oscura
  que indica la posición del nuevo elemento cuando esté el ratón sobre este icono. Cuando se trabaja
  con listas de lado a lado, este botón se moverá un elemento de la lista de la derecha a la lista de la izquierda.
- (Derecha) Icono - Se utiliza para mover elementos. Cuando se trabaja con listas de lado a lado, este botón mover un elemento de la lista de la izquierda a la lista de la derecha.
- (Signo de interrogación) Icono - Indica un enlace a las fuentes de ayuda o información adicional.

Si no está seguro de qué acción realizar un icono, coloque el cursor sobre el icono con el puntero del ratón y una información sobre herramientas mostrará una breve descripción de lo que se hará cuando el icono se ha hecho click.

Navegue rápidamente la interfaz gráfica de usuario con accesos directos

Muchas áreas de la interfaz gráfica de usuario tienen una barra de acceso directo de la actualidad, como se ve en la Figura 5.14, "Ejemplo de barra de acceso directo".
Estos atajos se pueden utilizar para navegar a páginas relacionadas dentro de la sección que se está viendo.

Figura 5.14. Barra de acceso directo Ejemplo

Por ejemplo, en la Figura 5.14, "Ejemplo de barra de acceso directo", los accesos directos tendría los siguientes efectos:

- Indicador de estado de servicio (Running) - Este icono está presente si el servicio en esta página se encuentra actualmente
  correr.
- Indicador de estado de servicio (Detenido) - Este icono está presente si el servicio en esta página se encuentra actualmente
  detenido.
- Servicio Inicio - Si se detiene el servicio, este icono le permite iniciar el servicio.
- Reiniciar servicio - Si el servicio se está ejecutando, este icono le permite detener y reiniciar el servicio.
- Deja de uso - Si el servicio se está ejecutando, este icono le permite detener el servicio.

- Página Principal - Cuando aparece este icono, que le llevará de vuelta a la página principal de esta sección.
- Página de estado Link - Este icono es un enlace a la página de estado de esta sección, si es que existe.
- Entrar Página Enlace - Si esta sección tiene una página de registro relacionado, este icono enlaces allí.
- Ayuda Enlace - Carga un tema de ayuda relacionado para esta página.

La página de estado de servicio (Estado Servicios) también ahora ha atajo controles también, para ayudar en la navegación
a páginas relacionadas con un determinado servicio, como se muestra en la Figura 5.15, "Accesos directos en Servicio de estado". Los iconos
tienen el mismo significado que anteriormente.

Figura 5.15. Accesos directos en Serv

Estos accesos directos talados en la cantidad de caza que uno tiene que hacer para localizar páginas relacionadas con Actualmente la está viendo. Uno puede navegar rápidamente entre la página de estado de un servicio, los registros y configuración. Los accesos directos para un tema determinado están presentes en todas las páginas relacionadas con ese tema.

Opciones de configuración generales

Algunas opciones generales del sistema se encuentran en Sistema Configuración general; la mayoría de ellos se verá familiarizado desde el Asistente de configuración.

El servidor de nombre de host y de dominio, servidores DNS, y la zona horaria y la hora NTP se puede cambiar si se desea, como cubiertos en el asistente de configuración.

En esta pantalla, puede agregar hasta cuatro servidores DNS, y además de especificar sus IPs, que
También puede seleccionar la puerta de entrada a utilizar para llegar a cada servidor. Esto es especialmente útil en un multi-WAN
escenario en el que idealmente tiene al menos un servidor DNS por la WAN. Más información sobre los DNS para Multi-WAN se puede encontrar en la sección llamada "Servidores DNS y rutas estáticas".

Junto con la capacidad de cambiar los servidores DNS, hay otra opción: Permitir que la lista de servidores DNS para ser anulado por DHCP / PPP en WAN. Esto básicamente hace lo que dice; Si está marcada, pfSense utilizará
los servidores DNS que se asignan de forma dinámica mediante DHCP o PPP. Ellos serán utilizados por el sistema sí mismo y como los servidores DNS upstream por el reenviador DNS. Estos servidores no serán transmitidos a los clientes DHCP detrás del sistema pfSense, sin embargo.

pfSense 2.0 y posteriores también consultarán propia Forwarder DNS del firewall por defecto para DNS. Este ofrece la ventaja de ser capaz de resolver las direcciones locales de los registros de DHCP y DNS anulaciones, así como consultar a todos los posibles servidores de DNS de una sola vez. Para algunos este comportamiento no es deseable, y
puede ser deshabilitado activando No utilice el reenviador DNS como servidor DNS para el servidor de seguridad.

En las versiones de pfSense antes de 2.0, el nombre de usuario admin y la contraseña se podrían establecer en esta pantalla. Ahora
esas opciones se manejan desde el Administrador de usuarios. La opción para cambiar el puerto WebGUI y Protocolo WebGUI se han trasladado a bajo Sistema Avanzo con el resto del control de la GUI opciones.

Nuevo en pfSense 2.1 es la posibilidad de seleccionar un idioma para la interfaz gráfica de usuario. El valor predeterminado es Inglés y el
único idioma disponible en la actualidad es Portugués (Brasil).

Por último, un tema también puede ser elegido. Varios de ellos están incluidos en el sistema base, y sólo crea cosméticos - no funcionales - cambios en el aspecto y la sensación de la WebGUI. El tema por defecto era cambiado en pfSense 2.0 a ser `pfsense_ng`. Varios otros temas fueron agregados en que la liberación, así, aportado por los miembros de la comunidad.

Opciones de configuración avanzada

En Sistema Avanzada se encuentra una gran cantidad de opciones que son de una naturaleza más avanzada. Ninguno de los
estas opciones deberían necesitar un ajuste para una configuración básica de enrutamiento / NAT, pero usted puede encontrar que algunos de los
los cambios que se rigen por estas opciones le ayudará en la personalización de la configuración de manera beneficiosa. Algunas de estas opciones pueden estar cubiertos en más detalle en otras secciones del libro donde su
discusión sería más tópica o relevantes, pero son todos los mencionados aquí con una breve descripción.

En pfSense 1.2.3 y antes, estas opciones se encuentran todos en una sola página. Debido al número de opciones
y el tamaño de la página, esta se ha dividido en varias pestañas y algunas opciones han convergido
aquí desde otras áreas también.

Administrador de acceso Tab

Las opciones que se encuentran en la ficha Administrador de acceso gobiernan los diversos métodos para administrar el servidor de seguridad,
incluso a través de la interfaz web, ssh, serie y consola física.

webConfigurator (WebGUI)

Protocolo

El Protocolo WebGUI se puede establecer en HTTP o HTTPS. Lo más recomendable sería el uso de HTTPS
de modo que el tráfico WebGUI es encriptada, especialmente si el firewall se gestionará de forma remota.

Certificado SSL

Si se opta por HTTPS, también debe seleccionar un certificado de la lista desplegable Certificado SSL. Fuera
de la caja, usted debe tener por lo menos una opción aquí, webConfigurator defecto. El certificado por defecto
es auto-firmado. Esa no es la situación ideal, pero es mejor que ningún cifrado en absoluto. Esta opción permite
el uso de un certificado existente para mejorar aún más la seguridad y proteger contra el man-in-the-middle
ataques. Si tiene un certificado SSL existente y clave, puede importarlos usando el Certificado
Manager y, a continuación, seleccione el certificado aquí. También puede presentar certificados adicionales mediante el uso de la
El administrador de certificados si es necesario.

El principal inconveniente de utilizar un certificado auto-generada a medida es la falta de seguridad de la identidad
del huésped, ya que el certificado no está firmado por una autoridad de certificación de confianza para tu navegador.
Además, dado que la mayor parte de los usuarios de Internet debe considerarse como un certificado no válido
un riesgo, los navegadores modernos se han tomando medidas enérgicas contra la forma en que se manejan. Firefox, por ejemplo,
da una pantalla de advertencia y obliga al usuario a importar el certificado y permitir una excepción permanente.
Internet Explorer mostrará una pantalla de advertencia con un enlace a seguir, al igual que Chrome. Opera mostrará
un cuadro de diálogo de advertencia que también permite una derivación permanente.

Puerto TCP

Traslado de la WebGUI a un puerto alternativo es también una buena táctica para mayor seguridad, y se va a liberar
los puertos web estándar para su uso con forwards del puerto y otros servicios como un proxy Squid. Por defecto
WebGUI utiliza HTTPS en el puerto 443 con una redirección desde el puerto 80 para la mejor compatibilidad y facilidad
de configuración inicial. Si desea cambiar el puerto, introduzca un nuevo número de puerto en el TCP
Campo Puerto.

Procesos Max

Si usted encuentra que usted ha varias personas que visitan la interfaz gráfica de usuario al mismo tiempo, y algunas páginas está tomando
demasiado tiempo para cargar, o en su defecto a la carga, entonces es posible que tenga que aumentar el valor de Max Procesos. Por defecto
se establece en 2, lo que se ejecuta dos procesos de servidor web.

WebGUI Redirect

De forma predeterminada, para facilitar el acceso y la compatibilidad, el firewall se ejecuta una redirección en el puerto 80 de manera que si
intentar acceder al router con HTTP, aceptará la solicitud y luego redireccionar la sesión para
HTTPS en el puerto 443. Esta redirección se puede desactivar mediante la comprobación Disable webConfigurator redirigir regla
si algo más tiene que enlazar con el puerto 80 o hay otra razón sería no deseado.

WebGUI Login Autocompletar

Para mayor comodidad, el formulario de acceso permite autocompletar para que su navegador puede guardar las credenciales de inicio de sesión. En
algunos entornos, como los que necesitan para cumplir con las directrices de seguridad específicas, este comportamiento es
no es aceptable. Como tal, se puede desactivar la comprobación Disable webConfigurator inicio de sesión de autocompletar.
Tenga en cuenta, sin embargo, que no todos los navegadores que respeten esta opción. En concreto, la ópera sigue siendo propondrá guardar
contraseñas incluso cuando la forma especifica que no se debe permitir. Esta autocompletar únicos controles
en el formulario de inicio de sesión. Incluso si autocompletado está habilitada para inicio de sesión, la cumplimentación de los formularios en el otro lugar
GUI permanece deshabilitado para evitar que el navegador se llenen automáticamente sus credenciales en relación campos.

Mensajes de inicio de sesión WebGUI

Los inicios de sesión con éxito se traducirá en un mensaje que se está imprimiendo a la consola, y en algún hardware esta voluntad
También causa un "pitido" para ser escuchado desde el dispositivo cuando se produzca un mensaje de este tipo de consola. Si no lo hace
desear ver este mensaje (o escuchar el pitido resultante), compruebe el registro de Deshabilitar webConfigurator cuadro de los inicios de sesión con éxito.

Anti-bloqueo

De forma predeterminada, el acceso a la WebGUI y SSH en la interfaz LAN siempre se permite, independientemente de las reglas de filtro definidas por el usuario. La activación de esta función permite el control más detallado sobre el cual Direcciones IP de LAN pueden acceder a la WebGUI, pero asegúrese de que usted tiene una regla de filtro en su lugar para permitir el acceso
antes de habilitar esta opción!

> **Nota**
>
> Restablecimiento de la IP LAN de la consola del sistema también se restablecerá esta opción. Si usted se encuentra bloqueado después de habilitar esto, elija la opción del menú de la consola para configurar la IP LAN e introduzca en la misma dirección IP y la información adjunta.

En pfSense 1.2.x esta regla permite que todo el tráfico para llegar a la dirección IP de LAN del servidor de seguridad. En pfSense 2.x, esta
comportamiento se limita a que sólo permite el acceso al puerto de interfaz gráfica de usuario y el puerto SSH. En pfSense 2.0 y
después, si sólo tiene una interfaz habilitada, la regla anti-bloqueo se activará en esa interfaz.

DNS Rebind Check

Las opciones restantes de esta sección controlan algunas de las nuevas medidas de seguridad puestas en marcha para proteger a la interfaz gráfica de usuario contra varios medios de ataques basados en el navegador. El primero de ellos es Revinculación DNS
Los cheques. Cuando se establece, este bloquea las respuestas de IP privadas de sus servidores DNS configurados. Comprobar
esta casilla para desactivar esta protección si interfiere con el acceso webConfigurator o resolución de nombres
en su entorno. Más detalles sobre los ataques de revinculación DNS se puede encontrar en Wikipedia [http://en.wikipedia.org / wiki / DNS_rebinding]. Para desactivar este comportamiento, consulte Disable DNS Revinculación
Los cheques. La causa más común para la desactivación de esto sería cuando el cortafuegos está configurado para utilizar un interno
Servidor DNS que devolverá (RFC1918) respuestas privadas para nombres de host. Si accede al servidor de seguridad Dirección IP, estos controles no se hacen cumplir porque el ataque sólo es relevante cuando se utiliza un nombre de host.

Cumplimiento HTTP_REFERER Browser

La GUI también comprueba la URL de referencia cuando se tiene acceso, para evitar que una forma en otro sitio desde la presentación de una solicitud al servidor de seguridad, el cambio de una opción cuando no tenía la intención de que eso suceda. Este
también rompe algunos comportamientos deseables, tales como tener una página que enlaza a los distintos dispositivos de firewall.
Si desea desactivar este comportamiento, puede marcar Disable Reviso de aplicación HTTP_REFERER.

Nombres de host alternativos

Si desea mantener las opciones anteriores está activada, pero controlar el comportamiento ligeramente, puede rellenar nombres de host alternativos en los nombres de los sistemas alternativos para Revinculación DNS y cheques HTTP_REFERER
caja. Por defecto, el sistema permitirá el acceso al host configurada en el servidor de seguridad y todas las IPs configurado en el sistema.

Man-in-the-middle / advertencia

Si intenta acceder al servidor de seguridad mediante una dirección IP que no está configurado en el sistema, tales como puerto hacia adelante desde otro servidor de seguridad, un mensaje será impreso que puede ser el resultado de un Man-In-The-middle (MITM) ataque. Si ha configurado un desvío por ejemplo a ti mismo, el mensaje puede ser de forma segura ignorado. Si no ha configurado el futuro, entonces usted debe tener mucho cuidado antes de iniciar la sesión en asegurarse de que sus credenciales de inicio de sesión no se enrutan a través de un sistema que no controlas o fideicomiso. Acceso
no está desactivada en este caso, sólo una advertencia, por lo que no hay ninguna opción para desactivar este comportamiento.

Secure Shell (SSH)

El servidor Secure Shell (SSH) se puede activar lo que permitirá a la consola remota y gestión de archivos. Usted puede conectar con cualquier cliente SSH estándar, como la línea de comandos OpenSSH ssh cliente, PuTTY, SecureCRT o iTerm. O bien el nombre de usuario WebGUI (como administrador) o la cuenta de root Pueden ser utilizados, y ambos aceptan la contraseña WebGUI para iniciar sesión. Si ha creado otros usuarios en el Administrador de usuarios y también tienen el Usuario - Sistema - Shell permiso de acceso de cuenta, entonces son permitido hacer login a través de ssh también.

Las transferencias de archivos desde y hacia el sistema pfSense también son posibles mediante el uso de un cliente de Secure Copy (SCP)
tales como la línea de comandos de OpenSSH scp, FileZilla, WinSCP o Fugu. Para utilizar SCP, debe conectarse como el usuario root, no la de administración. Si ha creado un usuario que tiene el usuario - sistema - Copiar archivos permiso, o todo el acceso, entonces se puede también utilizar SCP.

Habilitar Secure Shell

Para habilitar SSH, marque la casilla junto a Activar Secure Shell. Después de guardar con este ajuste se activa, el sistema generará las claves SSH (si no están ya presentes) e inicie el daemon SSH.

Método de autenticación

También puede establecer SSH sólo permitir las conexiones a base de teclado y no una contraseña. El cambio a única llave-
inicio de sesión basado es una práctica mucho más segura, aunque sí tener un poco más de preparación para configurar. Para ello, marque Desactivar contraseña de inicio de sesión de Secure Shell (sólo claves RSA). Para agregar claves de teclado
inicio de sesión basado en la edición de sus usuarios en el Administrador de usuarios y pegar las claves pública permitidas en el
Campo de texto de claves autorizadas para su cuenta. En pfSense 1.2.x y anteriores, había una caja para pegar

SSH Puerto

lo clave ya que no había una sola cuenta (admin).

También es más seguro para mover el servidor SSH a un puerto alternativo. Como con el movimiento de la WebGUI a un puerto alternativo, se proporciona una pequeña mejora en la seguridad, y libera el puerto si desea reenviar
a un sistema interno. Para cambiar el puerto, escriba el nuevo puerto en el cuadro Puerto SSH.

Mejores prácticas para SSH

Si usted se encuentra en una situación que requiere dejar el acceso SSH sin restricción por las reglas del cortafuegos, que puede ser peligroso, es muy recomendable que en esta situación que tanto se mueve el servicio SSH
a un puerto aleatorio alterno y cambie a la autenticación basado en claves. Mudarse a un puerto alternativo se evitar ruidos registro de fuerza bruta los intentos de inicio de sesión SSH y exploraciones ocasionales. Todavía se puede encontrar con un puerto
exploración, por lo que el cambio a la autenticación basada en clave siempre debe hacerse en cada acceso público Servidor SSH para eliminar la posibilidad de éxito de los ataques de fuerza bruta. Los inicios de sesión fallidos múltiples

de la misma IP resultará en el bloqueo a cabo el sistema remoto intentando autenticar, pero que solo no debe ser considerado una protección suficiente.

Serial Console

Si este sistema pfSense va a correr "sin cabeza" (sin teclado, vídeo, ratón adjunta) puede ser deseable para habilitar esta opción, que redirigir la consola de entrada / salida para el puerto serie. Esta voluntad No desactive el teclado a bordo, vídeo y ratón, pero le permitirá conectar un cable de módem nulo al puerto serie y gestionarlo directamente desde otro PC o dispositivo serie. Después de hacer los cambios, asegúrese de hacer clic en Guardar cuando haya terminado.

Tanto con la consola serie habilitado y, se prefiere la consola serie un monitor conectado, por lo que será recibir los mensajes de registro de arranque de pfSense. Algunos otros mensajes del kernel del sistema operativo se mostrará en todos los consolar a las conexiones, y ambas consolas tendrán un menú utilizable.

Para obtener más información sobre la conexión a una consola serie, consulte la sección "Conexión de un cable serie" y la sección denominada "Inicio de un cliente de serie".

Serie Velocidad Console

Nuevo en pfSense 2.1 es la capacidad de cambiar la velocidad de la consola serie. Anteriormente, esto siempre estaba cerrada a 9600 bps. Ahora puede ser mayor al seleccionar una velocidad más rápida en el menú desplegable. El más rápido velocidad posible es 115200 bps.

Menú Console

Normalmente, el menú de la consola siempre está mostrando en la consola del sistema, y estará disponible en tanto cuando usted tiene acceso físico a la consola serial o de vídeo. En algunas situaciones esto no es deseable, por lo Esta opción permitirá a la consola para ser protegido por contraseña. Usted puede iniciar sesión con el mismo nombre de usuario y la contraseña utilizada para la WebGUI. Después de establecer esta opción, debe reiniciar el sistema pfSense antes de que surta efecto.

Nota

Si bien esto se detendrá la pulsación accidental, y mantener fuera a los usuarios casuales, esta no es en absoluto un método de seguridad perfecto. Una persona bien informada con acceso físico todavía podía restablecer la contraseñas (ver la sección llamada "contraseña olvidada con una consola Bloqueado"). Usted debe considerar otros métodos de seguridad física si que es un requisito de su instalación.

Firewall / NAT Tab

Firewall avanzada

Compatibilidad IP Do-Not-Fragmento

Esta es una solución para los sistemas operativos que generan paquetes fragmentados con el no fragmentar (DF) bit. Linux NFS (Network File System) es conocido por hacer esto. Esto hará que el filtro para no caer tales paquetes, pero en vez de manifiesto la no fragmenten bits. El filtro también de forma aleatoria la identificación IP ámbito de los paquetes salientes con esta opción, para compensar los sistemas operativos que establecen el bit DF sino establecer un campo de cabecera de identificación IP cero.

Generación IP Random ID

Si Inserte un identificador más fuerte en la cabecera IP de los paquetes que pasan a través del filtro está marcada, el servidor de seguridad sustituye el campo de identificación de IP de los paquetes con valores aleatorios para compensar sistemas operativos que utilizar valores predecibles. Esta opción sólo se aplica a los paquetes que no están fragmentados después de la opcional reensamblaje de paquetes.

Opciones de optimización del servidor de seguridad

Hay algunas opciones aquí que controlan cómo el firewall expire estados:

Normal	El algoritmo de optimización estándar.
Alta latencia	Se utiliza para los enlaces de alta latencia, como los enlaces por satélite. Expira conexiones inactivas después de la morosidad.
Agresivo	Expira conexiones inactivas más rápido. Un uso más eficiente de la CPU y la memoria, pero puede soltar las conexiones legítimas antes de lo esperado. Esta opción también puede mejorar rendimiento en despliegues de alto tráfico con una gran cantidad de conexiones, como web servicios.
Conservador	Trata de evitar que se caiga ninguna conexión legítimos, a expensas de una mayor uso de la memoria y de la CPU.

Desactivar Firewall

Si elige Desactivar todos los filtros de paquetes, que a su vez su sistema de pfSense en un enrutamiento de solo plataforma. Como consecuencia, el NAT también se desactivará. Si sólo desea desactivar NAT, no hacer utilizar esta opción, preferiría ver la sección "Desactivación de salida NAT" para obtener más información sobre controlar el comportamiento NAT saliente.

Desactivar Firewall Scrub

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

Nota

Desactivación de matorrales también desactivará otras características que dependen de matorrales para funcionar, como bit DF compensación y la aleatorización ID.

Firewall Estados máxima

Establece el número máximo de conexiones de sostener en la tabla de estado del firewall. El valor predeterminado es dinámico, y dimensionado a 10% de la cantidad de RAM en el sistema. Este valor por defecto debería ser suficiente para la mayoría instalaciones, pero se puede ajustar más alto o más bajo 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 que usted tener RAM libre adecuado antes de aumentar este. Estados Firewall se discuten en la sección llamado "filtrado activo".

Tablas Máximo Firewall

El número máximo de tablas que pueden existir en el sistema para artículos tales como alias. Tenga en cuenta que este es el número de tablas / alias sí mismos, no el número de elementos en el interior alias (que es la siguiente opción). Por De forma predeterminada es 3000 entradas, que debido a las varias formas en que el sistema funciona de manera efectiva que limita a alrededor de 1500 los alias. Esto se puede aumentar, según sea necesario, con poco o ningún impacto sobre otros recursos, pero teniendo que muchos alias también serían difíciles de manejar en el GUI.

Firewall Entradas máximas de mesa

Número máximo de entradas que pueden existir dentro de las tablas de sistemas como los alias, sshlockout, esnifar, y así sucesivamente. Por defecto es el 200 000 entradas. Si utiliza características como alias de URL de tabla a cargar grandes bloques de espacio de direcciones en los alias, entonces es posible que tenga que aumentar este valor. Cada tabla entrada consumirá cierta cantidad de memoria RAM, así que ten cuidado de no fijar arbitrariamente alta.

Filtrado de rutas estáticas

Las reglas de firewall bypass para el tráfico en la misma opción de interfaz sólo se aplica si se ha definido una o más rutas estáticas. Si está habilitada, el tráfico que entra y sale a través de la misma interfaz no ser controlados por el servidor de seguridad. Esto puede ser deseable en algunas situaciones donde múltiples subredes están conectados a la misma interfaz, para evitar bloquear el tráfico que pasa a través del servidor de seguridad en uno dirección sólo por enrutamiento asimétrico. Vea la sección llamada "Reglas de derivación de firewall para el tráfico sobre la misma interfaz "para una discusión más a fondo sobre este tema.

Reglas VPN añadidas autodestruibles

Esto desactiva las reglas añadidas de forma automática para IPsec y PPTP. Normalmente, cuando se habilita uno de estos VPNs, se añaden automáticamente reglas para la interfaz adecuada que permitirá el tráfico a los puertos. Al desactivar estas reglas automáticas, usted puede tener un mayor control sobre lo que se permite añadir direcciones para conectarse a la VPN.

Desactivar Reply-To

Con Multi-WAN generalmente quiere asegurarse de tráfico deja la misma interfaz que llega, por lo tanto, reply-to se añade automáticamente de forma predeterminada para garantizar esta asociación para el tráfico de retorno. Al utilizar puente, debe desactivar este comportamiento si la puerta de enlace IP WAN es diferente de la puerta de enlace IP de los anfitriones detrás de la interfaz de puente. Otro caso de uso implica el enrutamiento estático a otros sistemas en un mayor subred WAN donde esta opción ayudaría a asegurar que las respuestas fueron de nuevo al sistema adecuado en lugar de ser enviados de nuevo a la puerta de enlace.

Desactivar reglas Negate

Con Multi-WAN generalmente quiere asegurar que el tráfico llega a las redes conectadas directamente y VPN redes cuando se utiliza la política de enrutamiento. pfSense insertará algunas reglas para pasar este tráfico local y VPN sin una puerta de entrada se especifica, para mantener la conectividad. Puede desactivar esta para fines especiales, pero si lo hace, debe crear manualmente las reglas para estas redes sin una puerta de enlace establecido para que puedan ser alcanzado sin la política de enrutamiento.

Network Address Translation

Reflexión NAT en Port Delanteros

El modo de reflexión NAT para el puerto reenvía opción controla cómo se hacen las reglas NAT reflexión. Estos NAT redirigir reglas le permiten acceder a puerto remite en sus direcciones IP públicas desde dentro sus redes internas. Estas reglas están deshabilitadas de forma predeterminada, no se crean reglas de reflexión para NAT a menos que cambie este ajuste. Consulte la sección titulada "Reflexión NAT" para una discusión sobre la méritos de Reflexión NAT cuando se compara con otras técnicas tales como DNS dividido.

El modo de proxy NAT + utiliza un programa de ayuda para enviar paquetes a la meta del puerto hacia adelante. Es útil en configuraciones donde la interfaz y / o puerta de enlace IP utilizada para la comunicación con el objetivo no puede determinarse con precisión en el momento se cargan las reglas. Reglas de reflexión no se crean para los rangos más de 500 puertos y no será utilizado por más de 1.000 puertos en total entre todos los desvíos de puerto. Sólo se admiten los protocolos TCP y UDP.

El modo NAT pura utiliza un conjunto de reglas NAT para dirigir los paquetes al destino del puerto hacia adelante. Tiene mejor escalabilidad, pero debe ser posible determinar con precisión la interfaz de puerta de enlace IP y utilizado para la comunicación con el objetivo en el momento se cargan las reglas. No hay límites inherentes a la número de puertos distintos de los límites de los protocolos. Todos los protocolos disponibles para los delanteros del puerto son apoyado.

Reglas NAT individuales también contienen una opción para reemplazar el comportamiento determinado por esta selección, por lo que que pueden tener NAT reflexión forzado dentro o fuera sobre una base caso por caso.

Tiempo de espera de Reflexión

El valor Tiempo de Reflexión permite forzar un tiempo de espera para las conexiones hechas al realizar Reflexión NAT para los delanteros de puerto en modo NAT + Proxy. Si algunas conexiones permanecen abiertas más tiempo
de lo deseado y causando problemas, esta opción podría ayudar a mitigar ese problema.

Reflexión NAT para NAT 01:01

Cuando checeked, esta opción añade mapeos NAT 01:01 adicionales para el acceso a 1:01 asignaciones de su direcciones IP externas desde dentro de sus redes internas. Esto le da a la misma funcionalidad que ya existe para los delanteros del puerto, pero para NAT 1:1. Hay algunos escenarios de enrutamiento complejas que pueden hacer
esta opción ineficaz. Además, esto sólo afecta a la ruta de entrada de NAT 1:1, no de salida.
El estilo de la regla subyacente es similar al modo NAT puro para los delanteros portuarios. Al igual que con puerto remite,
hay opciones por entrada para anular este comportamiento.

NAT saliente para 1:01 Reflexión NAT

Cuando la casilla está seleccionada para crear automáticamente reglas NAT salientes que ayudan NAT entrante reglas que dirigen el tráfico de vuelta a la misma subred que se originó, se hace lo que dice la opción.
Añade algunas reglas adicionales que permiten 01:01 Reflexión NAT funcione plenamente. En la mayoría de los casos, querrán marcar esta casilla si desea 1:01 Reflexión NAT para trabajar. Esto sólo funciona para la Asignación de interfaces. Otras interfaces requieren crear manualmente las reglas NAT salientes que dirigen la respuesta paquetes a través del enrutador.

TFTP Proxy

El proxy de TFTP incorporado voluntad conexiones proxy a los servidores TFTP que se encuentran fuera del cortafuegos, de modo que
conexiones de cliente se pueden hacer a los servidores TFTP remotas. Puede pulsar la tecla Ctrl o Mayús y haga clic para seleccionar
múltiples entradas de la lista. Si se eligen sin interfaces, el servicio de proxy TFTP está desactivado.

Redes Tab

Opciones IPv6

Permitir IPv6

Comenzando con pfSense 2.1, filtrado IPv6 está soportado por lo que la opción Permitir tráfico IPv6 está habilitado de forma predeterminada. Si usted no desea permitir el tráfico IPv6 a través de su servidor de seguridad, puede desactivar esta casilla
y todo el tráfico IPv6 a continuación, se bloqueará y sin registro.

IPv6 sobre IPv4

Usted también puede verificar Habilitar IPv4 NAT encapsulación de paquetes IPv6 marcando dicha casilla, permite 41/RFC protocolo IP 2893 reenvío a la dirección IPv4 especificada en el campo Dirección IP. Que le permita reenviar todo el tráfico IPv6 a un host detrás de este cortafuegos en vez de manejar de forma local.

Interfaces de red

Sondeo de dispositivos

Dispositivo de sondeo es una técnica que permite que el sistema de sondear periódicamente los dispositivos de red para los nuevos datos en lugar
de depender de las interrupciones. Esto evita que su WebGUI, SSH, etc de ser inaccesible debido a interrumpir inundaciones cuando está bajo carga extrema, a costa de la latencia ligeramente superior (hasta 1 ms). Este es generalmente
innecesario, a menos que se subdimensionada su hardware.
El sondeo también requiere soporte de hardware en las tarjetas de red de su sistema. De acuerdo con el sondeo (4) hombre
página para FreeBSD 8.3 (sobre la cual se basa pfSense 2.0), el `bge (4), dc (4), em (4), fwe (4),`

`capirotazo (4)`, `fxp (4)`, `ixgb (4)`, `nfe (4)`, `ESN (4)`, `re (4)`, `rl (4)`, `sf (4)`, `hermana (4)`, `ste (4)`,
`stge (4)`, `vge (4)`, `VR (4)`, y `xl (4)` dispositivos son compatibles, con soporte para otras pendientes en futuro de FreeBSD.

> **Nota**
>
> Con el sondeo se activa, el sistema aparecerá a utilizar el 100% de la CPU. Esto es normal, ya que el sondeo hilo está usando la CPU para buscar paquetes. El subproceso de sondeo se ejecuta con una prioridad más baja de modo que si
> otros programas necesitan tiempo de CPU, será renunciar a ella cuando sea necesario. El inconveniente es que esta opción
> hace que el gráfico de la CPU menos útil.

Offloading Checksum Hardware

Al seleccionar esta opción desactivará hardware checksum descarga. La descarga de la suma de comprobación se divide en
un poco de hardware, en particular algunas tarjetas Realtek. En raras ocasiones, los conductores pueden tener problemas con la suma de comprobación
descarga y algunas tarjetas de red específicas. Los síntomas típicos de la descarga de la suma de comprobación rota son paquetes corruptos y los malos resultados de rendimiento.

Offloading Segmentación TCP Hardware

Al seleccionar esta opción desactivará hardware segmentación TCP descarga (TSO, TSO4, TSO6). Este
la descarga se rompe en algunos controladores de hardware, y puede influir en el rendimiento con algunas tarjetas de red específicas.
Esta opción es más deseable para estaciones de trabajo / aparatos que para los routers y cortafuegos, de modo que se deja como
una opción en caso de que sí aumenta el performance para determinadas implementaciones.

Hardware Large Recibe Offloading

Al seleccionar esta opción desactivará hardware grande recibir descarga (LRO). Esta descarga de se rompe
en algunos controladores de hardware, y puede influir en el rendimiento con algunas tarjetas de red específicas. Al igual que con el TSO
opción anterior, esta opción es más deseable para estaciones de trabajo / aparatos que para los routers y cortafuegos, por lo que se deja como una opción en caso de que lo hace aumentar el rendimiento de ciertos despliegues.

Suprimir los mensajes ARP

Si tiene dos o más interfaces que comparten la misma red física, como en un escenario donde
múltiples interfaces están conectados en el mismo dominio de difusión, esta opción se oculta la ARP espuria mensajes que de otra forma sobrecarguen los registros con entradas inútiles.

Tab Varios

Soporte Proxy

Si este servidor de seguridad reside en una red detrás de un proxy, puede entrar en las opciones de proxy a continuación para que
solicitudes del servidor de seguridad para las cosas tales como paquetes y actualizaciones se enviarán a través del proxy.

Proxy URL

Esta opción especifica la ubicación del proxy para realizar las conexiones externas.

Puerto de proxy

El puerto que se utiliza para conectarse a la dirección URL de proxy. Por defecto, el puerto es 8080 para las URL de proxy http,
y 443 para las URL de proxy SSL.

Proxy Nombre de usuario

En caso necesario, este es el nombre de usuario que debe ser enviado cuando el cortafuegos debe usar el proxy.

Contraseña de proxy

Si es necesario, esta es la contraseña asociada con el nombre de usuario establecido en la opción anterior.

Equilibrio de carga

Conexiones Sticky

El texto en el WebGUI explica mejor opción Conexiones Sticky en esta sección: Los sucesivos conexiones serán redireccionados a los servidores de una manera round-robin con conexiones desde la misma fuente que se envía al mismo servidor web. Esta "conexión pegajosa" existirá mientras haya estados que se refieren a esta conexión. A la expiración de los estados, también lo hará la conexión pegajosa. Otras conexiones desde ese host será redirigido a otro servidor web en el round robin.

conexiones "Sticky" son deseables para algunas aplicaciones que se basan en las mismas direcciones IP se mantienen a lo largo de un determinado período de sesiones. Esto se utiliza en combinación con la funcionalidad de equilibrio de carga del servidor,
descrito en el capítulo 21, Equilibrio de carga del servidor.

Esta opción se aplica a Balanceo de carga saliente (multi-WAN), así como el equilibrio de carga del servidor.

También puede introducir un valor para el seguimiento de tiempo de espera de la fuente de las conexiones adhesivas. Esto retendrá la
asociación pegajosa de un anfitrión después de la totalidad de los estados de ese host caduca para sin embargo muchos segundos
se introducen en la caja. Por defecto, este valor no está establecido, que tomará valor 0 para el valor, la eliminación de la asociación tan pronto como expiren los estados. Si usted encuentra que pegajosa está trabajando para usted, pero parece detenerse
en trabajo hasta la mitad a través de sesiones, puede aumentar este valor para mantener una asociación más.

Puerta de enlace de conmutación

La opción Permitir conmutación puerta de enlace predeterminada, deshabilitado por defecto, permitirá a otras puertas de enlace para llevar
sobre si la puerta de enlace predeterminada a ser inalcanzable. Con múltiples WAN, esto aseguraría que el firewall siempre tiene una puerta de enlace predeterminada para que el tráfico desde el propio servidor de seguridad siempre se puede salir. Hay
Son muchos los casos en que esto no es deseable, sin embargo, como cuando tiene una "WAN" adicional que no está conectado a Internet. En el futuro, esta opción se ampliará para que pueda ser controlado en función de cada puerta de enlace.

Ahorro de energía

Si la opción Usar PowerD está marcada, entonces el powerd daemon está habilitada. Este demonio monitores el sistema y puede reducir la frecuencia de la CPU durante los períodos de baja actividad. Si los procesos necesitan la poder, se incrementará la velocidad de la CPU, según sea necesario. Esta opción reducirá la cantidad de calor una CPU genera, y el consumo de energía también puede disminuir. El comportamiento de esta opción depende en gran medida de el hardware en uso. En algunos casos, la frecuencia de la CPU puede disminuir pero no tienen ningún efecto mensurable sobre
el consumo y / o calor de potencia, donde otros se enfríe y usar menos energía considerablemente. Es considera seguro para funcionar, pero que queda desactivada de forma predeterminada.

El modo de powerd también pueden seleccionarse. Existen cuatro modos, máximo, mínimo, de adaptación, e hiadaptive. Máxima mantiene el rendimiento lo más alto posible. Mínimo mantiene el rendimiento en su nivel más bajo, para evitar el consumo de energía hacia abajo. Adaptativo intenta equilibrar ahorro al disminuir rendimiento cuando el sistema está inactivo y el aumento cuando hay mucha gente. Hiadaptive es similar a adaptativos pero afinado para mantener un alto rendimiento a causa de un mayor consumo de energía. Eleva el CPU frecuencia más rápida y cae más lento.

Aceleración de hardware criptográfico

Hay varias opciones disponibles para acelerar las operaciones de cifrado por hardware. Algunos son integrados en el núcleo, y otros son módulos cargables. Dos de los módulos opcionales son seleccionables aquí: La Geode LX AMD Bloque de Seguridad (glxsb) y AES-NI (Advanced Encryption Standard, Nuevas instrucciones).

La `glxsb` controlador se utiliza principalmente en sistemas embebidos Alix y Soekris. Es un criptográfica acelerador que puede mejorar el rendimiento de ciertos sistemas de cifrado, como AES-128. Esto puede mejorar Rendimiento de VPN y otros subsistemas que pueden utilizar AES-128, tales como SSH. Si selecciona AMD Geode LX Seguridad Block (glxsb), el controlador se carga en el inicio para que el chip acelerador puede ser utilizado. Este controlador puede entrar en conflicto con otras tarjetas aceleradoras criptográficas, como las de Hifn, y tienen prioridad sobre ellos cuando ambos se encuentran. Si usted tiene una tarjeta Hifn, debe desmarcar esta opción para que el `glxsb` dispositivo no está cargado. Si el controlador ya está en uso, debe reiniciar el sistema después establecer esta opción por lo que se puede descargar.

Si se elige AES-NI aceleración basada en CPU (AESNI), a continuación, se carga el módulo kernel cuando salvo y en arranque. Al igual que con `glxsb, AESNI` acelerará ciertos sistemas de cifrado basados en AES. Apoyo a la
AES-NI se encuentra en numerosas y recientes CPUs Intel y algunos procesadores de AMD. El soporte de CPU de Intel se puede encontrar
en Westmere (Excepto i3), Sandy Bridge (Excepto i3, Celeron, Pentium) y Ivy Bridge (todas las variantes tienen) CPUs. Apoyo AMD se limita a su línea Bulldozer partir de este escrito.
Estos conductores enganchan en la FreeBSD `crypto (9)` marco, por lo que muchos aspectos del sistema se utilizará automáticamente la función de los cifrados soportados. Para OpenVPN para usar estos aceleradores, en el Ajustes de VPN, encuentra el campo Crypto Hardware y la pusieron a BSD motor cryptodev.

Hay otros dispositivos criptográficos soportados, tales como `hifn (4)` (Véase el cuadro 3.4, "IPsec Throughput por Cipher - ALIX "), `ubsec (4),` y VIA `candado (4).` En la mayoría de los casos, si un acelerador apoyado se detecta el chip, que se mostrará en el widget Información del sistema.

Seguridad IP

Asociaciones de seguridad

Por defecto, si varias asociaciones de seguridad IPsec (SA) partido, el más reciente es el preferido si se trata de, al menos, 30 segundos de edad. Seleccione esta opción para preferir siempre viejo SAs sobre los nuevos. Esto es rara vez deseable, excepto cuando se trata de algunos de los dispositivos específicos de terceros. Para más información sobre asociaciones de seguridad, consulte
a la sección llamada "Asociación de Seguridad"

IPsec depuración

Si Iniciar racoon en modo de depuración está activada, el demonio de IPsec (mapache) se pondrá en marcha en modo de depuración.
Este modo se producen registros muy detallados, que puede ser útil para localizar problemas con Negociación del túnel IPsec. Si cambia esta opción, cuando se guarda la configuración de esta página, el mapache daemon se reiniciará, que retiren todos los túneles VPN activas.

MSS máxima

La sujeción Habilitar MSS en la opción de tráfico VPN permitirá a MSS de sujeción en TCP fluye a través de VPN. Esto ayuda a superar los problemas con PMTUD en enlaces VPN IPsec. Si deja en blanco, el valor predeterminado es 1400 bytes. Sin esta opción, los paquetes TCP que van a través de IPsec se fragmentaron y propensos a la pérdida Si PMTUD no da lugar a su tamaño se reduce automáticamente.

Horarios

Esta opción controla si los estados se borran cuando una transición de normas planificadas en un estado eso sería bloquear el tráfico. Si está activada, las conexiones se terminan cuando se acabe el tiempo. Si no se controla, conexiones se quedan solos y no serán cerradas automáticamente por el servidor de seguridad.

Monitorización de puerta de enlace

Al utilizar Mutli-WAN, el proceso de seguimiento vaciará estados para una puerta de enlace que va hacia abajo. Este opción anula ese comportamiento al no despejar estados de las conexiones existentes, lo que les deja un tiempo de salida por su cuenta o en algunos casos, continuar incluso si la calidad de una WAN es degradada pero todavía utilizable. Más

información sobre cómo esto afecta a múltiples WAN se puede encontrar en la sección llamada "Killing Estado / Forzado Cambie ".

Sistema optimizables Tab

La ficha Sistema optimizables proporciona un medio para establecer en tiempo de ejecución de FreeBSD tunables del sistema, también conocido como
sysctl OID. En casi todos los casos, estos deben dejarse en sus valores por defecto. Quienes están familiarizados con FreeBSD,
o hacerlo bajo la dirección de un representante desarrollador o soporte, puede que desee ajustar o agregar
valores de esta página para que se establecerá como el sistema se inicia.

> **Nota**
>
> Los valores aquí son distintos de los valores que se consideran cargadora optimizables. Cargador Optimizables están una vez que el sistema se ha arrancado los valores de sólo lectura, ya cambiar los valores deben definirse en `/ Boot / loader.conf.local` o `/ Boot / loader.conf`.

Notificaciones

Comenzando con pfSense 2.0, el servidor de seguridad es ahora capaz de enviar notificaciones remotas utilizando Growl o E-Mail a través de SMTP. Estas notificaciones son las mismas notificaciones que aparecerá en la interfaz gráfica de usuario como
desplazamiento previo aviso en la zona superior de la página. La ubicación exacta y el color de la pantalla varía en función
sobre el tema.

Gruñido

Growl proporciona un método bastante discreto de la entrega de notificaciones de escritorio. Estas notificaciones pop-up en el escritorio y luego ocultar o desaparecer. Growl está incorporado en Mac OSX, y es
disponible con el software adicional en Windows [http://www.growlforwindows.com/gfw/default.aspx]
y FreeBSD / Linux (Gnome [http://the.taoofmac.com/space/projects/DBUSGrowl] o KDE [http://www.pingle.org/2011/04/15/growl-server-kde]).

Registro de Nombre

Este es el nombre del servicio que utilizó para registrarse con el servidor de Growl. Por defecto, este es PHP-Growl. Considere esto como el tipo de notificación, según lo visto por el servidor Growl.

Nombre Notificación

El nombre de la producción de la notificación del sistema. El valor por defecto de alerta gruñido pfSense
puede ser suficiente, pero es posible personalizarla con el nombre de host del servidor de seguridad o cualquier otro valor para hacer
es distinta.

Dirección IP

La dirección IP a la que se enviarán las notificaciones de Growl.

Contraseña

Contraseña requerida por el servidor de Growl para entregar notificaciones.

SMTP E-Mail

Las notificaciones de correo electrónico se entregan por una conexión SMTP directa a un servidor de su elección. El servidor
éstos tendrán que estar configurado para permitir la retransmisión desde el servidor de seguridad, o puede utilizar la configuración
opciones siguientes para proporcionar credenciales para la autenticación SMTP.

Servidor de E-Mail

Coloque el nombre de host o dirección IP del servidor de correo electrónico a través del cual se enviarán las notificaciones.

Puerto SMTP del servidor de E-Mail

El puerto que se utilizará para comunicarse con el servidor SMTP. Los puertos más comunes son 25, 587, y 465. En la mayoría de los casos, 25 de mayo a funcionar. Algunos proveedores de bloquear conexiones salientes al puerto 25, por lo que
utilizando 587 (el puerto de Envío) se prefiere si el servidor lo admite. Puerto 465 es para SMTP seguro (smtps), por lo que el uso de ese puerto es probable que también requieren la comprobación Enable SSL / TLS. SSL / TLS
La autenticación puede ser utilizado en cualquier puerto si el servidor es compatible con SSL / TLS, pero es necesario en el puerto 465.

Desde e-mail

Esta es la dirección de correo electrónico que se utilizará como la fuente de la dirección de correo en la cabecera From. Usted puede
ajústelo a una dirección de correo electrónico que no existe, o la misma que la dirección de correo electrónico de destino, o algún otro
valor. Algunos servidores SMTP intentan validar esta dirección por lo que puede que tenga que utilizar una dirección válida
aquí si la dirección de correo electrónico se enruta a través de un servidor estricto.

Notificación dirección de E-Mail

Esta es la dirección de destino de la notificación por correo electrónico. Puede ser su propia dirección personal, un general
apoyar a cuenta, o cualquier otra dirección que desea recibir las notificaciones.

Notificación por correo electrónico de autenticación nombre de usuario

Si el servidor requiere un nombre de usuario y contraseña para SSL / TLS, puede entrar en el nombre aquí.

Notificación por correo electrónico la contraseña de autenticación

Si el servidor requiere un nombre de usuario y contraseña para SSL / TLS, puede entrar en el contraseña aquí.

Inicio / apagado de sonido

Si el hardware firewall tiene un altavoz de PC, normalmente pfSense reproducirá un sonido cuando termina el arranque, y de nuevo cuando se está iniciando un cierre. Al marcar Desactivar el pitido de arranque / parada, éstos
no se reproducirán sonidos.

Fundamentos del menú de la consola

Algunas de las tareas de configuración y mantenimiento también se pueden realizar desde la consola del sistema. La la consola puede ser alcanzado mediante el uso del teclado y el ratón, consola serie si está habilitado o utilizar incrustado, o mediante el uso de SSH. A continuación se muestra un ejemplo de lo que el menú consola se verá así, pero puede variar ligeramente
dependiendo de la versión y la plataforma.

```
*** Bienvenidos a pfSense 2.1-RELEASE-pfSense (amd64) en pfSense ***

 WAN (wan)         -> Em0          -> V4:  1.2.3.4/24
                                      v6:  FD01 :: 6/64
 LAN (lan)         -> Em1          -> V4:  192.168.28.1/24
                                      v6:  FD05 :: 1/64


 0)  Cerrar sesión (SSH solamente)          8)  Cáscara
 1)  Asigne Interfaces                      9)  pfTop
 2)  Interfaz del dispositivo (s) dirección10)  Registros del filtro
 3)  IP                                    11)  Reiniciar webConfigurator
 4)  Restablecer contraseña webConfigurator12)  pfSense desarrollador Shell
 5)  Restablecer los valores predeterminados13)  Actualización de la consola
 6)  de fábrica                            14)  Desactivar Secure Shell (sshd)
     Reinicie el sistema
     Sistema Halt
```

```
 7) anfitrión Ping                          15) Restaurar configuración reciente
```

Lo que sigue es una descripción general de lo que es posible mediante el uso de la mayoría de estas opciones. Como con otro
Opciones avanzadas, algunas de ellas pueden estar cubiertas con más detalle en otras secciones del libro donde su discusión sería más tópica o relevante.

Asigne Interfaces

Esto reiniciará la tarea de asignación de interfaz, que se trata en detalle en la sección llamada "Asignación de interfaces" y la sección "Asignación manual de interfaces". Puede crear VLAN interfases, reasignar las interfaces existentes, o asignar nuevos.

Interfaz Set (s) dirección IP

Esta opción se puede utilizar de la manera obvia, para establecer la WAN, LAN o OPT dirección IP de la interfaz, pero también hay algunas otras tareas útiles que suceden cuando reiniciar la IP LAN. Para empezar, cuando esto se establece, también tienes la opción de convertir DHCP activado o desactivado, y establecer el rango DHCP IP.

Si ha desactivado la regla anti-bloqueo WebGUI, se le pedirá que vuelva a activarlo. También se pronta 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 responsables a cabo el uso de la WebGUI recuperar el acceso.

Restablecer contraseña webConfigurator

Esta opción restablecerá el nombre de usuario y contraseña WebGUI volver a administración y pfSense, respectivamente.

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 de los paquetes instalados en el sistema operativo. Si usted sospecha que el sistema de
archivos se han dañado o alterado de alguna manera no deseable, lo mejor es hacer una copia de seguridad, y volver a instalar desde el CD u otro medio de instalación. (También posible en el WebGUI en Diagnóstico Valores predeterminados de fábrica)

Reinicie el sistema

Esto hará limpiamente apagar el sistema pfSense y reinicie el sistema operativo (Diagnósticos Reinicie en el WebGUI).

Sistema Halt

Esto hará limpiamente apagar el sistema y, o bien se detenga o se apague, según el soporte de hardware.
No se recomienda para tirar nunca el enchufe de un sistema en funcionamiento, incluso los sistemas embebidos. Vacilante
antes de quitar el poder es siempre la opción más segura si alguna vez necesita para apagar el sistema. En sistemas integrados, tirando del enchufe es menos peligroso, pero si el tiempo es malo también podría ser perjudicial
(Diagnóstico Parada del sistema en el WebGUI).

Anfitrión Ping

Solicita una dirección IP, el cual será enviado tres peticiones de eco ICMP. La salida de la ping- voluntad
se muestra, incluyendo el número de paquetes recibidos, los números de secuencia, los tiempos de respuesta, y el paquete de
porcentaje de pérdida. Si introduce una dirección IPv4 o nombre de host, ping- se ejecutará. Si introduce un IPv6 abordar, ping6 se ejecutará.

Cáscara

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 complejas pueden requerir de trabajo en el shell y algunos tareas de solución de problemas son más fáciles de lograr de aquí, pero siempre hay una posibilidad de causar daños irreparables al sistema si no se manejan con cuidado. La mayoría de los usuarios pfSense puede que nunca tocar la concha, o incluso saber que existe.

Los usuarios veteranos de FreeBSD pueden sentirse ligeramente en casa allí, pero hay muchos comandos que no son presentar en un sistema de pfSense, ya que se eliminan las partes innecesarias del sistema operativo por razones de seguridad
y las limitaciones de tamaño.

La cáscara comenzado de esta manera será tcsh, y la única otra shell disponible es SH. Si bien puede ser posible instalar otros proyectiles para la comodidad de aquellos que están muy familiarizados con el sistema operativo (véase la
sección titulada "Uso de Software de Sistema de Puertos de FreeBSD (paquetes)"), esto no es recomendable o apoyado.

PFtop

PFtop le da una visión en tiempo real de los estados de firewall y la cantidad de datos que se han enviado y recibido. Puede ayudar a determinar qué direcciones IP y las sesiones están utilizando actualmente el ancho de banda, y puede
también ayudar a diagnosticar otros problemas de conexión de red. Vea la sección llamada "Cómo ver con pftop" para más detalles.

Registros del filtro

Utilizando la opción de filtrar los registros, verá las entradas de registro del filtro aparecen en tiempo real en su forma cruda.
Se dispone de información bastante más demostrado por línea de lo que normalmente se ve en la vista de registro de en el WebGUI (Estado Registros del sistema, pestaña Firewall), pero no toda esta información es fácil de leer. firewall

Reiniciar webConfigurator

Reiniciar la webConfigurator se reiniciará el proceso del sistema que ejecuta el WebGUI. En raras ocasiones, ocasiones puede haber un cambio que podría necesitar esto antes de que entren en vigor, o en muy raras de los casos el proceso puede haber dejado por alguna razón, y al reiniciarse se restaurar el acceso.

Si por alguna razón la interfaz gráfica de usuario no responde y esta opción no restaura el acceso, puede ejecutar un reinicio más contundente desde el shell ejecutando:

#killall -9 php; killall -9 lighttpd; / Etc / rc.restart_webgui

pfSense desarrollador Shell (Formerly PHP shell)

El shell Developer, que solía ser conocido como el shell pfSense PHP, es una herramienta muy poderosa que permite ejecutar código PHP en el contexto del sistema en ejecución. Al igual que con la consola normal, es posible también
ser muy peligroso para su uso, y fácil que las cosas van mal. Esto se utiliza principalmente por los desarrolladores y los usuarios experimentados que están íntimamente familiarizados tanto con PHP y la base de código pfSense.

Scripts de reproducción

Hay varios guiones de reproducción para el desarrollador Shell pfSense que pueden automatizar algunas sencillas tareas que podrían ser necesarios para llevar a cabo desde la consola si el GUI es inalcanzable.

Estos scripts se ejecutan desde dentro de la cáscara de este modo:

`shell pfSense:` reproducción scriptname

También se pueden ejecutar desde la línea de comandos:

#pfSsh.php reproducción scriptname

disabledhcpd

Este script elimina toda la configuración DHCP de la configuración del firewall, desactivando efectivamente el servicio DHCP y eliminar por completo todos los rastros de su configuración.

disablerefererchеck

Este script deshabilita la comprobación HTTP_REFERER mencionado en la sección llamada "zonas horarias". Este puede ayudar a obtener acceso a la interfaz gráfica de usuario si la sesión del explorador que está activando esta protección.

enableallowallwan

Este script agrega una regla para permitir que todos los IPv4 e IPv6 a la interfaz WAN. Tenga mucho cuidado con esta opción, que está destinado a ser sólo una medida temporal para acceder a los servicios en la interfaz WAN del servidor de seguridad, tales como la interfaz gráfica de usuario, se pueden añadir reglas más precisas. Una vez que usted tiene un conjunto de reglas
permitir el acceso a la interfaz gráfica de usuario, según sea necesario, retire el permitir que todas las reglas añadidas por este script.

enablesshd

Este script permite SSHD, lo mismo que la opción del menú de la consola o la opción GUI.

externalconfiglocator

Esta secuencia de comandos buscará un archivo config.xml en un dispositivo externo, como una memoria USB, y la voluntad
moverse en su lugar para ser utilizado por el servidor de seguridad.

gitsync

Se trata de una escritura compleja que sincronizará el PHP y otras fuentes de script con los archivos de la pfSense repositorio git. Es muy útil en las instantáneas de desarrollo para recoger los cambios de más reciente comete. Puede ser peligroso usar en otras circunstancias, por lo que sólo utilice este bajo la dirección de un desarrollador con conocimientos o representante de soporte. Si ejecuta el comando sin ningún parámetro, se imprimirá un mensaje de ayuda esbozar su uso. Más información se puede encontrar en el pfSense Doc. Wiki [Http://doc.pfsense.org/index.php/Updating_pfSense_code_between_snapshots].

removepkgconfig

Este script elimina todos los rastros de configuración del paquete de la config.xml correr. Esto puede ser útil si un paquete ha corrompido la configuración o ha dejado de lo contrario los paquetes en un estado incoherente.

restartdhcpd

Este script se detendrá y reiniciar el demonio DHCP.

restartipsec

Este script se detendrá y reiniciará mapache, el demonio de IPsec.

Actualización de la consola

Al utilizar esta opción, es posible actualizar introduciendo una dirección URL completa de una imagen del firmware pfSense, o una a
ruta local completa de una imagen cargada de alguna otra manera. Este método de actualización se trata en más detalle en la sección denominada "Actualización con la consola".

Activar / Desactivar Secure Shell (sshd)

Esta opción le permitirá cambiar el estado del daemon de shell seguro, sshd. Funciona de manera similar a la misma opción en el WebGUI cubierto anteriormente en este capítulo, pero se puede acceder desde la consola.

Restaurar configuración reciente

Esta opción de menú se iniciará una secuencia de comandos que se pueden enumerar y restaurar copias de seguridad de la historia de la configuración.
Esto es similar a acceder a la historia de configuración de la interfaz gráfica de usuario en el Diagnóstico Backup / Restore.
Puede ver los últimos archivos de configuración, junto con una indicación de la hora y la descripción del cambio realizados en la configuración, el usuario y el IP que hizo el cambio, y la revisión de configuración. Esto es especialmente
útil si un error de configuración reciente eliminado accidentalmente el acceso a la interfaz gráfica de usuario.

Mueva el archivo de configuración de dispositivo extraíble

Si desea mantener la configuración del sistema de almacenamiento extraíble, como una unidad flash USB, esta opción se puede utilizar para reubicar el archivo de configuración. Una vez utilizada, asegúrese de asegurarse de los medios de comunicación
es accesible en tiempo de arranque de modo que pueda volver a cargarse. Esto no es un método normal de copias de seguridad de la
configuración. Para información sobre cómo realizar copias de seguridad, consulte el Capítulo 9, Copia de seguridad y restauración.

Sincronización de tiempo

Cuestiones de tiempo y el reloj no son tan poco comunes al configurar cualquier sistema, pero pueden ser importantes para hacerlo bien en los routers, especialmente si se están realizando todo tipo de tareas que implican la validación certificados como parte de una infraestructura PKI. Obtención de la sincronización de tiempo para que funcione correctamente es también un
necesidad absoluta en sistemas embebidos, algunos de los cuales no tienen una batería de a bordo para preservar su fecha y ajustes de hora cuando se desconecta la alimentación. Puede haber algunas peculiaridades para conseguir no sólo una
fecha y la hora correcta en el sistema, y mantener de esa manera, sino también en asegurarse de que el tiempo de zona se refleja correctamente.
No sólo va a conseguir todo esto en la línea de ayuda con las tareas críticas del sistema, sino que también asegura que su registro
archivos estén debidamente indicación de la hora, que puede ser de gran ayuda en la solución de problemas, el mantenimiento de registros, y en general
gestión del sistema.

Husos horarios

Usted verá un comportamiento inesperado si selecciona uno de la hora GMT compensar desplazamientos zones.The son el
contrario de lo que cabría esperar que se basan en sus nombres. Por ejemplo, la zona horaria GMT-5 en realidad es GMT + 5 horas. Esto viene de la base de datos TZ que FreeBSD y muchos otros Unix y sistemas operativos tipo Unix utilizan.

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

> Estas zonas se incluyen la compatibilidad con antiguos sistemas UNIX. Eres más probabilidades de convencer a los desarrolladores de bases de datos TZ a caer por completo de usted va a conseguir que cambien las definiciones. En cualquier caso, FreeBSD seguirá el práctica de la base de datos TZ.

En este momento, se recomienda utilizar zonas horarias sólo con nombre y no el GMT zonas offset.

Al compás de Problemas

Puede ejecutar en el hardware que tiene problemas significativos de mantenimiento de tiempo. Todos los relojes de PC se deriva de
en cierta medida, pero usted puede encontrar un poco de hardware que se deriva tanto como un minuto por cada par minutos que pasan y consiguen la sincronización de forma rápida. NTP está diseñado para actualizar periódicamente el sistema

tiempo para dar cuenta de la deriva normal, los relojes no pueden razonablemente correctas que se desplazan de manera significativa. Es
muy poco comunes, pero si usted encuentra que, a continuación se describirá las cosas que normalmente fijan esto.

Hay cuatro cosas que debe comprobar si se encuentra con problemas significativos de hardware con el tiempo de mantenimiento.

Network Time Protocol

Por defecto, pfSense está configurado para sincronizar su tiempo utilizando el Protocolo de Tiempo de Red ntp.org (NTP) del grupo de servidores. Esto asegura una fecha y hora exacta en el sistema, y se adaptará a
la deriva de reloj normal. Si la fecha y hora del sistema son incorrectos, garantizar la sincronización NTP es funcionamiento. El problema más común que impide la sincronización es la falta de DNS adecuado configuración en el servidor de seguridad. Si el firewall no puede resolver los nombres de host, la sincronización NTP fallar. Los resultados de la sincronización se muestran en el arranque en el registro del sistema y el estado de la NTP

la sincronización del reloj se puede ver en estado NTP.

Actualizaciones de BIOS

He visto a hardware antiguo que funcionó muy bien durante años en Windows encontrará grandes problemas de cronometraje
una vez redistribuido en FreeBSD (y por consecuencia, pfSense). Los sistemas estaban corriendo un BIOS Versión varias revisiones actualizado. Una de las revisiones abordaron una cuestión de cronometraje que aparentemente Nunca afectadas de Windows por alguna razón. La aplicación de la actualización de la BIOS solucionó el problema. Lo primero que
usted debe comprobar es asegurarse de que usted tiene la última BIOS de su sistema.

Configuración PNP OS en BIOS

Me he encontrado con otro hardware que había tiempo de mantenimiento dificultades en FreeBSD y pfSense menos PNP OS en el BIOS se establece en "No". Si su BIOS no tiene una opción de configuración PNP OS,
buscar una configuración de "OS" y ponerlo en "Otros".

Desactivar ACPI

Algunos fabricantes de BIOS han producido ACPI (Advanced Configuration and Power Interface) implementaciones que son errores en el mejor y en el peor, peligroso. En más de una ocasión que tenemos sistemas encontrados que no arranque o ejecutar correctamente a menos que el soporte ACPI fue desactivado en el BIOS y / o en el sistema operativo.

La mejor manera de desactivar ACPI en el BIOS. Si no hay una opción de BIOS para desactivar ACPI, entonces usted puede tratar de correr sin ella de dos maneras diferentes. El primer método, temporal es desactivar ACPI en el indicador de arranque. Al principio del proceso de arranque, aparecerá un menú con varias opciones, una de ellas es Boot pfSense con ACPI deshabilitado. Al elegir este, ACPI estará deshabilitado para esta sola bota. Si el comportamiento mejora, entonces usted debe desactivar ACPI de forma permanente.

Para desactivar permanentemente ACPI, debe añadir un ajuste a la `/ boot / device.hints` presentar. Usted puede hacer esto mediante la navegación a Diagnósticos Editar archivo, escriba `/ boot / device.hints` y luego haga clic en Cargar.
Agregue una nueva línea al final y luego escriba:

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

Luego haga clic en Guardar.

Para una forma alternativa de hacer esto, a partir de diagnósticos Comandos o desde un shell, escriba lo siguiente:

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

Nota

La `/ boot / device.hints` archivo se sobrescribirá durante una actualización. Tenga en cuenta que tendrá que repetir este cambio después de realizar una actualización de firmware.

Ajuste timeCounter Hardware Configuración

En muy pocos sistemas, es posible que el valor sysctl kern.timecounter.hardware que ser cambiado para corregir un reloj inexacta. Esto es conocido por ser un problema en VMware ESX 5 en combinación con basado amd64-an pfSense imagen (o cualquier imagen amd64 FreeBSD.). En estos sistemas, utilizando el timeCounter defecto, la reloj se detendrá tictac, causando problemas con la encriptación, VPNs, y servicios en general. Por otra sistemas, el reloj puede sesgar por grandes cantidades con el timeCounter mal. Para cambiar el timecouter

temporalmente, vaya a Diagnósticos Mando y ejecutar lo siguiente:

#sysctl-w = kern.timecounter.hardware i8254

Esto hará que el sistema utilice el chip timeCounter i8254, que normalmente mantiene buen momento, pero podrá no puede ser tan rápido como otros métodos. Las otras opciones timeCounter se explicarán a continuación.

Si el sistema mantiene la hora correcta después de hacer este cambio, es necesario hacer este cambio permanente. El cambio realizado previamente no sobrevivirá un reinicio. Vaya a Sistema Avanzado, vaya a la Ficha Sistema optimizables, y añadir una nueva entrada y ajustar la sintonizable para kern.timecounter.hardware y el Valor de i8254.

Haga clic en Guardar y, a continuación, que el ajuste se debe leer de nuevo en el siguiente arranque.
Dependiendo de la plataforma y el hardware, también puede haber otras timecounters apetitosas. Para obtener una lista de timecounters disponibles se encuentran en el sistema, ejecute el siguiente comando:

#sysctl kern.timecounter.choice

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

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

A continuación, podría tratar de probar cualquiera de estos cuatro valores para el ajuste kern.timecounter.hardware sysctl. En términos de "calidad" en este listado, cuanto mayor sea el número, mejor, pero el uso real varía dependiendo de de sistema a sistema. El TSC es un contador en la CPU, pero está ligada a la velocidad de reloj y no es legible por otras CPU. Esto hace que su uso en sistemas SMP imposible, y en aquellos con variable CPUs velocidad. El i8254 es un chip de reloj que se encuentra en la mayoría del hardware, lo que tiende a ser más seguro, pero puede tener
algunos inconvenientes de rendimiento. La contra-ACPI seguro, si lo admite correctamente en el hardware disponible, es una buena opción, ya que no sufre de las limitaciones de rendimiento de i8254, pero en la práctica su precisión y velocidad varían ampliamente dependiendo de la aplicación. Esto y más información sobre FreeBSD Timecounters se puede encontrar en el documento Timecounters: eficiente y precisa de cronometraje en núcleos SMP [http://phk.freebsd.dk/pubs/timecounter.pdf] Poul-Henning Kamp del FreeBSD Proyecto.

Ajuste la frecuencia del temporizador Kernel

En algunos casos, también puede ser necesario ajustar la frecuencia del temporizador del núcleo, o kern.hz núcleo sintonizable.
Esto es especialmente cierto en entornos virtualizados. El valor por defecto es 1000, pero en algunos casos 100, 50, o incluso 10 habrá un mejor valor en función del sistema. Cuando pfSense se instala en VMware, que detecta y configura automáticamente el 100, que debería funcionar bien en casi todos los casos con VMware productos. Al igual que con el establecimiento de la timeCounter anteriormente, para ajustar esta configuración se agrega una línea para `/ Boot /` `loader.conf` con el nuevo valor:
`kern.hz = 100`

Tiempo de sincronización GPS

Para ayudar en el mantenimiento de un reloj de precisión, se añadió la sincronización de tiempo GPS en pfSense 2.1. Cierto
dispositivos GPS de serie o USB son compatibles, y en combinación con los servidores de tiempo externo, pueden ayudar a
mantener el reloj de precisión. Para obtener más detalles, consulte la sección titulada "NTPD".

Solución de problemas

El Asistente para la instalación y las tareas de configuración relacionados funcionarán para la mayoría, pero puede haber algunas cuestiones
obtener paquetes a fluir normalmente en sus direcciones destinados. Algunos de estos problemas pueden ser exclusivos de
su configuración particular, pero se puede trabajar a través con un poco de solución de problemas básicos.

No se puede acceder WebGUI de LAN

Lo primero que hay que comprobar si no se puede acceder a la WebGUI de la LAN es el cableado. Si usted es conectar directamente un PC cliente a una interfaz de red en un sistema de pfSense, es posible que tenga un cruce cable a menos que una o las dos tarjetas de red compatible con Auto-MDIX.

Una vez que esté seguro de que hay una luz de enlace en ambas tarjetas de red del cliente y la interfaz LAN pfSense, el siguiente paso es comprobar la configuración de TCP / IP en el PC desde el que está intentando conectar.
Si el servidor DHCP está habilitado en el sistema de pfSense, ya que será por defecto, asegurarse de que el cliente También se establece para DHCP. Si DHCP está desactivado en el sistema de pfSense, tendrá que codificar una IP abordar en el cliente que reside en la misma subred que la dirección IP de LAN del sistema de pfSense, con el misma máscara de subred, y el uso de la dirección IP LAN pfSense como su puerta de enlace y servidor DNS.

Si la configuración de cableado y de red son correctas, usted debe poder hacer ping a la IP LAN del pfSense sistema de la PC del cliente. Si puede hacer ping, pero aún no puede acceder a la WebGUI, hay
todavía un poco más de cosas para probar. En primer lugar, si el error que usted recibe en el PC cliente es una conexión reajustar
o fracaso, entonces o bien el demonio del servidor que ejecuta el WebGUI no se está ejecutando, o usted está tratando de acceder a él desde el puerto equivocado. Si el error que usted recibe es en lugar de una conexión tiempo de espera, que los puntos más
hacia una regla de firewall.
Si recibe un restablecimiento de la conexión, es posible que primero se intenta reiniciar el proceso del servidor WebGUI del
consola del sistema, por lo general la opción 11. En caso de que no ayuda, inicie un shell de la consola (opción 8), y escriba:

```
#sockstat | grep lighttpd
```

Eso debería devolver una lista de todos los procesos que se ejecutan lighttpd, y el puerto sobre el que se está escuchando, de este modo:

```
raíz      lighttpd    33098 11 tcp4     *: 443                *: *
raíz      lighttpd    33098 12 tcp6     *: 443                *: *
raíz      lighttpd    33098 13 tcp4     *: 80                 *: *
```

En esa salida, se muestra que el proceso está escuchando en el puerto 443 de cada interfaz en IPv4 e IPv6, así como el puerto 80 en IPv4 para la redirección, sino que pueden variar según la configuración. Pruebe la conexión con el pfSense LAN IP utilizando directamente ese puerto, y con HTTP y HTTPS. Por ejemplo, si su IP LAN era 192.168.1.1, y se escucha en el puerto 82, trate de http://192.168.1.1:82 y https://192.168.1.1:82.

Si recibe un tiempo de espera de conexión, consulte la sección "¿Qué hacer si usted consigue acceder a WebGUI ". Con una conexión de red configurada correctamente, esto no debería ocurrir, y que el artículo ofrece formas de solucionar los problemas de reglas de firewall.

También es una buena idea para corroborar que la WAN y LAN no están en la misma subred. Si WAN es ajustado para DHCP y se enchufa en detrás de otro enrutador NAT, sino que también puede estar utilizando 192.168.1.1. Si el
misma subred está presente en WAN y LAN, resultados impredecibles pueden ocurrir, incluyendo no poder para enrutar el tráfico o acceder a la WebGUI. En caso de duda, desconecte el cable WAN, reinicie el pfSense router y vuelva a intentarlo.

Sin Internet desde la LAN

Si usted es capaz de llegar a la WebGUI, pero no por la Internet, hay varias cosas a considerar. La Interfaz WAN no esté configurado correctamente, la resolución DNS podría no estar funcionando, podría haber un problema con las reglas del firewall, las reglas de NAT, o incluso algo tan simple como una cuestión de puerta de enlace local.

WAN Interface Cuestiones

Primero, verifique la interfaz WAN para asegurarse de que pfSense ve como operacional. Vaya a Estado Interfaces y mirar el estado de la interfaz WAN allí. El estado debe mostrar como "arriba". Si muestra

abajo, revise el cableado y la configuración de WAN bajo Interfaces WAN. Si está usando PPPoE o PPTP para el tipo de WAN, hay una línea de estado adicional que indica si la conexión PPP está activa. Si no funciona, intente pulsar el botón Conectar. Si eso no funciona, vuelva a comprobar todos los ajustes en

Interfaces WAN, cheque o reiniciar el equipo ISP (módem de cable / DSL, etc), y tal vez consultar con su ISP para obtener ayuda en relación con los ajustes que debe utilizar allí.

DNS Resolución Cuestiones

Dentro de la WebGUI, vaya a Diagnósticos Ping, y entrar en su dirección de puerta de enlace de su ISP si usted sabe

ella. Se cotiza en Estado Interfaces para la interfaz WAN. Si usted no sabe la puerta de entrada, puedes probar alguna otra dirección conocida válida como 4.2.2.2. Si usted es capaz de hacer ping a esa dirección, luego repita la misma prueba ping desde el PC cliente. Abra un símbolo del sistema o en la ventana de terminal, y ping esa misma dirección IP. Si puede hacer ping la dirección IP, a continuación, intente hacer ping a un sitio por el nombre tan
como www.google.com. Inténtelo del pfSense WebGUI y desde el PC cliente. Si la prueba de ping IP funciona, pero no puede hacer ping por nombre, entonces hay un problema con la resolución DNS. (Véase la Figura 10.20,
"Resolución de 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 Configuración general, y en Estado Interfaces. Consulte con ping para verificar que estén accesibles. Si se puede llegar a la dirección de puerta de enlace de su ISP, pero no sus servidores DNS, puede ser recomendable llamar su ISP, revisa con esos valores. Si los servidores DNS se obtienen a través de DHCP o PPPoE y no se puede contactar con ellos, es posible que también tenga que ponerse en contacto con su proveedor de Internet con respecto a ese tema. Si todo lo demás falla,
es posible que desee considerar el uso de OpenDNS [http://www.opendns.com/] (ver la sección llamada "Free Filtrado de contenido con OpenDNS ") servidores de nombres de su enrutador pfSense lugar de las previstas por su ISP.

Si el DNS funciona desde el router pfSense, pero no desde un PC cliente, podría ser el Forwarder DNS configuración en el sistema pfSense, la configuración del cliente, o de reglas de firewall. Fuera de la caja, pfSense tiene un reenviador DNS que se encargará de las consultas DNS para los clientes detrás del enrutador. Si sus PCs clientes están configuradas con DHCP, que va a obtener la dirección IP de la interfaz del router al que pfSense están conectados como un servidor DNS, a menos que especifique una anulación. Por ejemplo, si un PC está en la LAN lado, y la dirección IP de LAN del sistema pfSense es 192.168.1.1, entonces el servidor DNS del cliente debe también ser 192.168.1.1. Si ha desactivado la Forwarder DNS, es posible que también necesite ajustar el DNS

servidores que se asignan a los clientes DHCP en Servicios DHCP Server. Normalmente, cuando el DNS Forwarder está desactivado, los servidores DNS del sistema se asignan directamente a los clientes, pero si eso no es el caso en la práctica para su configuración, defina aquí. Si el PC cliente no está configurado para DHCP, asegurarse de que tiene los servidores DNS apropiados establecidos: o bien la dirección IP de LAN del sistema pfSense o lo que sea
servidores internos o externos de DNS que le gustaría para que se utilice.

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

Gateway Client Issue

Para que el sistema de pfSense tendido apropiado para el tráfico de Internet para sus PCs clientes, debe ser su puerta de enlace. Si el PC cliente se configuran mediante el servidor DHCP de pfSense, este se ajustará automáticamente. Sin embargo, si los clientes reciben información de DHCP de un servidor DHCP alternativo o sus direcciones IP se han introducido manualmente, vuelva a comprobar que su puerta de entrada se establece para la dirección IP de la interfaz
al que se conectan en el sistema pfSense. Por ejemplo, si los clientes están en el lado pfSense LAN,

y la dirección IP para la interfaz LAN de pfSense es 192.168.1.1, a continuación, la dirección de puerta de enlace de un cliente debe
se establece en 192.168.1.1.

Firewall Rule Cuestiones

Si el defecto "LAN a ninguna" regla ha sido cambiado o retirado de la red LAN de la interfaz, el tráfico tratando de acceder a Internet desde los ordenadores clientes a través del router pfSense puede estar bloqueado. Esto debería ser
fácilmente confirmado por la navegación de Estado Registros del sistema, y mirando a la pestaña Firewall. Si hay entradas allí que muestran bloqueado las conexiones de LAN PC que intentan llegar a los hosts de Internet, revisar su

Conjunto de reglas a Firewall LAN Reglas, luego en la pestaña LAN y realice los ajustes necesarios para permitir que tráfico. Consulte el Capítulo 10, Firewall para obtener información más detallada sobre la edición o la creación adicional normas.

Si funciona desde el lado de la LAN, pero no de una interfaz OPT, asegúrese de tener las reglas en su lugar para permitir el tráfico para salir. No hay ninguna regla que se crea de forma predeterminada en las interfaces OPT.

NAT Regla Cuestiones

Si las reglas de NAT de salida han sido cambiados de los valores predeterminados, también puede ser posible que el tráfico
tratar de llegar a la Internet no tiene NAT aplica correctamente. Vaya a Cortafuego NAT,
e ir a la pestaña de salida. A menos que usted esté seguro de que lo que necesita es definido en manual, cambie el ajuste a Generación automática de reglas NAT saliente (pasarela IPSec) y luego tratar de acceder a Internet desde un PC cliente nuevo. Si eso no ayuda un PC de la LAN para salir, entonces el problema es probable que en otros lugares.

Si usted tiene este conjunto en Manual Outbound generación regla NAT (Advanced Outbound NAT (AON)), y funciona de LAN, pero no de una interfaz OPT, tendrá que configurar manualmente una regla que partidos tráfico que viene de allí. Mira la regla existente para LAN y ajustarlo en consecuencia, o consulte el capítulo NAT para más información sobre cómo crear reglas de NAT salientes. Lo mismo se aplica para los el tráfico proveniente de los usuarios de VPN: PPTP, OpenVPN, IPsec, etc Si estos usuarios necesitan acceder a Internet a través de este router pfSense, necesitarán reglas de NAT de salida para sus subredes. Vea la sección llamada "NAT de salida" para obtener más información.

Archivo de configuración XML de pfSense

tiendas pfSense todos de su configuración en un archivo de configuración en formato XML. Todos los ajustes del sistema - incluyendo
ajustes de paquetes - se llevan a cabo en este archivo. Todos los demás archivos de configuración de los servicios del sistema
y el comportamiento se generan de forma dinámica en tiempo de ejecución basado en los ajustes celebradas en el XML archivo de configuración.
Algunas personas que están familiarizadas con FreeBSD y sistemas operativos relacionados han encontrado esto de la manera difícil, cuando sus cambios en algunos archivos de configuración del sistema se sobrescriben varias veces por el sistema antes de que llegaron a comprender que pfSense maneja todo automáticamente.

La mayoría de las personas nunca necesitan saber dónde se encuentra el archivo de configuración, pero para referencia es en `/ Cf / conf / config.xml.` Típicamente, `/ Conf /` es un enlace simbólico `/ Cf / conf,` por lo que también puede ser
accesible directamente desde `/ Conf / config.xml,` pero esto varía según la plataforma y el diseño del sistema de archivos.

Edición manual de la configuración

Algunas opciones de configuración están disponibles únicamente editando manualmente el archivo de configuración, aunque
esto no es necesario en la gran mayoría de las implementaciones. Algunas de estas opciones se tratan en otra partes de este libro.

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

Si está familiarizado con el vi editor, y usted es muy cuidadoso, la viconfig comando editar
la configuración en ejecución en vivo, y cuando haya guardado y concluya, eliminará la configuración almacenada en caché
desde `/ Tmp / config.cache` y luego los cambios deben ser visibles en la interfaz gráfica de usuario, y estarán activos
próxima vez que el servicio correspondiente a la parte de edición de la configuración se reinicia / reloaded.

¿Qué hacer si usted consigue acceder a la WebGUI

Bajo ciertas circunstancias, usted puede encontrarse bloqueado fuera de la WebGUI, sobre todo debido al piloto de error. No tenga miedo de que si esto le sucede a usted; hay una serie de maneras de volver pulg Algunos métodos es un poco difícil, pero siempre debería ser posible recuperar el acceso. Los peores escenarios requieren acceso físico. Como usted recordará desde principios de este capítulo mencionamos que cualquier persona con discapacidad física
acceso puede pasar por alto las medidas de seguridad y ahora verás lo fácil que es.

He olvidado la contraseña

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

He olvidado la contraseña con una consola Bloqueado

Si la consola está protegido con contraseña y no conoce la contraseña, no todo está perdido. Tomará un pareja se reinicia de lograr, pero se puede arreglar con acceso físico a la consola:

• Reinicie el cuadro de pfSense

• Seleccione la opción 5 (modo de usuario único) desde el menú del gestor (el que tiene el logotipo de pfSense ASCII)

• Pulse Intro cuando se le solicite para iniciar / bin / sh

• Volver a montar todas las particiones como regrabable:

```
#/ Sbin / mount-a-t ufs
```

• Ejecute el comando integrado de restablecimiento de contraseña:

```
#/ Etc / rc.initial.password
```

• Siga las instrucciones para restablecer la contraseña

• Reboot

Ahora debería ser capaz de acceder al sistema con el nombre de usuario y la contraseña de forma predeterminada administración y
pfSense, respectivamente.

HTTP vs Confusión HTTPS

Asegúrese de que está conectando con el protocolo adecuado, HTTP o HTTPS. Si uno no funciona, trate de la otra. Usted puede encontrar que usted necesita para tratar el protocolo opuesto en el puerto de los demás, así:

•http://pfsensebox:443

•https://pfsensebox:80

Si tiene que reiniciar desde la consola, reinicie el IP LAN, introduzca la misma IP, y se le pedirá que restablecer el WebGUI volver a HTTP.

Acceso Bloqueado con reglas de firewall

Si ha bloqueado a sí mismo fuera 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 deshabilite la regla anti-bloqueo que mantiene el acceso a la Webgui de esa interfaz.

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

Remotamente Circumvent Firewall de bloqueo con las Reglas

Hay algunas maneras que usted puede manipular el comportamiento del cortafuegos en la cáscara que puede llevarle de vuelta pulg
Las siguientes tácticas se enumeran en orden de lo fácil que es y cuánto impacto que tienen en la sistema que ejecuta.

Agregar una regla con EasyRule

La forma más fácil, suponiendo que conoce la dirección IP que está intentando acceder al servidor de seguridad de, es utilizar el easyrule comando de shell para agregar una nueva regla de firewall para conseguir que en la interfaz gráfica de usuario. En el siguiente
ejemplo, se permitirá el acceso a la WAN interfaz, desde x.x.x.x (La IP del cliente) para y.y.y.y (Presumiblemente la IP WAN) en el puerto tcp 443.

```
#pase easyrule wan tcp x.x.x.x y.y.y.y 443
```

Una vez que la regla se ha añadido, a continuación, debería ser capaz de acceder a la interfaz gráfica de usuario.

Agregar una regla de permitir que todos WAN de la concha

Otra táctica consiste en activar temporalmente una regla de "permitir todo" en la WAN a dejarte entrar por la ejecución de este
comando en la shell:

```
#pfSsh.php reproducción enableallowallwan
```

Una vez que haya fijado las reglas y recuperado el acceso, eliminar el "permitir que todo dominio" en la WAN.

Deshabilitar el Firewall

Usted podría (muy temporalmente) deshabilitar las reglas del firewall mediante la consola. Puede utilizar la física consola, o si usted es todavía capaz de obtener a través de SSH, eso también funciona. Desde la consola, utilice la opción 8 para iniciar un shell y escriba:

```
#pfctl-d
```

Eso desactive el firewall, incluyendo todas las funciones de NAT. A continuación, debería ser capaz de entrar en la WebGUI desde cualquier lugar, por lo menos durante unos minutos, o hasta que se guarda algo en la WebGUI que hace que el conjunto de reglas que se va a cargar (que es casi todas las páginas). Una vez que haya ajustado las reglas y recuperado el acceso necesario, gire el firewall de nuevo escribiendo:

```
#pfctl-e
```

Manual Ruleset Edición

Alternativamente, el conjunto de reglas cargado se retiene en `/ Tmp / rules.debug.` Si está familiarizado con el conjunto de reglas de PF
sintaxis, puede editar ese para arreglar su problema de conectividad y recargar esas reglas de este modo:

```
#pfctl-f / tmp / rules.debug
```

Después de volver a meterse en el WebGUI con esa solución temporal, Haces el trabajo que hay que hacer en el WebGUI para hacer la solución permanente. Al guardar las reglas en el WebGUI, que conjunto de reglas temporales se sobrescribirá.

Remotamente Circumvent Firewall Bloqueo con SSH Tunneling

Si usted bloqueado el acceso a la WebGUI de forma remota, pero usted todavía tiene acceso a SSH, entonces hay una relativamente fácil manera de obtener en: SSH Tunneling.

Si el WebGUI es el puerto 80, configurado su cliente para reenviar el puerto local 80 (o 8080, o lo que sea) a distancia puerto "localhost: 80", y luego dirija su navegador a http://localhost:80 o cualquier puerto local
que eligió. Si su WebGUI es en otro puerto, utilice en su lugar. Si está utilizando HTTPS usted aún necesitará utilizar HTTPS para acceder a la WebGUI esta manera.

Figura 5.16. La creación de un puerto 80 SSH túnel en PuTTY

Rellene las opciones como se muestra en la Figura 5.16, "Configuración de un puerto 80 SSH túnel en PuTTY", a continuación, haga clic en
Agregar. Cuando se conecte y ingrese su nombre de usuario / contraseña, puedes acceder a la WebGUI de utilizar su puerto local redirigido.

Bloqueado debido a un error de configuración de Squid

Si configura accidentalmente Squid para utilizar el mismo puerto que el WebGUI, y luego no se puede volver a que arreglar la configuración, es posible que necesite arreglarlos con el siguiente procedimiento.

• Conéctese a la consola del sistema pfSense con SSH o el acceso físico

• Iniciar un shell, la opción 8 de la consola.

• Terminar el proceso de calamar de este modo:

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

Si eso no funciona, trate de esta manera:

#killall -9 calamar

o

#squid-k apagado

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 los calamares pueden ser
reiniciado automáticamente.

Pensamientos configuración final

Hay millones de maneras de configurar un sistema de pfSense, y por lo tanto 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 algunos
de las opciones de configuración generales. Los próximos capítulos entran en detalles sobre las capacidades individuales del software. Como hemos mencionado al final del capítulo introductorio, hay varios otros
vías para obtener ayuda. Si ha intentado todas las sugerencias aquí y todavía no son capaces de hacer pfSense funciona como se espera, hay foros, IRC, listas de correo, las búsquedas de Google y Comercial Apoyo. Usted es libre de tomar el enfoque de bricolaje, o si le gustaría profesionales para cuidar de la configuración para usted, el equipo de soporte comercial es más que capaz. Para los enlaces a la línea medios de soporte, consulte la sección "Obtención de ayuda".

Capítulo 6. Tipos de interfaz y Configuración

Muchos tipos diferentes de interfaces de red se pueden usar con pfSense, ya sea usando interfaces físicas directamente o por capas de otros protocolos en la parte superior como PPP o VLAN. En pfSense 1.2.3 esta era limitado principalmente a la utilización de las interfaces de sí mismos, VLAN, o PPPoE / PPTP. En pfSense 2.1, muchos se admiten nuevos tipos de interfaces. La mayoría de ellos fueron apoyados en pfSense 2.0.x, con los tipos de IPv6 siendo la mayor adición de pfSense 2.1.

Asignaciones de interfaz y la creación de nuevas interfaces virtuales se manejan bajo Interfaces (Asignar).

Interfaces físicas y virtuales

La mayoría de las interfaces discutidas en este capítulo se pueden asignar como WAN, LAN, o una interfaz OPT bajo Interfaces (Asignar). Se pueden utilizar diferentes combinaciones de opciones para utilizar las interfaces de sí mismos, o el uso de múltiples redes y protocolos en una interfaz única, o vincular múltiples interfaces juntas en una capacidad mayor o interfaz virtual redundante. Todas las interfaces definidos actualmente se enumeran bajo

Interfaces (Asignar). De forma predeterminada, esto es sólo las interfaces físicas, pero el uso de las otras fichas bajo

Interfaces (Asignar) se pueden crear interfaces virtuales y luego asignarlos.

pfSense 1.2.3 te limita a sólo DHCP o estática en LAN e interfaces OPT, pero con 2.0 y superiores, se puede utilizar cualquier tipo de interfaz como cualquier interfaz en pfSense. Todas las interfaces son tratados por igual; Usted puede cambiar el nombre de las interfaces WAN y LAN a otros nombres y utilizarlos en otras formas.

En esta sección, los diferentes tipos de interfaces que se pueden crear, asignar, y administrados serán cubierta.

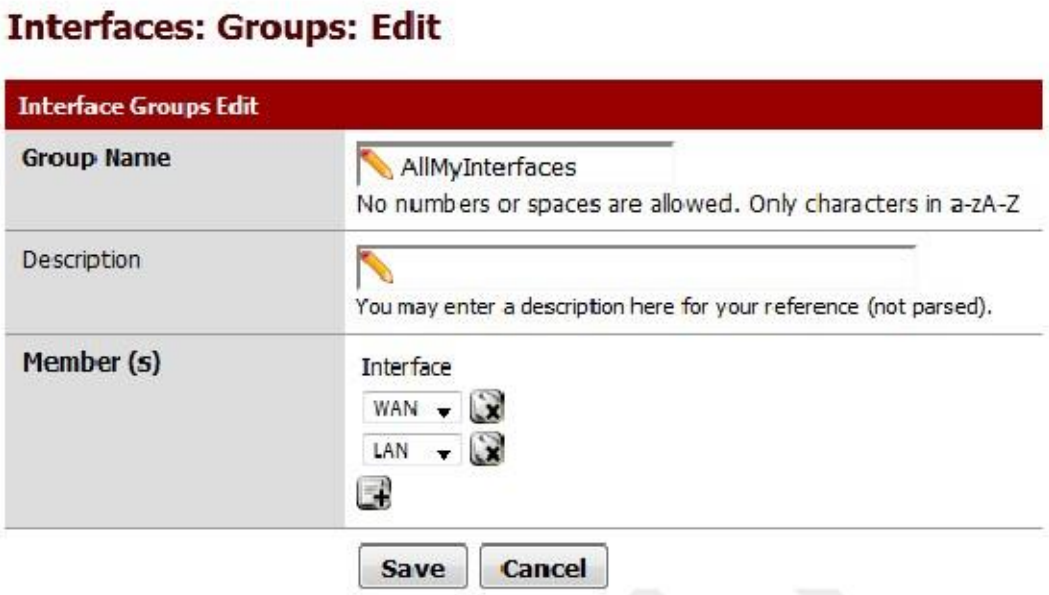
De grupos de interfaces

A diferencia de las otras interfaces de este capítulo, un grupo de interfaz no es un tipo de interfaz que puede ser asignado. De grupos de interfaces se utilizan para aplicar las reglas del cortafuegos o NAT a un conjunto de interfaces de un común tab. Si este concepto es familiar, considerar cómo las reglas de firewall para PPTP y OpenVPN trabajo. Hay son múltiples interfaces en el sistema operativo subyacente, pero las reglas para todos ellos se gestionan en una sola pestaña para cada tipo de VPN. Si va a haber muchas interfaces de una función similar que necesitan prácticamente idénticos reglas, un grupo de interfaz pueden ser creados para añadir reglas para todas las interfaces al mismo tiempo. La las interfaces todavía pueden tener sus propias reglas individuales, que se procesan antes de las reglas del grupo.

Para crear un grupo de interfaces, navegue hasta Interfaces (Asignar), e ir a la pestaña de grupos de interfaces.

Haga clic para crear un nuevo grupo. A continuación, introduzca un nombre de grupo. El Nombre de grupo sólo puede contener superior y minúsculas, no hay números, espacios o caracteres especiales. Para añadir interfaces de miembros a la grupo, haga clic en a continuación, seleccione la interfaz de la lista desplegable. Para eliminar una interfaz de la grupo, haga clic en Cuando termine de editar el grupo, haga clic en Guardar.

Figura 6.1. Agregar grupo Interface



Grupos de interfaz obtienen su propia pestaña en Cortafuegos Reglamento, cuando se gestionan sus reglas.

Figura 6.2. Interface Group Firewall Reglas Tab

Sin hilos

La ficha Wireless Interfaces bajo (Asignar) se utiliza para crear puntos de acceso virtuales adicionales (VAP) interfaces. El uso de productos antimicrobianos permite múltiples redes con SSID inalámbricas únicos que se ejecuten fuera de un solo
tarjeta, si esa función es compatible con el hardware y el controlador en uso. Se crea un VAP aquí, entonces asignado en la ficha asignaciones de interfaz. Información en profundidad acerca de esta característica se puede encontrar en el capítulo 22,
Wireless.

VLANs

VLAN etiquetada interfases o 802.1Q etiquetado de interfaces, se gestionan en la ficha VLAN bajo Interfaces (Asignar). Éstos permiten que el sistema para abordar el tráfico etiquetados por un interruptor que pueda 802.1Q por separado como
si cada etiqueta fuera su propia interfaz. Se crea una VLAN aquí, entonces asignado a las tareas de interfaz tab. Información en profundidad acerca de esta característica se puede encontrar en el capítulo 14, LAN virtuales (VLAN).

QinQs

La ficha QinQs bajo Interfaces (Asignar) permite la creación de una interfaz compatible con 802.1ad que es también conocido como Stacked VLANs. Esta característica permite que varias etiquetas VLAN a estar contenidos en un solo paquete.
Esto puede ayudar a transportar el tráfico de VLAN etiquetadas para otras redes a través de una red intermedia utilizando una etiqueta diferente o solapada. Información en profundidad acerca de esta característica se puede encontrar en el capítulo 14, Virtual
LAN (VLAN).

PPP

Hay cuatro tipos de interfaces PPP en pfSense 2.0 y posteriores: normal PPP para 3G/4G y módem dispositivos, PPPoE para ADSL o conexiones similares, y PPTP y L2TP para ciertos ISPs específicos que requieran para la autenticación en algunas regiones. En la mayoría de los casos éstos se gestionan desde la interfaz

ajustes directamente, pero también pueden ser editados bajo Interfaces (Asignar) en la pestaña PPP.

Multi-Link PPP (MLPPP)

Aparte de la configuración de opciones avanzadas, una de las razones para la edición de las interfaces PPP aquí es activo multi-
Enlace PPP (MLPPP) con los proveedores de admitidos. Esto le permite enlace múltiple PPP enlaces en un solo canal agregado más grande. A diferencia de otras técnicas de multi-WAN, con MLPPP es posible utilizar la ancho de banda completo de todos los enlaces de un solo sentido, y las preocupaciones habituales sobre el equilibrio de carga y
conmutación por error no se aplican. El enlace MLPPP se presenta como una interfaz con una dirección IP, y si uno enlace falla, las funciones de conexión de la misma pero con capacidad reducida. El principal inconveniente para MLPPP es la dificultad de controlar el estado de enlace de las líneas individuales.

Activación MLPPP se hace simplemente seleccionando más de una interfaz al editar una entrada de tipo PPP. Selección de múltiples entradas puede variar por OS y el navegador, pero más comúnmente se realiza mediante la celebración de
la Ctrl tecla mientras hace clic en los nombres de interfaz. Al configurar MLPPP, tenga en cuenta que el ISP debe ser compatible con MLPPP, todos los enlaces deben ser conectados a la misma ISP, y las mismas credenciales deben
será válida para todos los enlaces que se utilizarán al mismo tiempo. También funciona mejor cuando los circuitos son todos de la misma
la capacidad, pero puede trabajar con velocidades diferentes en algunos casos. Si no está seguro si sus soportes ISP MLPPP, consulte con ellos antes de pedir un circuito adicional para este propósito. Incluso si el proveedor no es compatible con MLPPP todavía puede ser posible utilizar los circuitos separado con un tradicional múltiples Configuración WAN.
Este tema también se discute en el Capítulo 15, Múltiples conexiones WAN.

Tipos de PPP (Point-to-Point Protocol) de la interfaz

Cuando se agrega o edita una entrada de PPP (Point-to-Point Protocol) en Interfaces (Asignar) en el APP tab, la primera opción no es el tipo de enlace. Desde allí se puede seleccionar uno de los siguientes tipos y configurar las opciones específicas de ese tipo.

PPP (3G/4G, Modem)

El tipo de vínculo PPP se utiliza para hablar con un módem a través de un dispositivo serie. Esto puede ser cualquier cosa, desde un viejo
módem de hardware para el acceso dial-up a un dongle USB 3G/4G para acceder a una red celular. Sobre seleccionar el tipo de enlace PPP, la lista Link Interface (s) se rellena con los dispositivos de serie que se pueden utilizar para comunicarse con un módem. Puede hacer clic en una entrada específica para seleccionarlo para su uso. Después de seleccionar
la interfaz, es posible que la opción de introducir una descripción para la entrada PPP.
Si una red 3G/4G está en uso, puede utilizar las opciones de proveedor de servicios para pre-llenar el restante información de la página. Primero, seleccione un país, como Estados Unidos. La lista de proveedores se aparecer con proveedores de celulares conocidos en ese país. Seleccione un proveedor de la lista, como T-Mobile, y luego la lista del Plan se mostrará. Cuando se elige un plan, los campos restantes serán cumplimentado según sea necesario con los valores conocidos para que el Proveedor y el Plan.

Las opciones se pueden configurar de forma manual si se necesitan otros valores, o para el uso de un proveedor que es no enumerado. Los campos Nombre de usuario y la contraseña son las credenciales utilizadas para la conexión PPP. El Teléfono
Número es el número del ISP que marcar para obtener acceso. Para dial-up es probablemente un teléfono tradicional número, pero para 3G/4G esto tiende a ser un número tal como * 99 # o # 777. El nombre del punto de acceso Opción (APN) es requerido por algunos proveedores de Internet para identificar el servicio al que se está conectando. Algunos
proveedores usan esto para distinguir entre consumidores y empresas planes o redes tradicionales.

PPPoE (Point-to-Point Protocol over Ethernet)

La mayoría se encuentran en las redes DSL comúnmente, PPPoE es un método popular de la autenticación y la obtención de
acceso a una red de ISP. Al seleccionar el tipo de enlace PPPoE, la lista Link Interface (s) está poblada
con interfaces de red que se pueden utilizar para PPPoE. Estos son por lo general las interfaces físicas pero puede
también trabajar sobre algunos otros tipos de interfaz, como VLAN. Seleccione al menos una interfaz a utilizar para este
enlace. Después de seleccionar la interfaz, es posible que la opción de introducir una descripción para la entrada de
PPPoE.
Como mínimo, debe rellenar los campos de nombre de usuario y contraseña. Estos serán proporcionados por su
proveedor de Internet, y
el nombre de usuario suele ser en forma de una dirección de correo electrónico, tales como
mycompany@ispexample.com.
El nombre de Servicio de nombres puede ser requerida por algunos proveedores de Internet, pero a menudo se deja en
blanco. Si usted está en duda,
dejarlo en blanco o póngase en contacto con su ISP y preguntar si es necesario. Algunos proveedores requieren que un
valor
NULL sea introducido en el nombre del servicio. Si ese comportamiento es requerido por su ISP, compruebe Configurar un
Nombre del servicio NULL.

PPTP (Point-to-Point Protocolo de tunel)

No se debe confundir con un PPTP VPN, este tipo de interfaz PPTP está destinado a conectarse a un ISP
y autenticar, la misma fue como funciona PPPoE. Al seleccionar el tipo de enlace PPTP, el Link
Interfaz (s) lista se rellena con interfaces de red que se pueden utilizar para PPTP. Estos son típicamente
interfaces físicas, pero también puede funcionar sobre otros tipos de interfaz, tales como VLAN. Seleccione al menos
una interfaz que se utilizará para este enlace. Después de seleccionar la interfaz, puede introducir opcionalmente una
descripción
para la entrada de PPTP.

Como mínimo, debe rellenar los campos de nombre de usuario y contraseña. Estos serán proporcionados por el ISP.

L2TP (Layer 2 Tunneling Protocol)

L2TP, ya que está configurado aquí, se utiliza para la conexión a un ISP que lo requiere para la autenticación como una
tipo de WAN. L2TP funciona de forma idéntica a PPTP. Puede hacer referencia a la sección anterior para la
configuración
información.

Opciones PPP avanzadas

Todos los tipos de APP tienen algunas opciones avanzadas en común que se pueden editar en sus entradas aquí. En la
mayoría
casos, estos ajustes no deben ser alterados, pero están aquí, si se desean ajustes no predeterminados. ¿Cuándo
edición de un registro PPP, estos ajustes se accede haciendo clic en Mostrar opciones avanzadas.

Dial On Demand

El comportamiento por defecto de un enlace PPP es conectar de inmediato, e inmediatamente, intentará
reconectarse cuando se pierde un enlace. Este comportamiento se describe como siempre encendido. El Active Dial-on-
Demand
modo retrasará este intento de conexión. Cuando se establece, se va a esperar hasta que el paquete intenta salir
el servidor de seguridad a través de esta interfaz, y luego se conectará. Una vez conectado, no lo hará de forma
automática
desconectar.

Idle Timeout

Como se mencionó anteriormente, una conexión PPP se mantiene abierta de forma indefinida por defecto. Si introduce un
valor de Tiempo de espera de inicio, en segundos, a continuación, el enlace será objeto de seguimiento para la actividad.
Si hay no es
tráfico en el enlace para ese período de tiempo, se desconectará el enlace. Si Enable Dial-on-Demand
modo también se ha establecido, se volverá a marcar la carta de modo.

Nota

Tenga en cuenta que pfSense realizará el monitoreo de puerta de enlace por defecto que va a generar una
Ping ICMP por segundo en la interfaz. Si no puede configurar un valor de tiempo de espera inactivo no está
causando un
desconecte cuando se esperaba, es la causa probable de la vigilancia del tráfico de gateway. Esto puede ser

trabajado en torno a la edición de la pasarela para el enlace PPP, y la comprobación Desactivar pasarela Seguimiento.

Compresión (vjcomp)

Esta opción controla si o no va a utilizar la compresión de cabeceras Van Jacobson TCP. De forma predeterminada, que se negociará con el par durante la entrada, por lo que si ambas partes admiten la función se va a utilizar. Comprobación vjcomp Disable hará que la función para siempre estar deshabilitado. Normalmente esta función es beneficioso, ya que ahorra varios bytes por paquete de datos TCP. Casi siempre se quiere salir de ella permitido. Esta compresión es ineficaz para las conexiones TCP con extensiones modernas habilitados como de fecha y hora o SACK, que modifican opciones TCP entre paquetes secuenciales.

Fix TCP MSS

La opción tcpmssfix hace que el daemon PPP para ajustar los segmentos SYN TCP entrantes y salientes de modo que el tamaño de segmento máximo solicitado (SMS) no es mayor que la cantidad permitida por el MTU de la interfaz. Esto es necesario en muchas configuraciones para evitar problemas causados por los routers que caen ICMP
mensajes "Datagram Too Big". Sin estos mensajes, la máquina de origen envía datos, que pasa a el router rogue continuación, golpea una máquina que tiene una MTU que no es lo suficientemente grande para los datos. Debido a que el
IP "no fragmentar" la opción está activada, la máquina envía un mensaje "de Datagrama Too Big" ICMP al ordenante y descarta el paquete. El router rogue coloca el mensaje ICMP y el autor
nunca llega a descubrir que se debe reducir el tamaño de los fragmentos y las caídas del IP No fragmentar opción sus datos salientes. Si por alguna razón usted no desea este comportamiento, consulte Disable tcpmssfix.

Nota

Los valores de MTU y MSS para la interfaz se pueden ajustar la configuración de la interfaz página en el menú Interfaces, como Interfaces WAN.

Secuencia corto (ShortSeq)

Esta opción sólo tiene sentido si MLPPP se negocia. Se prohíbe fragmento multibrazo más corto cabeceras, ahorrando dos bytes en cada fotograma. No es necesario deshabilitar esta para las conexiones que son No multibrazo. Si está utilizando MLPPP y necesita deshabilitar dicha función, compruebe Disable shortseq.

Dirección de control de campo Compresión (AFCComp)

Dirección y control de compresión de campo. Esta opción sólo se aplica a los tipos de enlace asíncrono. Se ahorra dos bytes por trama. Si necesita desactivar esto, compruebe Disable acfcomp.

Protocolo de compresión de campo (ProtoComp)

Compresión campo Protocolo. Esta opción guarda un byte por trama para la mayoría de los marcos. Si necesita desactivar esto, consulte Disable protocomp.

GRE (Generic Routing Encapsulation)

Generic Routing Encapsulation (GRE) es un método de tráfico de un túnel entre dos routers sin cifrado. Puede ser utilizado para enrutar paquetes entre dos lugares que no están conectados directamente, que no requieren cifrado. También se puede combinar con un método de cifrado que no hace realizar su propio túnel. Este es el caso de PPTP, que emplea a GRE túnel el tráfico de la VPN después de establecer un canal cifrado. IPsec, en el modo de transporte, también se puede utilizar para GRE tunelización encriptada tráfico. El protocolo GRE fue originalmente diseñado por Cisco, y es el valor por defecto el modo de túnel en muchos de sus dispositivos.

La interfaz de Padres del túnel GRE es la interfaz sobre la que el túnel GRE terminará. A menudo este será WAN o una conexión de tipo de WAN.

La dirección remota GRE es la dirección del par remoto. Esta es la dirección donde los paquetes GRE será enviado, por lo que sería la dirección enrutable para el otro extremo del túnel.

El túnel dirección local GRE es la dirección interna para este final del túnel. El tráfico en el interior de el túnel se obtiene de esta dirección, y el tráfico de túnel remoto se envían a esta dirección desde el otro lado.

La dirección remota túnel GRE es la dirección utilizada en el interior del túnel hasta llegar al otro extremo. Tráfico ir al otro extremo del túnel sería encaminada a esta dirección.

Si se selecciona túnel móvil, se enviará el tráfico tunelizado codificado en el protocolo IP móvil (55) en lugar de utilizar GRE (47).

El dispositivo GRE necesita una ruta al destino que es menos específico que el uno sobre el túnel a funcione correctamente. Básicamente, es necesario que haya una ruta hacia el extremo remoto que no se ejecuta en el túnel, ya que esto sería un bucle y el tráfico nunca pudo llegar a su destino. La forma de buscar la ruta opción controla este comportamiento, y se puede utilizar si el extremo remoto tal como se especifica más arriba en el GRE
dirección remota no es el sistema remoto donde efectivamente se recibe el tráfico GRE.

Por defecto, el Protocolo de Comunicación de Web Cache (WCCP) versión 1 se utiliza en el túnel GRE. Si desee utilizar WCCP versión 2 en lugar, comprobar la versión WCCP.

Por último, el campo Descripción le permite proporcionar una breve descripción de este túnel GRE para con fines de documentación.

GIF (interfaz de túnel genérico)

GIF, abreviatura de Generic Tunneling Interface, es similar al GRE, ya que es un medio para el tráfico de túnel entre dos hosts. Sin embargo, además de la construcción del túnel IPv4 o IPv6 directamente, GIF se puede utilizar para túneles IPv6 sobre redes IPv4 y viceversa. Túneles GIF se utilizan comúnmente para obtener IPv6 conectividad a proveedores de túneles como Hurricane Electric [http://www.tunnelbroker.net/] y SixXS [Http://www.sixxs.net/] en los lugares donde todavía no existe ninguna conectividad IPv6 nativa.

Interfaces de GIF llevan más información a través del túnel que se puede hacer con GRE, pero no es tan GIF amplio apoyo. Por ejemplo, con IPsec en modo de transporte, se puede utilizar un túnel entre el GIF criterios de valoración a la capa 2 del puente entre dos lugares. Aunque no se recomienda la práctica, no algunas circunstancias raras que requieren una configuración de este tipo.

Al igual que con GRE, la interfaz de Padres del túnel GIF es la interfaz sobre la que el túnel GIF se terminará. A menudo este será WAN o una conexión de tipo de WAN.

La dirección remota GIF es la dirección de la distancia entre pares, a la que se enviará el tráfico GIF. Para ejemplo, en un túnel IPv6-in-IPv4 a Hurricane Electric, esta sería la dirección IPv4 del túnel servidor, como 209.51.181.2.

La dirección local GIF túnel es la cara visible interior del túnel. Por ejemplo, cuando la tunelización IPv6 en-IPv4 a través de Hurricane Electric, se refieren a esto como la dirección IPv6 del cliente.

La dirección remota GIF túnel es la parte más alejada interno al túnel. Por ejemplo, cuando la tunelización IPv6 en-IPv4 a través de Hurricane Electric, se refieren a esto como la dirección IPv6 del servidor. El desplegable CIDR es utilizado para seleccionar el tamaño de subred para las direcciones de túnel. En este ejemplo sería 64.

Los controles de opción de almacenamiento en caché de ruta si la ruta hacia el extremo remoto se almacena en caché. Si su
ruta de la distancia entre pares es estático, al establecer esta puede evitar una búsqueda de rutas por paquete. Sin embargo, si la
camino hacia el otro lado puede cambiar, esta opción podría resultar en el tráfico GIF no fluya cuando el cambios de ruta.
La opción de comportamiento amistoso ECN controla si o no notificación explícita de congestión (ECN) - práctica amistosa de copiar el bit TOS a / fuera del tráfico del túnel se hace. Por defecto el bit TOS en los paquetes se borra o se establece en 0, dependiendo de la dirección del tráfico. Con este conjunto de opciones,

el bit se copia según sea necesario entre los paquetes de interior y exterior para ser más amigable con intermedio routers que pueden realizar la modulación del tráfico.

Por último, el campo Descripción le permite proporcionar una breve descripción de este túnel GIF para con fines de documentación.

> Nota
>
> En la mayoría de los casos tendrá que asignar esta interfaz GIF bajo Interfaces (Asignar). ¿Cuándo Al hacerlo, asegúrese de configurar la interfaz como una IP estática o interfaz IPv6, y utilizar la misma Dirección IP y la máscara de subred de longitud / prefijo, como en la dirección local GIF túnel. El túnel GIF dirección remota debe entonces ser añadida como una puerta de enlace.

Puentes

Interface Bridges, o múltiples interfaces atados juntos en una capa de 2 dominio compartido común de colisión, se crean y administran en la ficha Puentes bajo Interfaces (Asignar). Más información sobre puente, incluyendo la manera de crear y administrar los puentes, se puede encontrar en el capítulo 13, Tender un puente.

LAGG (Link Aggregation)

En FreeBSD, y por lo tanto pfSense, un `lagg (4)` interfaz (LAGG) se utiliza para la agregación de enlaces. En otra Es decir, utilizando múltiples interfaces juntos como uno. Hay varias maneras de que esto puede funcionar, ya sea para la obtención de ancho de banda adicional, la redundancia, o alguna combinación de los dos.

Una interfaz de LAGG se puede hacer de la selección de múltiples interfaces no utilizadas. La interfaz de Padres cuadro de selección en la pantalla de edición LAGG es donde se hace esto. Selección de múltiples entradas puede variar por el sistema operativo y el navegador, pero lo más frecuente es que se lleva a cabo mediante la celebración de la Ctrl tecla mientras hace clic en el nombres de interfaz. Una interfaz sólo puede añadirse a un grupo LAGG si no se asigna.

Después de crear una interfaz LAGG, se asigna la interfaz lagg como cualquier otro bajo Interfaces (Asignar) y darle una dirección IP, o usted puede construir otras cosas en la parte superior de la misma, tales como VLAN y asignar esos.

Debido a una limitación en FreeBSD, `lagg (4)` no es compatible `altq (4)` por lo que aún no es posible utilizar el conformador de tráfico en interfaces basadas en LAGG LAGG o. Como solución temporal, puede utilizar limitadores de el uso de ancho de banda en las interfaces de control Lagg.

Actualmente hay seis modos de funcionamiento diferentes para las interfaces de Lagg: conmutación por error, FEC, LACP, Load Equilibre, Round Robin y Ninguno.

Protocolo LAGG Failover

Cuando se utiliza el tráfico de protocolo LAGG Failover sólo se enviará en las interfaces primarias de la grupo, y si falla, entonces el tráfico usará la siguiente interfaz disponible. La interfaz principal es la primera interfaz seleccionada en la lista, y continuará en el orden hasta que se alcanza el final de las interfaces seleccionadas.

Protocolo LAGG FEC

El modo de FEC apoya Cisco EtherChannel. Esta es la configuración estática y no negocia la agregación con los marcos de pares o de cambio para controlar el enlace. Esta opción es esencialmente el mismo que el de carga Saldo.

Protocolo LAGG LACP

El protocolo LAGG más utilizado es LACP. Este modo es compatible con el estándar IEEE 802.3ad Enlace Aggregation Control Protocol (LACP) y el Protocolo de Marker. En el modo LACP, la negociación es realizado con el interruptor - que también debe ser compatible con LACP - para formar un grupo de puertos que son todos activo al mismo tiempo. Esto es lo conocido como Grupo de agregación de enlace, o LAG. La velocidad y la MTU

de cada puerto en un LAG deben ser idénticos y los puertos también deben funcionar a full-duplex. Si el enlace se pierde a un
puerto del LAG, sigue funcionando pero a una capacidad reducida. De esta manera, un LAGG LACP bundle usted puede ganar tanto la redundancia y mayor ancho de banda.

El tráfico será equilibrado entre todos los puertos del LAG, sin embargo, para la comunicación entre dos hosts individuales que sólo utilizará un máximo de un único puerto a la vez porque el cliente sólo quiere hablar con uno Dirección MAC a la vez. Para múltiples conexiones a través de múltiples dispositivos, esta limitación efectiva vuelve irrelevante para la mayoría de los patrones de tráfico y no es relevante para la conmutación por error.

Además de configurar esta opción en pfSense, también tendrá que configurar el interruptor para habilitar LACP en estos puertos o agruparlos en un grupo LAG allí. Ambas partes deben ponerse de acuerdo sobre la configuración con el fin de que funcione correctamente.

Cargue Protocolo LAGG Equilibrio

El modo de equilibrio de carga aceptará el tráfico de entrada en cualquier puerto del grupo LAGG. Es un estático instalación que no supervisa el estado de los vínculos o hacer cualquier negociación con el interruptor. El tráfico saliente es
equilibrio de carga basado en un hash calcula utilizando varios factores, como el origen y el destino de IP / MAC y la etiqueta de VLAN.

Ronda Protocolo LAGG Robin

El modo de Round Robin aceptará el tráfico de entrada en cualquier puerto del grupo LAGG, y enviar de salida tráfico que utiliza un algoritmo de planificación round robin. Normalmente, esto significa que el tráfico se envía en secuencia, el uso de cada interfaz del grupo a su vez.

Ninguno Protocolo LAGG

El modo Ninguno desactiva el tráfico en la interfaz LAGG sin tener que deshabilitar el real interfaz. El sistema operativo aún se cree que la interfaz está funcionando y utilizable, pero no hay tráfico será enviado o recibido
en el grupo.

OpenVPN

Después de que se haya creado, interfaces de OpenVPN pueden ser asignados en virtud de Interfaces (Asignar). ¿Cuándo
esto se hace, la interfaz debe ser habilitada en sus interfaces Página OPTX y ajuste a un tipo de propiedad intelectual de
Ninguna para IPv4 e IPv6. Asignación de una interfaz OpenVPN le permitirá crear la interfaz específica reglas, y también utilizan la interfaz de OpenVPN en otras partes de la interfaz gráfica que requiere una interfaz asignada. Si
la interfaz de OpenVPN está asignado es un cliente, esto también provoca la creación de una puerta de enlace dinámico. Esta pasarela puede ser utilizado para el encaminamiento de política, o en un grupo de pasarela para multi-WAN.

Configuración de la interfaz

Una vez que la interfaz ha sido asignado bajo Interfaces (Asignar), se le asigna un nombre por defecto, tales como OPT1, OPT2, y así sucesivamente. Las dos primeras interfaces se denominan WAN y LAN, por razones históricas, pero usted puede cambiar el nombre de ellos los usan como más te guste. Estos nombres OPTX aparecen bajo las Interfaces
menú, como Interfaces OPT1. Al seleccionar la opción de menú para la interfaz le llevará a que página de configuración de la interfaz.

Si usted nunca ha utilizado esta interfaz antes, usted será recibido por una página que contiene una sola opción - Active Interface. Al marcar Habilitar interfaz, aparecerá el resto de las opciones.

Descripción

La interfaz se puede cambiar mediante la introducción de un nuevo nombre en el cuadro Descripción. Esto cambiará el el nombre de la interfaz en el menú Interfaces, en los registros bajo Firewall Reglas, bajo Servicios

DHCP, y en otros lugares a lo largo de la interfaz gráfica de usuario. Estos nombres de interfaz sólo puede contener letras, números
y el único carácter especial que se permite es un guión bajo ("_"). Esto hace que sea mucho más fácil
recordar no sólo lo que es una interfaz para el, sino también para identificar una interfaz para agregar reglas de firewall o la elección de otra funcionalidad de cada interfaz.

Dirección MAC

Usted puede cambiar la dirección MAC de un interfaz en caso de que tenga que suplantar la dirección MAC de un anterior pieza de equipo. Por lo general esto se debe evitar, ya que el viejo MAC sería generalmente
limpiado reiniciando el equipo al que se conecta este servidor de seguridad o en la limpieza de la tabla ARP,
o esperar a que las viejas entradas ARP de expirar. En algunos casos puede ser deseable "clon" o "engañar"
la dirección MAC de una pieza de equipo anterior. Esto puede permitir una transición suave de un
viejo router a un router nuevo, de modo que las cachés de ARP en los dispositivos y routers upstream no son una preocupación. Lo
También puede ser usado para engañar a una parte del equipo en la creencia de que está hablando con el mismo dispositivo que
que estaba hablando antes, como en los casos en que un determinado router de la red utiliza ARP estática o de otra manera
filtros basados en direcciones MAC. Esto es común en los módems de cable, donde es posible que tenga que registrarse MAC con el ISP si y cuando cambia.
Una desventaja de la suplantación de la MAC es que, a menos que la vieja pieza de equipo se retiró de forma permanente, se corre el riesgo de que después han tenido un conflicto de direcciones MAC en su red, lo que puede llevar a la conectividad
problemas. También los problemas de caché de ARP tienden a ser muy temporal, resolviendo de forma automática dentro minutos o apagando y encendiendo otro equipo.

En caso de necesitar la antigua dirección MAC para ser restaurado, este cuadro debe ser limpiado hacia fuera y después el cortafuegos
debe ser reiniciado.

MTU (Maximum Transmission Unit)

El campo Tamaño de la unidad de transmisión máxima (MTU) normalmente se puede dejar en blanco, pero se puede cambiar
si se desea. Algunas situaciones pueden requerir una MTU más bajo para asegurar los paquetes están dimensionados adecuadamente para
su conexión a Internet. En la mayoría de los casos, los valores por omisión para el tipo de conexión WAN se asume funcione correctamente.

MSS (Maximum Segment Size)

Al igual que en el campo MTU, el campo MSS "sujetar" el tamaño de segmento máximo (MSS) de TCP conexiones con el tamaño especificado con el fin de evitar problemas con el Path MTU Discovery.

Velocidad y Dúplex

El valor predeterminado de velocidad del enlace y el modo dúplex es dejar que el sistema operativo de decidir qué es lo mejor. Que
opción por defecto es típicamente Autoselect, que negocia la velocidad mejor posible y dúplex
con los pares, normalmente un interruptor.

Bloque de Redes Privadas

Si selecciona las redes privadas de bloque, pfSense insertará una regla automática que va a impedir cualquier RFC 1918 redes (10.0.0.0 / 8, 172.16.0.0/12, 192.168.0.0/16) y bucle de retorno (127.0.0.0 / 8) a partir de la comunicación en esa interfaz. Esta opción es por lo general sólo es deseable en las interfaces de tipo WAN, a evitar la posibilidad de tráfico numerada privada que viene en más de una interfaz pública.

Redes Bloquear bogon

Si la opción redes del Bloque bogon está marcada, pfSense descargará periódicamente y bloquear el tráfico de una lista de redes no asignados y reservados. Ahora que el espacio IPv4 todo ha sido asignado, este
lista es bastante pequeña, que contiene en su mayoría las redes que se han reservado de alguna manera por la IANA. Estos
las redes no deben estar en uso activo en una red, en especial se encarga de Internet, por lo que es una buena

cosa para el uso en las interfaces de tipo WAN. Para IPv6, la lista es aún muy grande, que contiene trozos grandes del posible espacio IPv6 que aún no ha sido asignado. En los sistemas con bajas cantidades de RAM, esta lista puede ser demasiado grande, o el valor predeterminado del Firewall de Entradas máximas de la tabla puede ser demasiado pequeño. Que valor puede ser ajustado en Sistema Avanzado en el / pestaña NAT Firewall.

Tipos IPv4 WAN

Una vez que la interfaz se ha asignado, en la mayoría de los casos tendrá que configurar una dirección IP. Para IPv4 conexiones, se puede elegir entre: Estática, DHCP, PPP, PPPoE, PPTP, y L2TP. Estas opciones son seleccionado con el selector de tipo de configuración IPv4.

Ninguno

Configuración del tipo de configuración de IPv4 a Ninguno deshabilitará IPv4 en la interfaz. Esto es útil si el interfaz no tiene ninguna IPv4, o si la dirección de IP en la interfaz está siendo administrado de alguna otra manera, tales como para una interfaz OpenVPN.

IPv4 estático

Selección estática IPv4 le permitirá configurar manualmente la dirección IP para la interfaz que desea utilizar. Uso esta opción permite a los tres campos adicionales en la pantalla de configuración de la interfaz: dirección IPv4, un CIDR Selector de máscara de subred y un campo Gateway.

Introduzca la dirección IPv4 para la interfaz de la barra de dirección IPv4, y elegir la máscara de subred de el CIDR desplegable después de que el espacio para la dirección.

Si se trata de un tipo de interfaz WAN, debe seleccionar una puerta de enlace o agrega uno si uno no existe ya. Para elegir uno que ya existe, haga clic y seleccionado de la lista desplegable. Si hace clic en añadir uno nuevo, aparecerá un formulario para añadir el gateway. Si el campo de formulario no aparece, pruebe con un navegador web diferente.
Históricamente, Internet Explorer ha tenido problemas con algunas de nuestras formas impulsadas JavaScript y AJAX, éste en particular.

Para agregar una puerta de entrada, después de hacer clic en Agregar una nueva, rellenar los datos solicitados en el formulario nuevo. Si este
es la única red WAN o será un nuevo valor predeterminado WAN, Cheque Puerta de enlace predeterminada. Se utiliza el nombre de la pasarela
para referirse a la pasarela internamente, así como en lugares como Grupos de puerta de enlace, los gráficos de calidad, y en otro lugar. El campo Puerta de enlace IPv4 es donde se introduce la dirección IP de la pasarela real. Esta dirección debe estar dentro de la misma subred que la dirección estática IPv4. El cuadro Descripción le permite introducir un poco de texto para indicar el fin de la puerta de enlace. Cuando haya terminado, haga clic en Guardar Gateway.

Nota

Selección de una puerta de enlace de la lista desplegable, o la adición de una nueva puerta de entrada y la selecciona, se
hacer pfSense tratar esa interfaz como una interfaz de tipo WAN para NAT y las funciones relacionadas.
Esto no es deseable para las interfaces-el revestimiento interior, como LAN o una DMZ. Usted puede todavía utilizar puertas de enlace en esas interfaces con el propósito de rutas estáticas sin seleccionar una puerta de enlace
aquí en la pantalla de las interfaces.
Los predeterminados IPv4 e IPv6 gateways funcionan independientemente unos de otros. Los dos no tiene por qué
estar en el mismo circuito. Cambio de la puerta de enlace predeterminada IPv4 no tiene ningún efecto en la pasarela IPv6,
y viceversa.

DHCP

La elección de DHCP de la lista hará que pfSense para intentar la configuración IPv4 automática de esta interconectar a través de DHCP. Esta opción también activa tres campos adicionales en la página: Nombre de host, Alias Dirección IPv4, y un desplegable CIDR para la dirección IPv4 Alias. Bajo la mayoría de circunstancias éstas campos adicionales pueden simplemente dejar en blanco.

Algunos ISP requieren que el nombre de host de identificación del cliente. El valor en el campo Nombre de host se envía como
el identificador de cliente DHCP y el nombre de host al solicitar una concesión DHCP.

El valor introducido en el campo de dirección Alias IPv4 se utiliza como una dirección IPv4 alias fijado por el DHCP cliente. Esto puede ser útil para acceder a una pieza de arte en una red independiente, de forma estática numerada fuera del ámbito de DHCP. Un ejemplo sería el de llegar a la dirección de un módem de cable IP Dirección. Con IPv4 estáticas frente a usted puede simplemente añadir un VIP tipo de alias IP, pero como eso no es disponibles en DHCP, esta opción le permite a uno ser configurado.

Tipos de PPP

Los distintos tipos de conexión basados en PPP como PPP, PPPoE, PPTP, L2TP y fueron cubiertos en detalle anteriormente en este capítulo (la sección llamada "APP"). Cuando se selecciona aquí en las interfaces pantalla en la que puede definir o cambiar sus opciones básicas como se describe. Para acceder a las opciones avanzadas, siga
el enlace de esta página o navegar hasta Interfaces (Asignar) en la pestaña PPP, busque la entrada, y editar allí.

Tipos IPv6 WAN

Al igual que en IPv4, los controles de tipo de configuración IPv6 si y cómo se asigna una dirección IPv6 a una interfaz. Hay varias maneras diferentes de configurar IPv6, el método exacto que tendrá que utilizar depende de la red a la que está conectado y la forma en que el ISP ha desplegado IPv6 en que red. Para obtener más información acerca de IPv6, incluyendo una introducción básica, consulte la sección denominada "IPv6".

Ninguno

Configuración del tipo de configuración de IPv6 en None deshabilita IPv6 en la interfaz. Esto es útil si el interfaz no tiene ninguna IPv4, o si la dirección de IP en la interfaz está siendo administrado de alguna otra manera, tales como para una interfaz OpenVPN.

IPv6 estático

Selección estática IPv6 le permitirá ajustar manualmente la dirección IPv6 para la interfaz que desea utilizar. Uso esta opción permite a los tres campos adicionales en la pantalla de configuración de la interfaz: dirección IPv6, un Prefijo Selector de longitud, y un campo de Gateway.

Introduzca la dirección IPv6 para la interfaz de la barra de dirección IPv6, y elegir la longitud del prefijo de la lista desplegable después de que el espacio para la dirección.

Si se trata de un tipo de interfaz WAN, debe seleccionar una puerta de enlace o agrega uno si uno no existe ya. Para elegir uno que ya existe, haga clic y seleccionado de la lista desplegable. Si hace clic en añadir uno nuevo, aparecerá un formulario para añadir el gateway. Si el campo de formulario no aparece, pruebe con un navegador web diferente.
Históricamente, Internet Explorer ha tenido problemas con algunas de nuestras formas impulsadas JavaScript y AJAX, éste en particular.

Para agregar una puerta de entrada, después de hacer clic en Agregar una nueva, rellenar los datos solicitados en el formulario nuevo. Si este es el
sólo IPv6 WAN o será un nuevo valor predeterminado IPv6 WAN, Cheque Puerta de enlace predeterminada v6. El nombre de la pasarela
IPv6 se utiliza para referirse a la puerta de enlace internos, así como en lugares como Grupos de puerta de enlace, la Calidad
Gráficos, y otros lugares. El campo Puerta de enlace IPv6 es donde se introduce la dirección IP de la pasarela real. Este dirección debe estar dentro de la misma subred que la dirección IPv6 estática. El cuadro Descripción que permite para entrar un poco de texto para indicar el fin de la puerta de enlace. Cuando haya terminado, haga clic en Guardar Gateway.

Nota

Selección de una puerta de enlace de la lista desplegable, o la adición de una nueva puerta de entrada y la selecciona, se
hacer pfSense tratar esa interfaz como una interfaz de tipo WAN. Esto no es deseable para la interna-

las interfaces que enfrentan, tales como LAN o DMZ. Usted todavía puede utilizar puertas de enlace en las interfaces a las
el propósito de rutas estáticas sin seleccionar una puerta de enlace aquí en la pantalla de interfaces.

Los IPv6 e IPv4 gateways por defecto funcionan independientemente unos de otros. Los dos no tiene por qué estar en el mismo circuito. Cambio de la puerta de enlace predeterminada IPv6 no tiene ningún efecto en la pasarela IPv4,
y viceversa.

DHCP6

Elegir DHCPv6 de la lista hará que pfSense para intentar la configuración IPv6 automática de esta interconectar a través de DHCPv6. DHCPv6 configurará el interfaz con una dirección IP, la longitud de prefijo, DNS servidores, y así sucesivamente - pero no una puerta de enlace. La puerta de enlace todavía se obtiene a través de anuncios de enrutador, por lo
esta interfaz se puede configurar para aceptar anuncios de enrutador. Esta es una opción de diseño como parte del IPv6 especificación, no una limitación de pfSense. Para obtener más información sobre los anuncios de enrutador, consulte la sección llamada "anuncios de enrutador".

Cuando DHCPv6 está activo, otro campo también está disponible: tamaño DHCPv6 Prefijo Delegación. Si su ISP le está proporcionando una red IPv6 enrutada a través de la delegación de prefijo, ellos le dirán que la
El tamaño de la delegación, que se puede seleccionar aquí. Es típicamente un valor en algún lugar entre 48 y 64. Para más información sobre cómo funciona DHCPv6 prefijo delegación, consulte la sección llamada "DHCPv6 Prefijo Delegación ".

SLAAC

La elección de configuración automática de direcciones sin estado, o SLAAC, como el tipo IPv6 hará intento pfSense para configurar la dirección IPv6 para la interfaz de anuncios de enrutador (RA) que anuncian la
prefijo y la información relacionada. Tenga en cuenta que el DNS no se proporciona normalmente a través de la AR, por lo pfSense se sigue
intentará obtener los servidores DNS mediante DHCPv6 al utilizar SLAAC. En el futuro, las extensiones RDNSS para el proceso RA puede permitir que los servidores DNS que se obtienen a partir de la AR. Para obtener más información en el router
anuncios, ver la sección "anuncios de enrutador".

6RD Túnel

6RD es la tecnología de túneles IPv6 am empleado por algunos proveedores de Internet para permitir rápidamente el soporte IPv6 para su
redes, pasando por el tráfico de IPv6 dentro de paquetes IPv4 especialmente diseñados entre el router del usuario y la Relé del ISP. Se relaciona con 6a4, pero está destinado a ser utilizado dentro de la red del ISP, utilizando los ISP Direcciones IPv6 para el tráfico de clientes. Para utilizar 6RD, su ISP debería haberle suministrado con tres piezas de Información adicional: El prefijo 6RD, el 6RD Border Relay, y la longitud 6RD IPv4 Prefijo.

En el cuadro prefijo 6RD, introduzca el prefijo 6RD IPv6 asignado por su proveedor de Internet, tales como 2001: db8 :: / 32.

El 6RD Border Relay es la dirección IPv4 del relé 6RD de su ISP.

La longitud 6RD IPv4 Prefijo controla qué parte de la dirección IPv4 del usuario final está codificada dentro de el prefijo 6RD. Esto es normalmente suministrado por el proveedor de Internet. Un valor de 0 significa que toda la dirección IPv4 se
ser embebido dentro del prefijo 6RD. Este valor permite a los ISP para dirigir con eficacia las direcciones de más de IPv6 a los clientes mediante la eliminación de información redundante IPv4 si la asignación de un ISP es todo dentro de la misma
subred más grande.

6to4 Túnel

Similar a 6RD, 6a4 es otro método de túnel tráfico IPv6 dentro de IPv4. A diferencia, sin embargo 6RD,
6to4 utiliza prefijos y relés constantes. Como tal no hay configuraciones ajustables por el usuario para el uso de la 6to4 opción. El prefijo 6to4 siempre es 2002 :: / 16. Cualquier dirección en el interior del 2002 :: / 16 se considera un 6to4 abordar en lugar de una dirección IPv6 nativa. También a diferencia de 6RD, un túnel de 6to4 se puede terminar en cualquier lugar
en Internet, no sólo en el ISP del usuario, por lo que la calidad de la conexión entre el usuario y el Relé de 6to4 puede variar ampliamente.

Túneles 6to4 siempre terminan en la dirección IPv4 de 192.88.99.1. Esta dirección IPv4 se anycasted, lo que significa que a pesar de la dirección IPv4 es el mismo en todas partes, se puede encaminar hacia regionalmente un nodo cerca del usuario.

Otra deficiencia de 6a4 es que es se basa en otros routers para transmitir el tráfico entre la red 6a4 y el resto de la red IPv6. Hay una posibilidad de que algunos pares IPv6 pueden no tener conectividad a la red 6to4, y por lo tanto estos serían inalcanzables por los clientes que se conectan a 6to4 relés, y esto también puede variar dependiendo del nodo 6a4 a la que el usuario está conectado realmente.

Track Interface

La opción Track Interface trabaja en conjunto con otra interfaz IPv6 usando DHCPv6 Prefijo Delegación. Cuando se recibe una delegación de la ISP, esta opción designa qué interfaz se asignar las direcciones IPv6 delegadas por el ISP.

Después de seleccionar Track Interface, la opción de interfaz IPv6 parece que enumera todas las interfaces en el sistema actualmente establecido para DHCPv6. Seleccione la interfaz de la lista que va a recibir la Información DHCPv6 desde el ISP.

Si el ISP ha delegado más de un prefijo a través de DHCPv6, los controles de identidad IPv6 Prefijo de cuál de los subredes delegadas serán utilizados en esta interfaz. Este valor se especifica en hexadecimal. Si usted es sin saber qué poner aquí, deje en blanco o póngase en contacto con su ISP.

Para obtener más información sobre cómo funciona DHCPv6 prefijo delegación, consulte la sección titulada "DHCPv6 Prefijo Delegación ".

Capítulo 7. Administración de usuarios y Autenticación

En pfSense 2.0, el Administrador de usuarios se introdujo para permitir la adición de varios usuarios a la interfaz gráfica de usuario. Estos
los usuarios pueden utilizar para acceder a la interfaz gráfica de usuario, utilice los servicios de VPN como OpenVPN e IPsec, y el uso de la Cautiva
Portal.
El Administrador de usuarios también se puede utilizar para definir las fuentes de autenticación externos tales como RADIUS y
LDAP.

Cuando esto fue cambiado de la antigua pfSense 1.2.3 estilo, que hizo una página personalizada de inicio de sesión que sea posible, y
También hizo posible el registro de usuario actual a través del Sistema Salir.

Soporte largo pfSense

Al escribir estas líneas, no todas las áreas de pfSense enganchan de nuevo en el Administrador
de usuarios.

- pfSense GUI - Compatible con los usuarios en el Administrador de usuarios, y por medio de RADIUS o LDAP. Los usuarios de
  RADIUS o LDAP todavía necesita tener definiciones en el Administrador de usuarios local para gestionar su acceso
  permisos.
- OpenVPN - Compatible con los usuarios en el Administrador de usuarios, RADIUS o LDAP a través de Administrador de usuarios.
- IPsec - Compatible con los usuarios en el Administrador de usuarios, RADIUS o LDAP a través de Administrador de usuarios.
- Portal Cautivo - Compatible con los usuarios en el Administrador de usuarios, y los usuarios de RADIUS a través de ajustes en el Cautivo
  Página de Portal.
- PPTP - Compatible con los usuarios en la configuración de PPTP, y por medio de RADIUS en la configuración de PPTP.
- L2TP - Compatible con los usuarios en la configuración de L2TP, y por medio de RADIUS en la configuración de L2TP.
- PPPoE Servidor - Soporta los usuarios en la configuración PPPoE, ya través de RADIUS en la configuración PPPoE.

Gestión de usuarios

El Administrador de usuarios se encuentra en el Sistema Administrador de usuarios. Desde allí se puede mantener usuarios, grupos,
configuración de los servidores, y el cambio que rigen el comportamiento del Administrador de usuarios.

Privilegios

Gestión de permisos para usuarios y grupos se realiza de forma similar, así que vamos a cubrir aquí en lugar de duplicar el esfuerzo a continuación. Si usted dirige un usuario o grupo, la entrada debe ser creado y guardado primero antes de que usted puede agregar permisos a la cuenta o grupo. Para agregar los permisos, al editar el

usuario o grupo existente, haga clic en los privilegios asignados o sección Privilegios eficaces.

Una lista de los permisos se muestra en la pantalla, que contiene todos los permisos posibles disponibles. Por defecto todos ellos son sin seleccionar. Usted puede agregar permisos de uno en uno, o de selección múltiple. Si hay otro permisos ya presente en el usuario o grupo, que se ocultan de la lista por lo que no se pueden añadir
dos veces.

Selección de un permiso se mostrará una breve descripción de lo que hace en el área de descripción bajo el lista de permisos. La mayoría de los permisos son bastante explica por sí mismo sobre la base de sus nombres, pero algunos
Permisos notables son:

• WebCFG - Todas las páginas - Permite al usuario el acceso a cualquier página de la interfaz gráfica de usuario
• WebCFG - Dashboard (todos) - Le permite al usuario el acceso sólo la página de panel y todos sus asociados funciones (widgets, gráficos, etc)

• WebCFG - Sistema: Password Manager usuario Page - Si el usuario tiene acceso a esta página solo, que puede iniciar sesión en la interfaz gráfica de usuario para configurar su propia contraseña, pero no hacer nada más.

• Usuario - VPN - IPSec xauth Dialin - Permite al usuario conectar y autenticar IPsec para xauth

• Usuario - Config - Denegar Config Write - No permite que el usuario pueda realizar cambios en el firewall config (config.xml). Tenga en cuenta que esto no impide que el usuario pueda tomar otras acciones que hacen no implica por escrito a la config.

• Usuario - Sistema - acceso a la cuenta de carcasa - Proporciona al usuario la posibilidad de acceder a través de ssh, aunque la usuario no tiene acceso a nivel de raíz para la funcionalidad es limitada. En el futuro, sudo soporte puede ser añadido para mejorar esta característica.

En pfSense 2.1, el menú del sistema que aparece en la página sólo muestra las entradas de menú a la que el usuario tiene acceso. En pfSense 2.0.x, todos los elementos de menú se muestran pero el usuario se niega el acceso a la los que no podían cargar.

Usuarios Adición / Edición

La pestaña Usuarios en Sistema Administrador de usuarios es donde se gestionan los usuarios individuales. Para agregar un nuevo usuario, haga clic en . Para editar un usuario existente, haga clic en

Antes de agregar permisos a un usuario, primero se debe crear, por lo que el primer paso es añadir siempre el usuario. Si va a tener varios usuarios que necesitan los mismos permisos, es más fácil para agregar un grupo y luego agregar los usuarios al grupo.

Para agregar un usuario, haga clic en . Aparecerá la nueva pantalla de usuario.

La casilla de verificación Disabled controla si este usuario estará activo. Si tiene que desactivar esta cuenta, usted puede marcar esta casilla.

Se requiere el nombre de usuario y debe tener 16 caracteres o menos y sólo puede contener letras, números, y un punto, guión o guión bajo.

Los campos de contraseña también se requieren. Estas contraseñas se almacenan en la configuración de pfSense como hashes. Asegúrese de que los dos campos coinciden para confirmar la contraseña.

El campo Nombre completo opcional se puede utilizar para introducir el nombre de un usuario o una descripción de la cuenta.
Una fecha de caducidad también puede definirse si desea desactivar el usuario de forma automática cuando esa fecha ha sido alcanzado. La fecha debe ser inscrita en MM / DD / YYYY formato.

Si ya ha definido los grupos y desea agregar un usuario a ellos, entonces usted puede utilizar el Grupo Membresías controlan para definir qué grupos de que el usuario va a ser un miembro de. Para añadir un grupo para este usuario, búsquelo en la lista, selecciónelo y haga clic para moverlo a la Miembro de la columna. Para eliminar un usuario de el grupo, selecciónelo de la Miembro de la columna y haga clic para moverlo a la No miembro de la columna.

El Privilegios parte efectiva del editor usuario sólo aparece si está editando un usuario existente. Lo hace no aparecen cuando se agrega un usuario. Vea la sección llamada "Privilegios" para obtener información sobre la gestión de privilegios. Si el usuario forma parte de un grupo, los permisos del grupo se muestran en esta lista, pero los permisos no se pueden editar, sin embargo se pueden agregar permisos adicionales.

El comportamiento de la porción Certificado de los cambios de la página en función de si va a agregar un usuario o la edición de un usuario. Al agregar un usuario, para crear un cheque certificado Haga clic para crear un certificado de usuario para mostrar la forma de crear un certificado. Escriba el nombre descriptivo, elija una entidad emisora de certificados, seleccione

una longitud de clave, y entrar en un curso de la vida. Para obtener más información sobre estos parámetros, consulte la sección llamada
"Crear un certificado interno". Si va a editar un usuario, esta sección de la página en lugar se convierte en un
lista de certificados de usuario. A partir de aquí, puede agregar clickto un certificado para el usuario. Los ajustes en
esa página es idéntica a la sección llamada "Crear un certificado interno" excepto aún más de la
datos es rellenado previamente con el nombre del usuario. Si ya existe el certificado, puede seleccionar Elija una
Certificado existente y luego recoger un certificado existente de la lista.

Las teclas de la parte autorizada de la configuración del usuario le permite pegar en clave pública SSH del usuario para la cáscara o
otro acceso SSH. Para agregar una clave, marque Haga clic para pegar una clave autorizada y luego pegar en los datos clave.

El campo Pre-Shared Key IPsec se puede utilizar para una configuración de IPsec móviles no de xauth. Si un Pre-Shared Key se introduce aquí, el nombre de usuario se utiliza como el identificador. También puede ver el PSK bajo VPN IPsec en la ficha Pre-Shared Keys. Si sólo va a utilizar el móvil IPsec con xauth, este campo puede
dejarse en blanco.

Después de guardar el usuario puede hacer clic en cada fila del usuario para editar la entrada.
en

Adición / Edición de grupos

Los grupos son una gran manera de manejar conjuntos de permisos para dar a los usuarios de modo que no es necesario que
mantener de forma individual en cada cuenta de usuario. Por ejemplo, usted podría tener un grupo para IPsec
usuarios XAuth, o un grupo que puede acceder el salpicadero del servidor de seguridad, un grupo de administradores de firewall o
cualquier otra cosa que te ocurrió.

Al igual que con los usuarios, con el fin de agregar permisos a un grupo, se debe crear primero, y entonces usted tiene que salvar
y volver a editar el grupo.

Grupos son administrados bajo el Sistema Administrador de usuarios en la ficha Grupos. Para agregar un nuevo grupo a partir de este
pantalla, haga clic en Para editar un grupo existente, haga clic en

Al agregar un grupo, lo primero que debe hacer es darle un nombre de grupo. El nombre del grupo tiene el mismo restricciones como un nombre de usuario: Debe ser 16 caracteres o menos y sólo puede contener letras, números y un punto, guión o guión bajo.

A continuación, tiene la opción de dar al grupo una descripción para su referencia, para identificar mejor el propósito del grupo en caso de que el nombre de grupo no es suficiente.

Si ya ha definido los usuarios y desea agregarlos a este grupo, entonces usted puede utilizar el Grupo Membresías controlan para definir qué usuarios serán miembros. Para agregar un usuario a este grupo, encontramos en el lista, selecciónelo y haga clic para moverlo a la columna de los Miembros. Para eliminar un usuario de un grupo, seleccione
desde el Memberscolumn y haga clic en para moverlo a la columna de la que no son miembros.

Si va a editar un grupo existente, entonces la sección de privilegios asignados estará presente en la pantalla. Esta sección le permite agregar permisos al grupo. Vea la sección llamada "Privilegios" anteriormente en esta sección para obtener información sobre la gestión de privilegios.

Configuración

La ficha Configuración en el Administrador de usuarios le permite controlar dos cosas: ¿Cuánto tiempo de una sesión de inicio de sesión es válida,
y donde los inicios de sesión de GUI preferirán estar autenticado.

Los ajustes de tiempo de espera de sesión especifica cuánto tiempo va a durar una sesión de inicio de sesión de GUI cuando está inactivo. Este valor es
especifica en minutos, y el valor predeterminado es de cuatro horas (240 minutos). Puede introducir un valor de 0desactivar
la caducidad de sesión, por lo que las sesiones de inicio de sesión válidas para siempre, pero no recomendaría hacer esto como
que es un riesgo potencial para la seguridad.

El selector de autenticación del servidor le permite seleccionar la fuente de autenticación principal para el registro de usuarios
en el GUI. Esto puede ser un servidor RADIUS o LDAP, o el valor por defecto Base de datos local. Si el

RADIUS o LDAP servidor es inaccesible por alguna razón, la autenticación se caerá de nuevo a Local Base de datos incluso si se elige otro método. Cuando se utiliza un servidor RADIUS o LDAP, los usuarios y la pertenencia a grupos aún deben definirse en el servidor de seguridad con el fin de asignar correctamente los permisos, como no hay todavía un método para obtener permisos dinámicamente a partir de un servidor de autenticación.

Servidores de autenticación

Uso de la ficha Servidores, en Sistema Administrador de usuarios, un servidor RADIUS o LDAP puede definirse como una fuente de autenticación. Vea la sección llamada "Apoyo A lo largo de pfSense" para obtener información sobre donde estos servidores se pueden usar en pfSense actualmente. Para agregar un nuevo servidor desde esta pantalla, haga clic en 
Para editar un servidor existente, haga clic en 

RADIUS

Para agregar un servidor RADIUS para pfSense, primero llenar el campo Nombre descriptivo con el nombre de este Servidor RADIUS. Este nombre se utiliza para identificar el servidor en toda la interfaz gráfica de usuario pfSense. Hacer Asegúrese de que el servidor RADIUS tiene el firewall definido como un cliente antes de intentar ajustar los valores en esta página.

Desde el campo Tipo, seleccione RADIUS. Las configuración del servidor RADIUS se mostrará.

La primera de estas opciones, el nombre de host o dirección IP, es la dirección del servidor RADIUS. Esto puede ser un nombre completo de dominio, una dirección IP IPv4 o una dirección IPv6 IP.

El secreto compartido es la contraseña establecida para este servidor de seguridad en el software del servidor RADIUS.
El selector Servicios ofrecidos permite elegir los servicios que se ofrecen por este RADIUS servidor. Usted puede elegir Autenticación y contabilidad, sólo Autenticación, o simplemente Contabilidad. Cambiando este campo controla el cual los servicios RADIUS debe utilizar en este servidor, y controla cuál de los valores de puerto por debajo se mostrará en la página. Autenticación utilizará esta Servidor RADIUS para autenticar a los usuarios. Contabilidad enviará RADIUS arranque / parada contabilidad de paquetes los datos de las sesiones de inicio de sesión.

Si la autenticación es uno de los servicios en uso, a continuación, aparecerá el ajuste del valor de puerto de autenticación. El puerto de autenticación RADIUS predeterminada es 1812, pero si el servidor utiliza un puerto diferente, especifique que aquí.

Si la contabilidad es uno de los servicios en uso, a continuación, aparecerá el ajuste del valor del puerto de Contabilidad. La puerto de cuentas RADIUS predeterminada es 1813, pero si el servidor utiliza un puerto diferente, especifique aquí.

Haga clic en Guardar y luego este servidor estará listo para su uso.

LDAP

Para añadir un servidor LDAP para pfSense, primero llenar el campo Nombre descriptivo con el nombre de esta LDAP servidor. Este nombre se utiliza para identificar el servidor en toda la interfaz gráfica de usuario pfSense.

Desde el campo Tipo, seleccione LDAP.

La primera de estas opciones, el nombre de host o dirección IP, es la dirección del servidor LDAP. Esto puede ser una nombre completo de dominio, una dirección IP IPv4 o una dirección IPv6 IP.

El valor Port especifica en qué puerto del servidor LDAP está escuchando para las consultas LDAP. El valor por defecto Puerto TCP es 389, y para SSL es 636. Este campo se actualiza automáticamente con el valor por defecto apropiado valor basado en el transporte seleccionado a continuación.

Controles de transporte que método de transporte se utilizará para comunicarse con el servidor LDAP. La en primer lugar, y por defecto, la selección es TCP - Estándar que utiliza conexiones TCP sin formato en el puerto 389.

Una opción más segura, si su servidor LDAP soporta, es SSL - Cifrado en el puerto 636. La Opción SSL codificará las consultas LDAP realizados en el servidor, lo cual es especialmente importante si su Servidor LDAP no está en un segmento de red local. Se recomienda siempre usar SSL cuando sea posible, aunque TCP llano es más fácil de configurar y diagnosticar desde una captura de paquetes mostraría el contenido de las preguntas y las respuestas.

Si ha elegido SSL - Cifrado para el transporte, entonces usted debe seleccionar una entidad emisora de certificados Peer para validar el certificado del servidor LDAP. Si se conecta a un servidor de Active Directory, usted debe asegurarse de que la CA seleccionada coincida con el CA en Active Directory de otro modo los problemas se surgir. Vea la sección llamada "Gestión de Autoridad de certificación" para obtener más información sobre la creación o la importación de las CA.

El selector Protocol versión le permite elegir qué versión del protocolo LDAP se emplea por su servidor LDAP, ya sea 2o 3.

Búsqueda ámbito determina dónde y qué tan profundo, una búsqueda irá por un partido. En Nivel, usted puede elegir entre Una Planta o Subárbol completo para controlar la profundidad de la búsqueda irá. La Campo Base DN controla donde la búsqueda se iniciará.

Contenedores de autenticación es una lista separada por comas de los lugares potenciales de cuenta, o contenedores. Estos contenedores se antepondrá a la DN de base de búsqueda anteriores o usted puede especificar contenedor lleno camino aquí y deje en blanco el DN Base. Si su servidor LDAP soporta, y la configuración de vinculación son correcta, puede hacer clic en el botón Seleccionar para navegar contenedores del servidor LDAP y seleccionar en que uno.
Algunos ejemplos de estos recipientes serían:

- CN = Users, DC = ejemplo - Esto sería buscar los usuarios en el interior del componente de dominio ejemplo, una sintaxis común ver para Active Directory

- CN = Users, DC = ejemplo, DC = com, OU = OtherUsers, DC = ejemplo, DC = com - Esta sería buscar en dos lugares diferentes, la segunda de las cuales se limita a la OtherUsers unidad organizativa.

El cuadro Consulta Extended le permite especificar un bit adicional para consultar después de que el nombre de usuario, que le permite
para especificar una membresía de grupo para filtrar. Para definir una consulta ampliada, marque la casilla y complete la valor con algo como CN = Groupname, OU = MyGroups, DC = ejemplo.

La opción de credenciales de enlace controla cómo este cliente LDAP intentará enlazar con el servidor. Por defecto el uso anónimo se une a resolver cuadro de nombres distinguidos se comprueba para realizar un anónimo unirse. Si el servidor requiere autenticación para unirse y realizar una consulta, desactive esa casilla y luego especificar un DN de usuario y contraseña que se utilizará para el enlace.

El selector de la plantilla inicial será pre-llenar el resto de opciones de la página con los valores predeterminados comunes
para un determinado tipo de servidor LDAP. Las opciones incluyen OpenLDAP, Microsoft AD, y Novell eDirectory.

Atributo de nombre de usuario es el atributo utilizado para identificar el nombre de un usuario, por lo general cn o samAccountName.

Grupo nombrar atributo es el atributo utilizado para identificar a un grupo, como cn.

Atributo de miembro de grupo es el atributo de un usuario que significa que es el miembro de un grupo, tales como miembro, memberOf, o uniqueMember.

Haga clic en Guardar y luego este servidor estará listo para su uso.

Solución de problemas

Hay una página disponible para probar estos servidores de autenticación en el Diagnóstico Autenticación. Desde esa página, puede seleccionar el servidor de autenticación, introduzca un nombre de usuario y contraseña y, a continuación, pulse

el botón de prueba. El servidor de seguridad intentará autenticar ese usuario en el servidor especificado y devolverá el resultado. Por lo general, es mejor probar al menos una vez antes de intentar utilizar el servidor.

Si recibe un error al probar la autenticación, vuelva a comprobar la configuración del servidor, realice cualquier ajustes necesarios y vuelva a intentarlo.

Capítulo 8. Gestión de certificados

Introducción Básica a X.509 Public Key Infraestructura

Una de las opciones de autenticación para redes VPN es utilizar claves X.509. Una discusión en profundidad 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 los detalles. En este capítulo se proporciona la comprensión muy básica que necesita para crear y gestionar certificados en pfSense.

Con PKI, primero se crea una autoridad de certificación (CA). Esta CA firma entonces todos los individuos certificados en su PKI. El certificado de la CA se utiliza en los servidores y los clientes OpenVPN para verificar la autenticidad de los certificados utilizados. El certificado de la CA puede ser utilizado para verificar la firma de los certificados,
pero no para firmar los certificados. La firma de certificados requiere la clave privada de la CA. La privacidad de la CA clave privada es lo que asegura la seguridad de su PKI. Cualquier persona con acceso a la clave privada de la CA puede generar certificados para ser usados en su PKI, por lo que debe mantenerse segura. Esta clave no se distribuye
a los clientes o servidores.

Asegúrese de que usted nunca copiar más archivos a los clientes que son necesarias, ya que esto puede resultar en la seguridad de
la PKI está comprometida.

Un certificado se considera válido si ha sido confiado por una CA dada. En este caso de las VPN, esto significa que un certificado a partir de una CA específica sería considerado válido para cualquier VPN usando esa CA. Para eso es que a menudo se sugiere que se crea una entidad emisora única para cada VPN que tiene un nivel diferente de la seguridad. Por ejemplo, si tiene dos VPNs de acceso móvil con el mismo acceso a la seguridad, el uso de la misma CA para aquellos VPNs está bien. Sin embargo, si usted tiene un VPN para los usuarios y una red privada virtual para el control remoto
gestión, cada uno con diferentes restricciones, entonces usted debe utilizar un CA único para cada VPN.

Listas de revocación de certificados (CRL) son listas de certificados que han sido comprometidos o de otra manera necesitan ser invalidado. La revocación de un certificado hará que se puede considerar no es de confianza tanto tiempo como la
aplicación utilizando el CA también utiliza una CRL. CRL se generan y firmaron contra una CA utilizando su clave privada, por lo que con el fin de crear o agregar certificados a una CRL en la interfaz gráfica de usuario, que debe tener la CA de
clave privada importada en la interfaz gráfica de usuario.

Gestión de Autoridad de Certificación

Autoridades de certificación se gestionan desde System Administrador de Cert, en la ficha CA. Desde esta pantalla puede agregar, editar, exportar o eliminar las CA.

Crear una nueva autoridad de certificación

Para crear un nuevo CA, vaya a Sistema Administrador de Cert en la ficha CA. A partir de ahí, haga clic en el
para iniciar el proceso de añadir una CA.


botón

Primero, introduzca un nombre descriptivo para la CA. Esto se utiliza como una etiqueta para esta entidad emisora a lo largo de la interfaz gráfica de usuario.
¿Cómo se procede de aquí depende de qué tipo de CA que está tratando de agregar. El desplegable Método selector tiene tres opciones, cada una se describe a continuación, crear una autoridad certificadora interna, Importar un Existing Certificate Authority, y crear una Autoridad de certificación intermedia.

Crear una autoridad certificadora interna

El método más común utilizado desde aquí es crear una autoridad certificadora interna. Esta voluntad hacer una nueva emisora raíz en base a la información que introduce en esta pantalla.

El campo Longitud de la clave elige cómo "fuerte" del CA es en términos de encriptación. Cuanto más larga sea la clave, más segura es. Sin embargo, las claves más largas pueden tardar más tiempo de CPU para procesar, por lo que no siempre es aconsejable
utilizar el valor máximo. El valor por defecto de 2048 es un buen equilibrio.

El campo Lifetime especifica el número de días en que la CA será válida. La frecuencia con que desea
para hacer esto depende de sus preferencias personales y políticas del sitio. Cambio de la CA con frecuencia es más seguro, pero también es un dolor de cabeza de gestión, ya que requeriría volver a emitir nuevos certificados cuando el CA caduque. Por defecto, la interfaz gráfica de usuario sugiere el uso de 3.650 días, que es poco menos de 10 años.

La sección de nombre distinguido determina qué parámetros personalizados voy a entrar en la CA. Estos suelen ser llenado con la información de su organización, o en el caso de un individuo, su personal información. Esta información es principalmente cosméticos, y se utiliza para verificar la exactitud de la CA, y para distinguir una CA de otro. El código de país, estado o provincia, ciudad, organización y correo electrónico Dirección si todos se rellenada con sus datos. El campo Common Name (CN) es la interna
nombre que identifica a la CA. A diferencia de un certificado, el CN para una entidad emisora no tiene por qué ser el nombre de host,
ni nada específico. Por ejemplo, se le puede llamar VPNCA o MiCA. A pesar de que no se considera una inválida CN, lo mejor es evitar el uso de espacios en la NC.

Cuando haya terminado de introducir la información, pulse Guardar. Si hay algún error, como no válido caracteres u otros problemas de entrada, que se describirán en la pantalla. Corrija los errores e intentar para salvar de nuevo.

Importar una autoridad de certificación existente

Si usted tiene una CA existente de una fuente externa que tiene que importar, se puede hacer mediante la selección Método de una entidad emisora de certificados de importación existentes. Esto puede ser útil de dos maneras. Uno de ellos, de las CA
te has hecho con cualquier otro sistema, y dos, de las CA hechos por otros que tiene que confiar.

Si usted está confiando en una CA de otra fuente, sólo necesita introducir los datos de certificado para la CA. Es normalmente contenido en un archivo que termina en `. Crt.` Sería texto plano, y encerrado en un bloque, tales como:

```
----- BEGIN CERTIFICATE -----
[Un montón de datos codificados en base64-aleatorias en
busca]
----- END CERTIFICATE -----
```

Si va a importar su propia CA, o una CA hecha para usted que es capaz de generar su propia certificados y listas de revocación de certificados, también se necesitará importar la clave privada de la CA. Es normalmente en un archivo con extensión `Clave..` Sería de datos de texto sin formato encerradas en un bloque, tales como:

```
----- BEGIN RSA PRIVATE KEY -----
[Un montón de datos codificados en base64-aleatorias en
busca]
----- END RSA PRIVATE KEY -----
```

Si ha importado la clave privada de la CA, es esencial que usted entra en el serial para el próximo valor certificado. Una CA creará certificados, cada uno con un número de serie único en secuencia. Este valor controla qué la serie será para el siguiente certificado generado de esta CA. Es esencial que cada certificado tener una serie único, o tendrá problemas en el futuro con la revocación del certificado. Si usted no sabe lo que debería ser la próxima serie, intento de estimar el número de certificados se han hecho a partir de la CA y, a continuación, establecer el número lo suficientemente alto que no debería haber una colisión.

Crear una Autoridad de certificación intermedia

Una CA intermedia le permitirá crear una nueva emisora que es capaz de generar los certificados, pero depende en otra CA más alta por encima de ella. Para crear una, seleccione Crear una Autoridad de certificación intermedia desde el menú desplegable Método. Usted puede elegir la CA de nivel superior para firmar el certificado de esta CA mediante
Firmar el desplegable autoridad de certificación. Sólo las entidades emisoras de certificados con claves presentes se le aparecen, ya que es
obligados a firmar correctamente este nuevo CA. El resto de parámetros para la creación de esta CA son idénticos a aquellos para Crear una autoridad certificadora interna.

Edición de una entidad emisora de certificados

Después de una CA se ha añadido, se puede editar de la lista de entidades emisoras de encontrar en Sistema Cert Gerente
en la pestaña de las CA. Para editar una CA, haga clic en el botónpara al final de su fila. La pantalla presenta permite editar los campos como si fuese importado la AC. Para obtener información sobre los campos de esta pantalla, consulte la sección llamada "una entidad emisora de certificados de importación existentes". En la mayoría de los casos el objetivo de esta pantalla
sería para corregir serie de la CA, si es necesario utilizar la serie para la próxima entrada de certificado, o añadir una clave
a un CA importado por lo que se puede utilizar para crear y firmar certificados y CRLs. Una vez que haya ajustado los ajustes que necesita, haga clic en Guardar.

Exportación de una entidad emisora de certificados

En la lista de entidades de certificación en el Sistema de Administrador de Cert en la ficha AC, también puede exportar el certificado de un CA
y o / privado. En la mayoría de los casos usted no quiere exportar la clave privada de un CA, a menos que
se mueve el CA a una nueva ubicación, o hacer una copia de seguridad. Cuando se utiliza la CA para una VPN o más otros fines, sólo es necesario exportar el certificado de la CA. Si la clave privada de la CA se mete en el mal
las manos, la otra parte podría generar nuevos certificados que serían considerados válidos en contra de la CA.

Para exportar el certificado de la CA, haga clic botón en la izquierda. Para exportar la clave privada de la CA, haga clic en el botón en la derecha. Para confirmar que desea exportar el archivo adecuado, pasa el ratón por encima del botón y una información sobre herramientas mostrará la acción a realizar. Los archivos se descargarán con el descriptivo CA nombre que el nombre de archivo y la extensión `. Crt` para el certificado, y `Clave.` para la clave privada.

Quitar una entidad emisora de certificados

Para eliminar una CA, primero debe ser eliminado de su uso activo. Si se está utilizando por una VPN u otro subsistema, debe ser retirado de allí. Luego, visite System Administrador de Cert en la ficha CA. Encontrar

la CA en la lista, haga clic en el botón y, a continuación, haga clic en Aceptar en el cuadro de diálogo de confirmación. Si recibe un
error, siga las instrucciones que aparecen en pantalla para corregir el problema y vuelva a intentarlo.

Gestión de Certificados

Los certificados se gestionan desde System Cert Manager, en la ficha Certificados. Desde esta pantalla puede agregar, editar, exportar o eliminar certificados.

Crear un nuevo certificado

Para crear un nuevo certificado, vaya a Sistema Administrador de Cert en la ficha Certificados. A partir de ahí, haga clic en
la botón para iniciar el proceso de añadir un certificado.

Primero, introduzca un nombre descriptivo para el certificado. Esto se utiliza como una etiqueta para esta entidad emisora en todo el
GUI. ¿Cómo se procede de aquí depende de qué tipo de certificado que está tratando de agregar. El Método selector desplegable tiene tres opciones, cada una se describe a continuación, Importar un certificado existente, Crear Certificado Interna y Creación de una solicitud de firma de certificado.

Importar un certificado existente

Si usted tiene un certificado existente a partir de una fuente externa que necesita importar, puede ser realizado por Selección del método de importación un certificado existente. Esto puede ser útil para los certificados que tenga hecho por sí mismo utilizando otro sistema, o para los certificados que se han proporcionado a usted por un tercero.

Es preciso entrar en tanto los datos del certificado y los datos de la clave privada del certificado. Para comenzar, ingrese el
Datos del certificado. Por lo general está contenido en un archivo que termina en `. Crt.` Sería texto plano, y cerrado en un bloque, tales como:

```
----- BEGIN CERTIFICATE -----
[Un montón de datos codificados en base64-aleatorias en
busca]
----- END CERTIFICATE -----
```

A continuación, debe importar los datos claves privadas. Esto es por lo general en un archivo con extensión `Clave..` Sería
datos de texto sin formato encerradas en un bloque, tales como:

```
----- BEGIN RSA PRIVATE KEY -----
[Un montón de datos codificados en base64-aleatorias en
busca]
----- END RSA PRIVATE KEY -----
```

Haga clic en Guardar para finalizar el proceso de importación. Si se encuentran errores, siga las instrucciones que aparecen en pantalla
para resolverlos. El error más común es no pegando en la parte derecha del certificado o privada
clave. Asegúrese de incluir toda la manzana, incluyendo la cabecera que comienza y termina el pie alrededor
los datos codificados.

Crear un Certificado Interna

El método más común utilizado de aquí es crear un certificado interno. Esto hará que un nuevo
certificado mediante una de sus autoridades de certificación existentes.

En primer lugar, seleccione la entidad emisora de certificados por los que se firmará este certificado. Sólo una CA que tiene una
presente la clave privada puede estar en esta lista, ya que se requiere la clave privada para que la CA para firmar un certificado.

El campo Longitud de la clave elige cómo "fuerte" el certificado es en términos de encriptación. Cuanto más tiempo la clave, más segura es. Sin embargo, las claves más largas pueden tardar más tiempo de CPU para procesar, por lo que no siempre es
aconsejable utilizar el valor máximo. El valor por defecto de 2048 es un buen equilibrio.

El campo Tipo de Certificado le permite establecer el propósito de este certificado. Si el certificado se utiliza en una Servidor VPN o un servidor HTTPS, seleccione Certificado de servidor. Esto indica dentro del certificado que fuere ser usado en una función de servidor, y ningún otro. Si se elige un certificado de usuario, el certificado puede ser utilizado en un extremo-
la capacidad del usuario, tal como un cliente de VPN, pero no se puede utilizar como un servidor. Esto evita que un usuario utilice
su propio certificado de hacerse pasar por un servidor. Ni el certificado de servidor, ni certificado de usuario puede ser utilizado para crear certificados adicionales. Si desea crear una CA intermedia, elija Certificado Autoridad. Un certificado generado de esta manera estará subordinada a la CA elegida. Puede crear su propio certificados, pero la CA raíz también deben ser incluidos cuando se utiliza. Esto también se conoce como "encadenamiento".

El campo Lifetime especifica el número de días en que el certificado será válido. ¿Con qué frecuencia
que quieres hacer esto depende de sus preferencias personales y políticas del sitio. Cambio del certificado
con frecuencia es más seguro, pero también es un dolor de cabeza de gestión, ya que requeriría volver a emitir una nueva certificado cuando el certificado caduque. Por defecto, la interfaz gráfica de usuario sugiere el uso de 3.650 días, lo que es poco menos de 10 años.

La sección de nombre distinguido determina qué parámetros personalizados voy a entrar en el certificado.
La mayoría de estos campos se rellena previamente con datos de la CA. Estos suelen ser llenados con su información de la organización, o en el caso de un individuo, su información personal. Esta información
es sobre todo estética, y se utiliza para verificar la exactitud del certificado, y para distinguir un certificado de otro. El código de país, estado o provincia, ciudad, Organización y Dirección de correo electrónico todos debemos cumplimentar con sus datos. El campo Common Name (CN) es el nombre interno que identifica
el certificado. A diferencia de una CA, el CN del certificado debe ser un nombre de usuario o nombre de host. Por ejemplo,
se puede llamar así VPNCert, user01, o vpnrouter.example.com. Aunque no se considera
un CN no válida, es mejor evitar el uso de espacios en la NC.

Si el certificado tiene varios nombres que deberían ser válidos para el CN, por ejemplo, dos nombres de host diferentes, un
adicional de dirección IP, una dirección URL o una dirección de correo electrónico, estos pueden ser administrados bajo los nombres alternativos. Si
usted no sabe lo que para ingresar en este campo, que probablemente se dejará en blanco. Para agregar una nueva alternativa
un
Nombre, haga clic en y luego aparecerá una fila con un tipo y campo Valor. El campo Type debe contener uno de DNS (FQDN o nombre de host), IP (Dirección IP), URI, o de correo electrónico. el campo de valor debe contener

valor con el formato correcto basado en el tipo entró. Si decide que no es necesario una fila, se puede ser eliminado haciendo clic en el al final de la fila.

Cuando haya terminado de introducir la información, pulse Guardar. Si hay algún error, como no válido caracteres u otros problemas de entrada, que se describirán en la pantalla. Corrija los errores e intentar para salvar de nuevo.

Crear una solicitud de firma de certificado

Una solicitud de firma de certificado le permitirá crear un nuevo archivo de solicitud que puede ser enviada a un tercero CA para ser firmado. Esto se usaría si usted desea obtener un certificado de un certificado raíz de confianza. A crear uno, seleccione Certificado de solicitud de firma de la lista desplegable Método. Los parámetros restantes para la creación de este certificado son idénticos a aquellos para crear un certificado interno.

Exportación de un certificado

En la lista de certificados de Sistema Cert Manager en la ficha Certificados, también puedes exportar una certificado y / o de su clave privada. Para exportar el certificado, haga clic en el botón en la izquierda. Para exportar el la clave privada del certificado, haga clic en el botón en la medio. Para exportar el certificado y su clave privada juntos en un archivo PKCS # 12, haga clic en el botónpara derecha. Para confirmar que está exportando el correcto archivo, sitúe el puntero del ratón sobre el botón y una información sobre herramientas mostrará la acción a realizar. Los archivos descargará con el nombre descriptivo del certificado como nombre de archivo y la extensión `. Crt` para la y certificado `Clave.` para la clave privada, o `. P12` para un archivo PKCS # 12.

Quitar un certificado

Para eliminar un certificado, primero debe ser eliminado de su uso activo. Si se está utilizando por una VPN u otro subsistema, debe ser retirado de allí. Luego, visite System Cert Manager en los Certificados tab. Encuentre el certificado en la lista, haga clic en el botónpara y, a continuación, haga clic en Aceptar en el cuadro de diálogo de confirmación.
Si recibe un error, siga las instrucciones que aparecen en pantalla para corregir el problema y vuelva a intentarlo.

Los certificados de usuario

Si una VPN está siendo utilizado que requiere certificados de usuario, que se pueden crear en uno de varios, dependiendo en donde se realiza la autenticación de la VPN y estén o no el certificado existe.

Si no hay ninguna autenticación de usuario, o si la autenticación de usuario se está haciendo en un servidor externo (RADIUS, LDAP, etc), entonces usted puede hacer un certificado de usuario al igual que cualquier otro certificado descrito anterior. Asegúrese de seleccionar un certificado de usuario para el Certificado de Tipo, y se establece el nombre común ser el nombre del usuario.

Si la autenticación de usuario se está realizando en pfSense, el certificado de usuario se puede hacer dentro de el Administrador de usuarios (Sistema Administrador de usuarios) al crear el usuario. En su interior, agregar un nuevo usuario, rellenar el nombre de usuario y contraseña, y en la sección Certificados de usuario, seleccione Haga clic aquí para crear un usuario certificado. Esto le mostrará una forma sencilla de crear un certificado de usuario. Introduzca una breve nombre descriptivo, puede ser el nombre de usuario o algo tal como Acceso remoto de VPN Bob Cert. Elija el Certificado de autoridad adecuada para la VPN. La Longitud de la clave y de por vida también se pueden ajustar si es necesario.
Al guardar el usuario, un certificado será generado por ellos.

Para agregar un certificado para un usuario existente, edite el usuario, encontrar los certificados de usuario y haga clic en. A partir de ahí usted puede elegir cualquiera de las otras opciones disponibles en el proceso de creación del certificado se describe en la sección "Crear un nuevo certificado", o también puede elegir un certificado existente para crear una asociación entre el usuario y un certificado que ya existe.

Para obtener más información sobre cómo agregar y administrar usuarios, consulte el Capítulo 7, Gestión y usuario Autenticación.

Gestión de listas de revocación de certificados

Listas de revocación de certificados (CRL) son una parte del sistema X.509 que le permiten publicar una lista de los certificados que ya no se debe confiar. Estos certificados pueden haber sido comprometidas o de lo contrario deben ser invalidadas. Una aplicación que utiliza una CA, como OpenVPN también debe usar un CRL, por lo que puede comprobar la conexión de los certificados de clientes. Una CRL es generado y firmado en contra de una CA
utilizando su clave privada, por lo que con el fin de crear o agregar certificados a una CRL en la interfaz gráfica de usuario, debe tener la
clave privada de la CA importados en la interfaz gráfica de usuario. Si la gestión del CA externa y no tiene la La clave privada de CA en el servidor de seguridad, aún puede importar una CRL genera fuera del firewall. La forma tradicional de usar una CRL es sólo para tener una CRL por CA y sólo añadir certificados no válidos para que el CRL. En pfSense, sin embargo, se pueden crear varias listas CRL para una sola CA, pero sólo una CRL puede ser elegido para una instancia de VPN. Esto podría ser utilizado, por ejemplo, para evitar un certificado específico se conecten a una instancia al tiempo que permite que se conecte a otro.

Listas de revocación de certificados se gestionan desde System Cert Manager, en la revocación de certificados tab. Desde esta pantalla, puede agregar, editar, exportar o eliminar entradas de CRL. La lista mostrará todos los de su Autoridades de certificación y una opción para agregar una CRL. La pantalla también indica si el LCR interna o externa (importado), y muestra un recuento de la cantidad de certificados han sido revocados en cada CRL.

Crear una nueva lista de revocación de certificados

Para crear una nueva CRL, busque la fila con la CA que el CRL se creará, a continuación, haga clic en  en el final de la fila.

En la siguiente pantalla, para elegir el método Crear una revocación de certificados interna Lista.

Introduzca un nombre descriptivo para la CRL, que se utiliza para identificar esta CRL en las listas de todo el GUI. Es normalmente es mejor incluir una referencia al nombre de la entidad emisora y / o finalidad de la CRL en este nombre.

En el menú desplegable de autoridad de certificación, asegúrese de que está seleccionada la CA adecuada.

En el cuadro de por vida, introduzca el tiempo que desea que el CRL sea válida. El valor predeterminado es 9999 día, o casi 27 años y medio.

Ahora haga clic en Guardar y volverá a la lista CRL, y la nueva entrada se le mostrará allí.

Importar una lista de revocación de certificado existente

Para importar una CRL de una fuente externa, busque la fila con la CA que se importará el CRL

para, a continuación, al final de la fila.
haga clic en
En la siguiente pantalla, para elegir el método Importar una revocación de certificados existente Lista.

Introduzca un nombre descriptivo para la CRL, que se utiliza para identificar esta CRL en las listas de todo el GUI. Es normalmente es mejor incluir una referencia al nombre de la entidad emisora y / o finalidad de la CRL en este nombre.

En el menú desplegable de autoridad de certificación, asegúrese de que está seleccionada la CA adecuada.

A continuación, debe importar los datos de CRL. Esto es por lo general en un archivo con extensión `. Crl.` Sería sencillo
datos de texto encerradas en un bloque, tales como:

```
----- BEGIN CRL X509 -----
```

```
[Un montón de datos codificados en base64-aleatorias en
busca]
----- END X509 CRL -----
```

Haga clic en Guardar para finalizar el proceso de importación. Si se encuentran errores, siga las instrucciones que aparecen en pantalla
para resolverlos. El error más común es no pegando en la parte derecha de la CRL. Asegúrese de que
incluir toda la manzana, incluyendo la cabecera que comienza y termina el pie alrededor de los datos codificados.

Exportar una lista de certificados revocados

En la lista de CRL en Sistema Cert Manager en la pestaña de revocación de certificados, también puede

exportar una CRL. Para exportar la CRL, haga clic en el botón. El archivo se descargará con el descriptivo CRL
nombre que el nombre de archivo y la extensión `. Crl.`

Eliminación de una lista de certificados revocados

Para eliminar una CRL, primero debe ser eliminado de su uso activo. Si se está utilizando por una VPN u otro subsistema, debe ser retirado de allí. Luego, visite System Administrador de Cert en el Certificado

Ficha Revocación. Encuentra la CRL en la lista, haga clic en el botónpara y, a continuación, haga clic en Aceptar en la confirmación de
diálogo. Si recibe un error, siga las instrucciones que aparecen en pantalla para corregir el problema y vuelva a intentar de nuevo.

Revocar un Certificado

Una CRL no es muy útil a menos que haya revocado certificados enumerados. Un certificado es revocado por la adición de la
certificado a una CRL, y hacer de esto, editar una CRL interna haciendo clic. Se presentará una pantalla
que enumera todos los certificados revocados en la actualidad, y un control para agregar otros nuevos.

En esta pantalla, hay una lista desplegable etiquetada Elige un Certificado a revocar y esta lista contiene
todos los certificados que se sabe que el servidor de seguridad para la entidad emisora que utiliza esta CRL. Seleccione el certificado que
desee revocar de esta lista.

El campo Reason le permite indicar qué se va a revocar un certificado. Esta información no
afectará a la validez del certificado es simplemente de carácter informativo. Usted puede seleccionar cualquiera de los valores de la lista, si se aplican, o dejarlo en el predeterminado.

Haga clic en Agregar y en el certificado se agregará a la CRL.

Puede eliminar un certificado de la CRL desde esta pantalla también. Encuentra el certificado en la lista y

haga clic en ebotón para quitarla de la CRL.

Después de añadir o retirar un certificado, el CRL será re-escrito si está actualmente en uso por cualquier
Instancias de OpenVPN para que los cambios de CRL serán inmediatamente activa.

Actualización de una lista importada de revocación de certificados

Para actualizar una CRL importado, búsquelo en la lista y haga clic enheat al final de su fila. A continuación, puede borrar el contenido pegado en el cuadro de datos de CRL y reemplazarlo con el contenido de la nueva CRL, y pulse Guardar.

Después de actualizar la CRL importado, será re-escrito si está actualmente en uso por cualquier OpenVPN
casos de manera que los cambios CRL serán inmediatamente activa.

Importar desde EasyRSA

En pfSense 1.2.3, los certificados no podían ser gestionados desde la interfaz gráfica de usuario por lo que había recomendado la creación
y la gestión de una estructura de certificado en EasyRSA. En pfSense 2.x, es mucho más fácil de manejar

certificados de la interfaz gráfica de usuario, y estos serán respaldados y restaurados en la configuración por lo que es también más seguro. Así
qué hacer si se actualiza? Cuando se actualiza de 1.2.3 a 2.0 el proceso de actualización importará su certificado existente CA (s), y los certificados introducidos en las cajas de los OpenVPN clientes / servidores.
No va a importar la clave de CA o certificados para los clientes de acceso remoto porque los que no se almacenaron en la configuración en cualquier lugar .. Si ha seguido el viejo EasyRSA cómo-a éstos todavía deben estar en las llaves antiguas
carpeta debe estar bajo `/ root/easyrsa4pfsense/keys.`
Si esa carpeta no está y usted no tiene una copia de seguridad, entonces no hay manera de generar nuevos certificados de esta CA. Si usted tiene estos archivos respaldados en algún lugar, busque la copia de seguridad de los archivos. Suponiendo que el
archivos están presentes, accede a la cubierta, a continuación, ejecute:

```
# Cat / root/easyrsa4pfsense/keys/ca.key
----- BEGIN RSA PRIVATE KEY -----
[...]
----- END RSA PRIVATE KEY -----
```

Que le mostrará la tecla CA existente. Luego, desde la GUI, vaya a Sistema □ Cert Manager, encontrar el

importados CA y haga clic en el botónpara tocar el tema. Copiar / pegar la clave (incluyendo el BEGIN / END líneas) en el campo de datos de la clave privada en la interfaz gráfica de usuario. Ajuste el nombre descriptivo si quieres, probablemente
tiene un nombre genérico del proceso de actualización. No pulse Guardar todavía.

Tenemos que averiguar lo que debería ser el número de serie para la siguiente certificado. Esto se puede encontrar en ejecutar este comando desde el shell:

```
# Printf "% d \ n" 0x `cat / root/easyrsa4pfsense/keys/serial`
```

Eso debería devolver un número decimal, como 11, que es el número de serie del certificado siguiente a hacer. Copie ese número en la interfaz gráfica de usuario en el campo de serie, haga clic en Guardar. Es importante que usted
corregir el número de serie, de lo contrario usted puede terminar para arriba con dos certificados que tienen el mismo serial
número, lo que dará lugar a problemas con la revocación de la carretera. Los certificados son revocados por serie, dos certs con el mismo serial ambos serían revocados si usted revoca cualquiera de ellos.
En ese punto, usted debe ser capaz de crear nuevos certificados en la ficha Certificados del Administrador de Cert en la interfaz gráfica de usuario que utiliza este CA.

Cualquier certificado para que CA en el GUI también deben presentarse para su uso dentro del OpenVPN Client Exportación
paquete. Si desea que sus viejos / certificados preexistentes en aparecer ahí, puede importarlos desde EasyRSA también. En la pestaña Certificados, haga clic en. En Método, elija Importar una existente certificado. Agregar un nombre descriptivo (como el nombre del certificado). Ahora para obtener ese certificado, y tecla, volver a la shell y encontrar la llave en / Root/easyrsa4pfsense/keys /. Por ejemplo:

```
# Cd / root/easyrsa4pfsense/keys /
# ls-l probador *
-Rw-r - r - 1 root personal de 3739 03 de febrero 2010
tester.crt
-Rw-r - r - 1 root personal 688 03 de febrero 2010 tester.csr
-Rw ------- 1 root personal 887 03 de febrero 2010 tester.key
```

A continuación, puede gato la `. Crt` y `Clave.` archivos, y copiar el bloque. / END BEGIN / .. que incluye el versión codificada en el lugar adecuado en la interfaz, haga clic en Guardar.

Repita este último proceso para cada tecla que desea importar y, a continuación, todos ellos deben estar en la interfaz gráfica de usuario como
así. No se requiere que usted tiene los certificados de usuario en la interfaz gráfica de usuario para que los clientes se conecten;
Sólo necesitan estar allí para su uso con el paquete OpenVPN Client Export.

Capítulo 9. Backup y recuperación

Gracias al archivo de configuración basado en XML utilizado por pfSense, las copias de seguridad son una brisa. Todos los ajustes para que el sistema se llevan a cabo en un solo archivo (consulte la sección "Archivo XML de configuración de pfSense"). En la gran mayoría de los casos, este archivo se puede utilizar para restaurar un sistema a un estado completamente de trabajo idéntico a lo que se estaba ejecutando anteriormente. No hay necesidad de hacer una copia de seguridad de todo el sistema, como la los archivos del sistema de base no son modificados por una normal, funcionamiento, sistema. La única excepción es el caso de algunos paquetes, tales como FreeSWITCH, que contienen los datos fuera del archivo de configuración.

Estrategias de respaldo

Lo más recomendable es hacer una copia de seguridad después de cada cambio de menor importancia, y antes y después de cada gran el cambio (o serie de cambios). Por lo general, se toma una copia de seguridad inicial en caso de que se realice el cambio tiene efectos indeseables. Una copia de seguridad después de los hechos se toma después de evaluar el cambio y asegurando que tenido el resultado previsto. Copias de seguridad periódicas también se ser útiles, independientemente de los cambios, especialmente en los casos en que una copia de seguridad manual se pueden perder por una razón u otra.

pfSense hace una copia de seguridad interna en cada cambio, y que es una buena idea para descargar uno manual así. Las copias de seguridad automáticas realizadas en cada cambio son buenos para volver a las configuraciones anteriores después de esos cambios han demostrado ser perjudiciales, pero no son buenas para la recuperación de desastres ya que están en el sistema sí mismo y no guardaste el exterior. Como es un proceso bastante sencillo y sin dolor, debe ser fácil de hacer una hábito de la descarga de una copia de seguridad de vez en cuando, y mantenerlo en un lugar seguro. Si dispone de una suscripción en portal.pfsense.org [https://portal.pfsense.org], las copias de seguridad se pueden manejar fácilmente y de forma automática para usted.

Si realiza cambios en los archivos del sistema, como los parches personalizados o modificación de los códigos, debe recuerde hacer una copia de estos cambios con la mano o con el paquete de copia de seguridad se describe en la sección llamada "Los archivos de copia de seguridad y directorios con el paquete de copia de seguridad", ya que no se realizará una copia de seguridad o restauración de el sistema de copia de seguridad integrada. Esto incluye modificaciones a los archivos de sistema mencionados en otras partes del libro, tal como `/ boot / device.hints, / boot / loader.conf, / etc / sysctl.conf,` y otros.

Además de hacer copias de seguridad, también debe probarlos. Antes de la colocación de 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 tratar algunos de los 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 probar periódicamente las copias de seguridad en un equipo ajeno a la producción o de la máquina virtual. La única cosa peor que una copia de seguridad que falta es una copia de seguridad inutilizable!

En pfSense 1.2.x, los datos gráficos RRD, ubicados en `/ Var / db / rrd,` no está respaldada por ninguna de las acciones los procesos de copia de seguridad. Este problema se solucionará en la próxima versión, donde los datos RRD pueden ser considerados en el XML copia de seguridad del archivo de configuración, pero esto todavía no puede ser conveniente para algunas personas debido al aumento de tamaño esto trae. Hay otras maneras de asegurar que estos datos se copia de seguridad, sin embargo. Vea la sección llamada "Los archivos y directorios de copia de seguridad con el paquete de copia de seguridad" más adelante en este capítulo.

Hacer copias de seguridad de los WebGUI

Hacer una copia de seguridad en el WebGUI es bastante simple. Sólo tienes que visitar Diagnóstico Backup / Restore. En el Sección de configuración de copia de seguridad de la página, asegúrese de que el Área de copia de seguridad está establecido en TODOS, (La opción predeterminada) a continuación, haga clic en Descargar Configuración (Figura 9.1, "Copia de seguridad WebGUI").

Figura 9.1. WebGUI de copia de seguridad

Su navegador web entonces pedirá que guarde el archivo en algún lugar del ordenador que esté utilizando para ver el WebGUI. Será nombrado `config-<hostname> -. <timestamp> xml,` pero eso se puede cambiar antes de guardar el archivo.

Usando el paquete AutoConfigBackup

Suscriptores sobre portal.pfsense.org [https://portal.pfsense.org] tener acceso a nuestra Automático Servicio de copia de seguridad de configuración, AutoConfigBackup. La información más actualizada sobre AutoConfigBackup se puede encontrar en el sitio de documentación de pfSense. [Http://doc.pfsense.org/index.php / AutoConfigBackup]

Funcionalidad y Beneficios

Cuando se realiza un cambio en la configuración, se cifra automáticamente con la frase de contraseña entrado en su configuración, y subido a través de HTTPS a nuestro servidor. Configuraciones Sólo cifrados se conservan en nuestro servidor. Esto le da instantánea de copia de seguridad, seguro fuera del sitio de su cortafuegos con ningún usuario intervención.

pfSense Compatibilidad de versiones

El paquete AutoConfigBackup trabajará con pfSense 1.2-RELEASE y todas las versiones posteriores incluyendo 2,0.

Nota

Hay una advertencia para el uso de este paquete en pfSense 1.2 - la única manera en que podíamos empatar el copia de seguridad automática en 1,2 liberación es desencadenarla sobre cada recarga filtro. La mayor página de guarda dará lugar a una recarga de filtro, pero no todos.

Instalación y Configuración

Para instalar el paquete, visite System Paquetes y haga clic thenext al AutoConfigBackup paquete. Se descarga e instala el paquete. Luego haga clic en el logotipo de pfSense en la parte superior de la página, que volverá a la primera página, y refrescar sus menús. A continuación encontrará AutoConfigBackup en el menú Diagnósticos.

Configuración del nombre de host

Asegúrese de tener un nombre de host único y dominio establecido en el Sistema La página de configuración general. La
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 va a respaldar tiene un FQDN único, de lo contrario el sistema no puede
diferenciar entre múltiples instalaciones.

Configuración AutoConfigBackup

El servicio se configura en Diagnósticos AutoConfigBackup. En la ficha Configuración, introduzca su
portal.pfsense.org nombre de usuario y contraseña, e introduzca una contraseña de cifrado. Usted debe usar un largo,
contraseña compleja para asegurar que su configuración es segura. Para su seguridad, conservamos sólo cifrada
configuraciones que son inútiles sin la contraseña de cifrado.

> **Nota**
>
> Es muy importante almacenar esta clave de cifrado en algún lugar fuera de su firewall - si pierde
> ella, no será posible restaurar la configuración si se pierde el disco duro en el servidor de seguridad.

La funcionalidad de copia de seguridad de Pruebas

Hacer un cambio de forzar una copia de seguridad de configuración, como editar y guardar un firewall o regla NAT,
haga clic en Aplicar cambios. Visita de los diagnósticos Pantalla AutoConfigBackup, y se le mostrará la
Ficha Restaurar, que enumerará las copias de seguridad disponibles, junto con la página que realiza el cambio (donde
disponible).

Copias de seguridad manuales Up

A veces, es posible que desee forzar una copia de seguridad de su configuración. Usted puede hacer esto en la pestaña Restaurar
de la página AutoConfigBackup haciendo clic en el botón Copia de seguridad ahora en la parte inferior. Esto hará que aparezca
un cuadro en el que puede introducir manualmente una descripción de la copia de seguridad. Es posible que desee hacer esto antes
hacer una serie de cambios significativos, ya que le dejan con una copia de seguridad que muestra específicamente la
razón de la copia de seguridad, que a su vez hace que sea fácil para volver a la configuración antes de iniciar la
cambios. Debido a que cada cambio de configuración desencadena una copia de seguridad, cuando usted hace una serie de cambios que
puede ser difícil saber por dónde empezar si necesita revertir. O puede que desee de forma manual
copia de seguridad antes de actualizar a una nueva versión pfSense, y el nombre de la copia de seguridad por lo que es claro que es la razón
usted hizo la copia de seguridad.

Restauración de su configuración

Para restaurar una configuración, haga clic en el botón a la derecha de la configuración como se muestra en la
Diagnóstico AutoConfigBackup pantalla en la ficha Restaurar. Se descargará la configuración
especificada de nuestro servidor, descifrarlo con su clave de encriptación, y restaurarlo. De forma predeterminada,
no se reiniciará. En función de los elementos de configuración restauradas, un reinicio puede no ser necesario. Para
ejemplo, las reglas del firewall y NAT se vuelve a cargar automáticamente después de la restauración de una
configuración. Después
restaurar, se le pedirá si desea reiniciar el sistema. Si su configuración restaurada cambia nada
aparte de NAT y las reglas del cortafuegos, debe elegir Sí.

Restauración de metal desnudo

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

1. Instale pfSense en el nuevo disco duro.
2. Abra LAN y WAN, y asignar el nombre de host y de dominio exactamente lo mismo que lo que era antes configurado.

3. Instale el paquete AutoConfigBackup.

4. Configure el paquete AutoConfigBackup como se describió anteriormente, la utilización de su cuenta de portal y la misma contraseña de cifrado tal como se utiliza anteriormente.

5. Visita la ficha Restaurar y seleccione la configuración que desea restaurar.

6. Cuando se le pida que reinicie después de la restauración, que lo
hagan.
Ahora estará de nuevo al estado de su servidor de seguridad a partir del último cambio de configuración.

Comprobación del estado AutoConfigBackup

Usted puede comprobar el éxito de una AutoConfigBackup ejecutar mediante la revisión de la lista de copias de seguridad que aparece en
en la ficha Restaurar. Esta lista se extrae de nuestros servidores - si está en la lista la copia de seguridad allí, fue exitosamente
creado.
Si falla una copia de seguridad, una alerta se registra, y verá que el desplazamiento en la parte superior de la interfaz web.

Técnicas de Backup Remoto Alternos

Las siguientes técnicas también pueden utilizarse para realizar copias de seguridad de forma remota, pero cada método tiene sus
problemas de seguridad propios que pueden descartar su uso en muchos lugares. Para empezar, estas técnicas no encriptan la configuración, que puede contener información sensible. Esto puede resultar en la configuración que se transmite a través de un enlace inseguro en el claro. Si tiene que usar uno de estos técnicas, lo mejor es hacerlo desde un enlace no WAN (LAN, DMZ, etc) oa través de una VPN. El acceso a la medios de almacenamiento que sostienen la copia de seguridad también deben ser controlados, si no cifrada. El AutoConfigBackup
paquete es un medio de la automatización de copias de seguridad remotas mucho más fácil y más seguro.

Tire con wget

La configuración puede ser recuperada desde un sistema remoto mediante el uso wget, y podría ser con guión con la cron o por algunos otros medios. Incluso cuando se utiliza HTTPS, esto no es un modo de transporte realmente segura desde
cheques certificados está deshabilitada para acomodar los certificados con firma, permitiendo hombre en el medio ataques. Al ejecutar las copias de seguridad con wget a través de redes no seguras, debe utilizar HTTPS con un certificado que puede ser verificada por wget.

Para un router que ejecuta HTTPS con un certificado auto-firmado, el comando sería algo así como
como esta:

```
#wget-q - no-check-certificado - post-data 'Enviar = descarga' \
    https://admin:pfsense @ 192.168.1.1/diag_backup.php \
    -O config-hostname-`date +% Y% m% d% H% M% S`. Xml
```

Para un router que ejecuta HTTP regular, el comando sería:

```
#wget-q - post-data 'Enviar = descarga' \
    http://admin:pfsense @ 192.168.1.1/diag_backup.php \
    -O config-hostname-`date +% Y% m% d% H% M% S`. Xml
```

En ambos casos, reemplace el nombre de usuario y contraseña con los suyos, y la dirección IP haría
sea el que sea la dirección IP se puede acceder desde el sistema de realización de la copia de seguridad. El sistema de rendimiento
la copia de seguridad también tendrá acceso a la WebGUI, para ajustar las reglas de firewall en consecuencia. Realización
esto a través de WAN, no se recomienda, como mínimo se debe utilizar HTTPS, y restringir el acceso a WebGUI a un conjunto de confianza de IPs públicas. Es preferible hacer esto a través de VPN.

Empuje con SCP

La configuración también puede ser empujado desde el cuadro de pfSense a otro sistema UNIX con scp. Uso
scp para empujar una copia de seguridad de una sola vez con la mano puede ser útil, pero usarlo de forma automatizada lleva

algunos riesgos. La línea de comandos para scp variará en gran medida dependiendo de la configuración del sistema, pero pueden ser:

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

Con el fin de impulsar la configuración de manera automática lo que se necesita para generar una clave SSH sin una contraseña. Debido a la naturaleza insegura de una tecla sin una frase de paso, la generación de una clave tales se deja como ejercicio para el lector. Esto añade un cierto riesgo debido al hecho de que cualquier persona con acceso a dicha archivo tiene acceso a la cuenta designada, sin embargo debido a que la clave se guarda en el servidor de seguridad, donde el acceso está muy restringido, no es un riesgo considerable en la mayoría de los escenarios. Si usted hace esto, asegúrese de que el usuario remoto está aislado y tiene poco o nada de privilegios en el sistema de destino. Un entorno chroot podrá SCP ser deseable en este caso. Consulte la scponly shell disponible para la mayoría de las plataformas UNIX que permite SCP presentar copias pero niega las capacidades de inicio de sesión interactivo. Algunas versiones de OpenSSH tiene soporte chroot incorporado para sftp (Secure FTP). Estas medidas limitan en gran medida el riesgo de compromiso con respecto a la servidor remoto, pero aún deja tus datos de copia de seguridad en riesgo. Una vez que se configura el acceso, un cron entrada podría ser añadido al sistema de pfSense para invocar scp. Para más información, visita el Wiki de documentación pfSense o buscar en los foros.

Copia de seguridad básica de SSH

Similar a la copia de seguridad SCP, hay otro método que funcione de un sistema UNIX a otro. Este método no invoca la capa SCP / SFTP, que en algunos casos puede no funcionar correctamente si un sistema ya está en un estado no.

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

Cuando se ejecuta, este comando producirá un archivo llamado `backup.xml` en el directorio de trabajo actual que contiene la configuración del sistema pfSense remoto. La automatización de este método utilizando cron es también posible, pero este método requiere una clave SSH sin como frase de contraseña en el host de realizar la copia de seguridad. Esta clave le permitirá el acceso administrativo a su servidor de seguridad, por lo que debe ser estrechamente controlada. (Vea el sección llamada "Secure Shell (SSH)" para obtener más información de configuración SSH.)

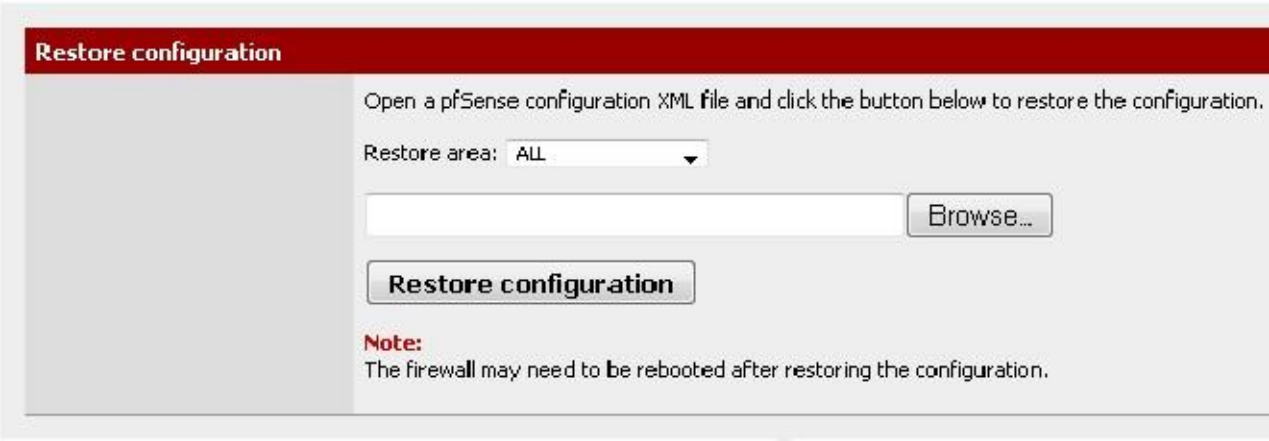
Restauración a partir de copias de seguridad

Las copias de seguridad no va a hacer mucho bien sin un medio para recuperar estos datos, y, por extensión, ponerlas a prueba. pfSense ofrece varios medios para la restauración de configuraciones. Algunos son más complejas que otras, pero cada uno debe tener el mismo resultado final: un sistema en funcionamiento idéntico a lo que estaba allí cuando se hizo la copia de seguridad.

Restauración con los WebGUI

La forma más fácil para la mayoría de la gente para restaurar una configuración es mediante el uso de la WebGUI. Navegue hasta Diagnóstico Backup / Restore, y mirar la sección de configuración de Restaurar (Figura 9.2, "WebGUI Restaurar "). Para restaurar la copia de seguridad, seleccione el área a restaurar (típicamente ALL), a continuación, haga clic en Examinar. Localizar el archivo de copia de seguridad en su PC y, a continuación, haga clic en el botón Restaurar configuración. La configuración será aplicada, y el servidor de seguridad se reiniciará con los ajustes obtenidos a partir del archivo de copia de seguridad.

Figura 9.2. WebGUI Restore



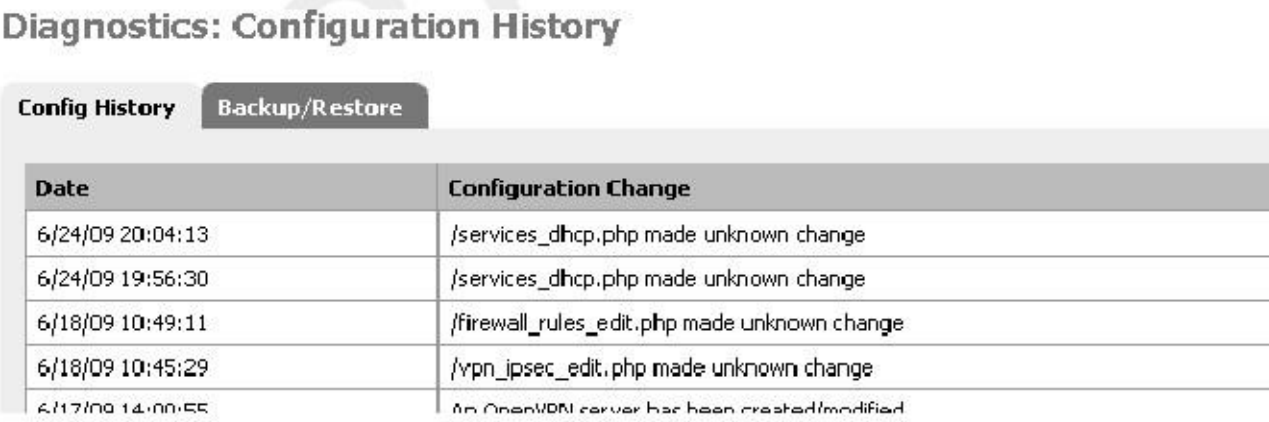
Mientras que es fácil trabajar con, este método tiene algunos requisitos cuando se trata de una restauración completa de un nuevo sistema. En primer lugar, tendría que hacerse después de que el nuevo sistema de destino está completamente instalado y funcionando.
En segundo lugar, se requiere un PC adicional conectado a una red de trabajo (o cable cruzado) detrás de la sistema pfSense que está siendo restaurado.

Restauración de la Historia Config

Para los problemas de menor importancia, una de las copias de seguridad internos de pfSense puede ser la forma más fácil de hacer una copia de un cambiar. A partir de los diagnósticos Página Backup / Restore, haga clic en la ficha Config Historia (Figura 9.3, "Historia de configuración"). Las 30 configuraciones anteriores se almacenan, junto con la ejecución actual

configuración. Para cambiar a una de estas configuraciones anteriores, haga clic en junto a su entrada.

Figura 9.3. Historia de configuración



La configuración se puede cambiar, pero el reinicio no es automática cuando sea necesario. Pequeños cambios hacen no requiere un reinicio, aunque revirtiendo algunos cambios importantes serán. Para estar seguro, es posible que desee reiniciar
el router con la nueva configuración, vaya a Diagnósticos Reinicio del sistema y haga clic en Sí.

Configuraciones previamente guardados se pueden eliminar haciendo clic, pero no es necesario eliminarlos manualmente para ahorrar espacio; las viejas copias de seguridad de configuración se borran automáticamente cuando se crean otros nuevos.
Es posible que desee eliminar una copia de seguridad de un cambio de configuración-conocida mala para asegurarse de que no es
accidentalmente restaurado.

Restauración con PFI

Cubierto en la sección denominada "Instalación de Recuperación", El Pre-Flight Installer (PFI) tendrá un archivo de configuración que se ha guardado en una unidad USB y restaurarlo como la configuración en ejecución

durante el proceso de instalación. Esto es probablemente el método más rápido para la restauración de una configuración, como se
que ocurre durante el proceso de instalación sin intervención manual en el cuadro de pfSense. Se arranca el primera vez con la nueva configuración, y usted no tendrá que preocuparse de tener un PC a mano a partir de que realizar la restauración a través de la WebGUI.

Restauración de Montaje de la CF / HDD

Este método es popular entre los usuarios incorporados. Si adjunta la CF o disco duro del sistema de pfSense para un equipo que ejecuta FreeBSD puede montar la unidad y copiar una nueva configuración directamente en un sistema instalado, o incluso copiar una configuración de un sistema fallido.

> **Nota**
>
> También puede realizar esto en un sistema pfSense separada en lugar de un equipo que ejecuta FreeBSD, pero no use un router de producción activa para este propósito. En su lugar, utilice un repuesto sistema o router de prueba.

El archivo de configuración se guarda en `/ Cf / conf /` tanto incrustado y las instalaciones nuevas, pero la diferencia está en
la ubicación donde se encuentra este directorio. Para instalaciones integrados, esto es en un segmento independiente, como
`ad0s3` si la unidad está `ad0`. Gracias a GEOM (marco de almacenamiento modular) las etiquetas de las versiones recientes
de FreeBSD y en uso en sistemas de archivos integrados basados en NanoBSD, también se puede acceder a esta porción sin tener en cuenta el nombre del dispositivo mediante el uso de la etiqueta `/ Dev / ufs / cf`. Para instalaciones

Ejemplo Embedded

normales, suele ser la raíz
slice (típicamente `ad0s1a`). Los nombres de las unidades pueden variar dependiendo del tipo y posición en el sistema.

En primer lugar, conecte el CF a un lector de tarjetas USB en un sistema FreeBSD u otro sistema pfSense inactiva (Véase la nota en la sección anterior). Para la mayoría, se mostrará como `da0`. También debe ver la consola mensajes que reflejan el nombre del dispositivo y las etiquetas GEOM recientemente disponibles.

Ahora montar la partición de configuración:

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

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

Ahora, copiar una 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. Ahora el router debe estar en ejecución con la configuración anterior. Si desea copiar la configuración desde la tarjeta, el proceso es el mismo
pero los argumentos de la cp comando se invierten.

Rescate Config durante la instalación

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

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 sistema.
Para la mayoría, esto no es necesario, pero puede ser útil para realizar copias de seguridad de datos RRD o para paquetes como
FreeSWITCH que puede tener archivos que desea conservar (por ejemplo, mensajes de correo de voz.) Para instalar el paquete,
vaya a Sistema Paquetes, encontrar refuerzos en la lista y haga clic en  . Una vez instalado, está disponible
en Diagnóstico Copia de seguridad de archivos / Dir. Es bastante simple de usar, como se muestra en el siguiente ejemplo.

Copia de seguridad de datos RRD

El uso de este paquete de copia de seguridad que debería ser bastante fácil de hacer una copia de seguridad de sus datos de gráficos RRD (ver
la sección llamada "los gráficos RRD").

En primer lugar, vaya a Diagnósticos Copia de seguridad de archivos / Dir. Clickto añadir una nueva ubicación para el grupo de respaldo. En el
Campo Nombre, escriba RRD Datos. En el campo Ruta, introduzca / Var / db / rrd. Establezca Enabled en Es cierto, y para
la Descripción, introduzca RRD Gráfico de datos. Haga clic en Guardar.
Desde la pantalla de copia de seguridad principal, haga clic en el botón Copia de seguridad, y luego se le presentará con un archivo de
descarga que deberá contener los datos RRD junto con cualquier otro directorio en el conjunto de copia de seguridad. Guardar en un lugar seguro, y considere mantener varias copias si los datos son muy importantes para usted.

Restauración de datos RRD

Del diagnóstico Copia de seguridad de archivos / Dir, haga clic en Examinar y busque un archivo de copia de seguridad que anteriormente era
descargado. Haga clic en Cargar, y los archivos se deben restaurar. Debido a que los ficheros RRD sólo se tocan cuando se actualiza una vez cada 60 segundos, usted no debería tener que reiniciar o reiniciar los servicios una vez que el archivos se restauran.

Advertencias y Gotchas

Mientras que el archivo XML de configuración guardado por pfSense incluye todos los ajustes, que no incluye los cambios que se hayan realizado con el sistema de la mano, como por ejemplo las modificaciones manuales de la fuente
código. Además algunos paquetes requieren métodos de copia de seguridad extra para sus datos.

El archivo de configuración puede contener información confidencial, como las claves de VPN o certificados, y contraseñas (excepto la contraseña de administrador) en texto sin formato en algunos casos. Algunos contraseñas deben ser
disponibles en texto en tiempo de ejecución, lo que hace de hash seguro de las contraseñas imposible. Cualquier ofuscación sería trivial para invertir para cualquier persona con el acceso al código fuente - es decir todos. La decisión consciente de diseño se hizo en m0n0wall, y continuó en pfSense, para dejar las contraseñas
en claro para que sea sumamente claro que el archivo contiene contenido sensible y debe ser protegida
como tal. Por lo tanto usted debe proteger las copias de seguridad de estos archivos de alguna manera. Si los almacena en medios extraíbles, cuidan de la seguridad física de que los medios de comunicación y / o cifrar la unidad.

Si tiene que usar el WebGUI través de la WAN sin una conexión VPN, al menos debe utilizar HTTPS.
De lo contrario, una copia de seguridad se transmite sin cifrar, incluyendo cualquier información sensible dentro de esa copia de seguridad
presentar. Se recomienda que usted utiliza un enlace de confianza o conexión encriptada.

Capítulo 10. Firewall

Una de las funciones primarias de pfSense independientemente de la función en la que se despliega es el filtrado tráfico. Este capítulo trata de los fundamentos de los cortafuegos, las mejores prácticas y la información que necesita para configurar las reglas necesarias para su entorno de servidor de seguridad.

Cortafuegos Fundamentos

Esta sección se ocupa principalmente de los conceptos introductorios de firewall y sienta las bases para ayudar a a entender la mejor manera de configurar apropiadamente las reglas del firewall en pfSense.

Terminología básica

Regla y conjunto de reglas son dos términos utilizados en este capítulo. Regla se refiere a una sola entrada en su Firewall Pantalla de las reglas. Una regla es una configuración o la acción para saber cómo mirar o manejar la red tráfico. Conjunto de reglas hace referencia a todas las reglas del firewall en su conjunto. Esta es la suma de todo el usuario configurado
y añade automáticamente las reglas, que están cubiertos aún más a lo largo de este capítulo.

En pfSense, conjuntos de reglas se evalúan en una base del partido. Esto significa que si usted lee el conjunto de reglas para un
Interfaz de arriba a abajo, la primera regla que coincida será el utilizado. El proceso se detiene después de llegar a este partido y luego se toma la acción especificada por la regla. Siempre mantenga esto en mente cuando la creación de nuevas normas, sobre todo 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 excepciones se pueden hacer por encima de
ellos.

Con estado de filtrado de

pfSense es un firewall con estado. Esto significa que sólo permiten el tráfico en la interfaz donde el tráfico es iniciados. Cuando se inicia una conexión que coincide con una regla de pase en el cortafuegos, se crea una entrada en tabla de estado del servidor de seguridad, donde se retiene información sobre las conexiones activas a través del firewall. El tráfico de respuesta a las conexiones iniciadas dentro de la red se deja automáticamente de nuevo en su la red de la tabla de estado. Esto incluye todo el tráfico relacionado con el uso de un protocolo diferente, como ICMP mensajes de control que pueden ser proporcionados en respuesta a una red TCP, UDP, o de otro tipo de conexión.

Vea la sección llamada "Firewall Advanced" y la sección "Tipo de Estado" sobre las opciones de estado y tipos.

Tamaño de la tabla Estado

La tabla de estado de servidor de seguridad tiene un tamaño máximo, para evitar el agotamiento de la memoria. Cada estado tiene
aproximadamente 1 KB de RAM. (Vea la sección llamada "grandes tablas de estado" sobre grandes tablas de estado.) El tamaño de la tabla de estado de forma predeterminada en pfSense es 10.000. Esto significa que si usted tiene 10.000 conexiones activas
navegación por el Sistema Página Avanzadas, y el desplazamiento hacia abajo en virtud de Traffic Shaper y Firewall atravesar el servidor de seguridad, se quitarán todas las conexiones adicionales. Este límite se puede aumentar por Avanzada (Figura 10.1, "El aumento de tamaño de la tabla de estado a 50.000"). Introduzca el número deseado para Firewall
Estados Máximo, o deje la casilla en blanco para el valor predeterminado 10000. Usted puede ver su estado histórico uso en Estado RRD gráficos. En la ficha Sistema, seleccione Unidos En los gráficos desplegables.

Figura 10.1. El aumento de tamaño de la tabla de estado a 50.000

Ingress Filtering

El filtrado de entrada se refiere al cortafuegos del tráfico que llega a su red desde Internet. En implementaciones con múltiples WAN que tienen múltiples puntos de ingreso. La política de entrada por defecto en pfSense
es bloquear todo el tráfico, ya que no hay reglas de permiso de WAN por defecto. Las respuestas al tráfico iniciado desde dentro de su red están autorizados automáticamente a través de la tabla de estado.

Filtrado de salida

Filtrado de salida se refiere al filtrado de tráfico iniciado dentro de la red destinado a Internet o cualquier otra interfaz en el firewall. pfSense, como fuente de casi todas similares y comercial abierta soluciones, viene con una regla de LAN que permite todo, desde la LAN hacia Internet. Este no es el mejor manera de operar, sin embargo. Se ha convertido en el valor por defecto de facto en la mayoría de las soluciones de firewall, porque
es simplemente lo que la mayoría de la gente desea. El error común es creer cualquier cosa en la red interna es "digno de confianza", por lo que ¿por qué preocuparse de filtrado?

¿Por qué debo utilizar filtrado de salida?

Desde mi experiencia en el trabajo con un sinnúmero de servidores de seguridad de numerosos vendedores a través de muchos diferentes
organizaciones, en su mayoría pequeñas empresas y redes domésticas no utilizan filtrado de salida. Se puede aumentar la carga administrativa, ya que cada nueva aplicación o servicio puede requerir la apertura de puertos adicionales o protocolos en el servidor de seguridad. En algunos entornos, es difícil debido a que los administradores no hacen realmente
saber lo que está sucediendo en la red, y no se atreven a romper cosas. En otros, es imposible por razones de la política del lugar de trabajo. Pero usted debe esforzarse para permitir sólo el mínimo necesario para el tráfico
salir de su red, siempre que sea posible. Filtrado de salida aplicado es importante por varias razones:

1. Limitar el impacto de un sistema comprometido - malware utiliza comúnmente puertos y protocolos que no se requieren en muchas redes. Muchos robots se basan en conexiones IRC a teléfono de su casa y recibir instrucciones. Algunos utilizarán los puertos más comunes, tales como el puerto TCP 80 (HTTP normalmente) para evadir
filtrado de salida, pero muchos no lo hacen. Si usted no permite que el puerto TCP 6667, el puerto de IRC de costumbre, usted puede
paralizar los robots que se basan en el IRC para funcionar.

   Otro ejemplo que he visto es un caso en el que la interfaz dentro de un pfSense instalar estaba viendo 50-60 Mbps de tráfico, mientras que la WAN tenía menos de 1 Mbps de rendimiento. No había otra interfaces del firewall. Algunos investigación mostró que la causa es un sistema comprometido en la LAN ejecutar un bot que participe en una denegación de servicio distribuido (DDoS) contra un chino El sitio web de juegos de azar. Se utiliza el puerto UDP 80, probablemente por un par de razones. En primer lugar, UDP que permite
   enviar paquetes grandes sin completar un protocolo de enlace TCP. Con firewalls son la norma, paquetes TCP grandes no pasarán hasta que el apretón de manos se completa con éxito, y esto limita la eficacia de los ataques DDoS. En segundo lugar, los que lo hacen emplear filtrado de salida son normalmente demasiado
   permisiva, lo que permite TCP y UDP, donde sólo se requiere TCP, como en el caso de HTTP. En este red, el puerto UDP 80 no fue permitido por el conjunto de reglas de salida, por lo que todo el DDoS estaba logrando estaba golpeando la interfaz interna del firewall con el tráfico que se estaba caído. Yo estaba buscando en el servidor de seguridad para una razón no relacionada y encontré este; fue felizmente resoplando sin degradación del rendimiento y el administrador de la red no sabían lo que estaba ocurriendo.

   SMTP saliente es otro ejemplo. Sólo se debe permitir SMTP, el puerto TCP 25, para dejar su de red de su servidor de correo. O si su servidor de correo está alojado externamente, sólo permita que su interior sistemas para hablar con ese sistema fuera específico en el puerto TCP 25. Esto evita que cualquier otro sistema en el su red sea utilizada como un zombi correo no deseado, ya que su tráfico SMTP será dado de baja. Este tiene la ventaja obvia de hacer su parte para limitar el spam, y también evita que la red de ser introducido en numerosas listas negras a través de Internet que le impedirá el envío de legítima correo electrónico a muchos servidores de correo.

   La solución correcta es evitar que este tipo de cosas sucedan en el primer lugar, pero la salida filtrado proporciona otra capa que puede ayudar a limitar el impacto si sus otras medidas fallan.

. 2 Evitar que un compromiso - en algunas circunstancias, filtrado de salida puede evitar que sus sistemas de sean comprometidos. Algunas brechas y gusanos requieren acceso saliente para tener éxito. Un viejo pero

Buen ejemplo de ello es el gusano Code Red desde 2001. El exploit causó sistemas afectados a tirar de un archivo ejecutable a través de TFTP (Trivial File Transfer Protocol) y luego ejecutarlo. Su web servidor es casi seguro que no es necesario que utilice el protocolo TFTP, y el bloqueo de la salida a través de TFTP filtrado de prevenir la infección con Code Red, incluso en los servidores no actualizados. Esto es en gran parte sólo es útil
para detener los ataques completamente automatizados y gusanos, como un verdadero atacante humano encontrará todos los agujeros
que existen en el filtrado de salida y utilizarlos para su propio beneficio.
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 atípicos o protocolos para su funcionamiento. Mientras que un
creciente número de peer-to-peer y mensajería instantánea le port hop hasta encontrar algo les permite salir de la red, muchos se impedirá que funcionen por una salida restrictiva conjunto de reglas, y este es un medio eficaz de limitación de muchos tipos de conectividad VPN.

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

. 5 Evitar fugas de información - ciertos protocolos se deben nunca permitir que salir de su red. Ejemplos específicos varían de un entorno a otro. Microsoft RPC (Remote Procedure Llamada) en el puerto TCP 135, NetBIOS sobre TCP y UDP 137 a 139, y SMB / CIFS (Servidor Internet File System mensaje Bloquear / Común) en el puerto TCP y UDP 445, son ejemplos comunes de servicios que no se debe permitir que salir de su red. Esto puede evitar que la información acerca la red interna se escape a la Internet, y evitará que sus sistemas de iniciación autenticación intenta con hosts de Internet. Estos protocolos también caen bajo "limitar el impacto de una sistema comprometido ", como se expuso 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 son syslog, SNMP, y trampas SNMP. La restricción de este tráfico evitará que los dispositivos de red mal configurados enviar registro y otra información potencialmente sensible a cabo en Internet. En lugar de preocuparse por qué protocolos pueden filtrar información de su red y deben ser bloqueados, permita exclusivamente el tráfico que se requiere.

Enfoques para la aplicación de filtrado de salida

En una red que históricamente no ha empleado filtrado de salida, puede ser difícil saber qué el tráfico es realmente necesario. Esta sección describe algunos de los enfoques para la aplicación de filtrado de salida en su red.

Permitir lo que sabe sobre, bloquear el resto, y trabaja a través de las consecuencias

Un método consiste en agregar reglas de firewall para el tráfico que usted conoce necesita ser permitido. Comience con lo que
una lista de las cosas que usted sabe son necesarios, como en la Tabla 10.1, "El tráfico de egreso requerido".

Tabla 10.1. Tráfico de egreso requerido

Descripción	IP de origen	IP de destino	Puerto de destino
HTTP y HTTPS ningún desde todos los hosts		cualquier	TCP 80 y 443
SMTP desde servidor de correo electrónico servidor IP		cualquier	TCP 25
IPs de servidores DNS RecursiveDNS consultas de los internos Los servidores DNS		cualquier	TCP y UDP 53

A continuación, configure las reglas del firewall en consecuencia, y dejar todo lo demás de la gota.

Entrar tráfico y analizar los registros

Otra alternativa es la de habilitar el registro en sus reglas de paso, y enviar los registros a un servidor Syslog, donde se puede analizar para ver qué tráfico está dejando su red. Dos paquetes de análisis de registros con soporte para el formato de registro de PF son fwanalog1 y Hatchet2. Puede que le resulte más fácil de analizar los registros con una secuencia de comandos personalizada si usted tiene experiencia con archivos de texto de análisis. Esto ayudará a construir la necesaria conjunto de reglas con menos secuelas que usted debe tener una mejor idea de lo que es necesario el tráfico en su red.

Bloquear vs Rechazar

Hay dos maneras de no permitir el tráfico en las reglas del firewall pfSense - bloque y rechazan. La configuración de bloqueo silenciosamente descarta el tráfico. Este es el comportamiento de la denegación predeterminada regla en pfSense, por lo tanto, en una forma predeterminada configuración, todo el tráfico iniciados desde Internet se suprimen silenciosamente.

Rechazar envía una respuesta a la denegación de tráfico TCP y UDP, dejando que el host que inició el conocimiento del tráfico que la conexión fue rechazada. Tráfico TCP Rechazado consigue un TCP RST (reset) en respuesta, y rechazó Tráfico UDP recibe un mensaje ICMP inaccesible en respuesta. Aunque puede especificar rechazar para cualquier regla de firewall, protocolos IP que no sean TCP y UDP no son capaces de ser rechazado - estas reglas silencio caer otros protocolos IP. Esto es porque no hay un estándar para rechazar otros protocolos.

¿Debo usar el bloque o rechazar?

Ha habido mucho debate entre los profesionales de la seguridad en los últimos años en cuanto al valor del bloque frente a rechazar. Algunos argumentan que el uso de bloque tiene más sentido, afirmando que "ralentiza" los atacantes de exploración Internet. Cuando se utiliza rechazar, una respuesta se envía de vuelta inmediatamente que el puerto está cerrado, mientras que bloque cae silenciosamente el tráfico, causando escáner de puertos del atacante que esperar por una respuesta. Ese argumento en realidad no retienen el agua, porque todo buen escáner de puertos puede escanear cientos o miles de servidores al mismo tiempo, y no está allí sentado esperando una respuesta de sus puertos cerrados. Hay una mínima diferencia en el consumo de recursos y la velocidad de exploración, pero tan leve que no debe ser un consideración. Si bloquea todo el tráfico de Internet, hay una diferencia notable entre el bloque y rechazar - nadie sabe que su sistema está realmente en línea. Si usted tiene incluso un puerto abierto, el valor es mínimo porque el atacante sabe que estás en línea, y también sabrá qué puertos están abiertos si usted rechaza las conexiones bloqueadas. Si bien no hay un valor significativo en el bloque por encima de rechazo, Aún así, recomiendo siempre usar bloqueador en sus reglas WAN.

Para conocer las reglas en las interfaces internas, le recomiendo usar rechazar en la mayoría de las situaciones. Cuando un host intenta acceder a algo que no está permitido en las reglas del cortafuegos, la aplicación acceder a él se puede bloquear hasta que los tiempos de conexión hacia fuera. Con rechazar, ya que la conexión es rechazada de inmediato, evita estos cuelga. Generalmente no es nada más que una molestia, pero todavía generalmente recomienda el uso de rechazar a evitar problemas de aplicaciones potenciales que en silencio dejando caer el tráfico dentro de su red podría inducir.

Hay un efecto secundario de esto que puede ser un factor en su elección de bloque o rechazar. Si utiliza rechazar, que hace que sea más fácil para las personas dentro de su red para determinar sus políticas de filtrado de salida como del firewall les hará saber lo que está bloqueando. Todavía es posible para los usuarios internos para asignar su salida normas al utilizar el bloque, sólo se necesita un poco más de tiempo y esfuerzo.

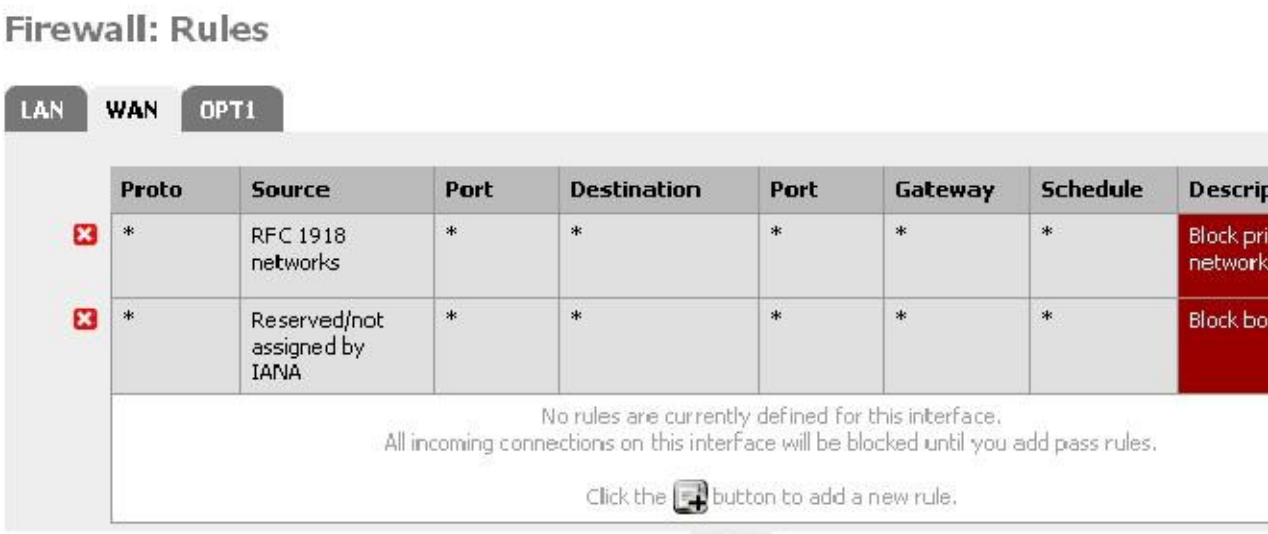
Introducción a la pantalla de las reglas del cortafuegos

En esta sección se ofrece una introducción y una visión general de la pantalla de las reglas del cortafuegos. En primer lugar, vaya a Firewall> Reglas. Con ello se abre el conjunto de reglas de la WAN, que por defecto no tiene entradas que no sean los para el Bloque redes privadas y redes Bloquear Bogon si habilitó aquellos, como se muestra en la Figura 10.2,

"Default reglas WAN". Si hace clic en theTo la derecha de las redes privadas de bloque o bloque bogon reglas de las redes, que le llevará a la página de configuración de interfaz WAN, donde estas opciones pueden ser activado o desactivado. (Vea la sección llamada "Block Private Networks" y la sección "Bloquear Bogon Redes "para más detalles sobre el bloqueo de las redes privadas y bogon.)

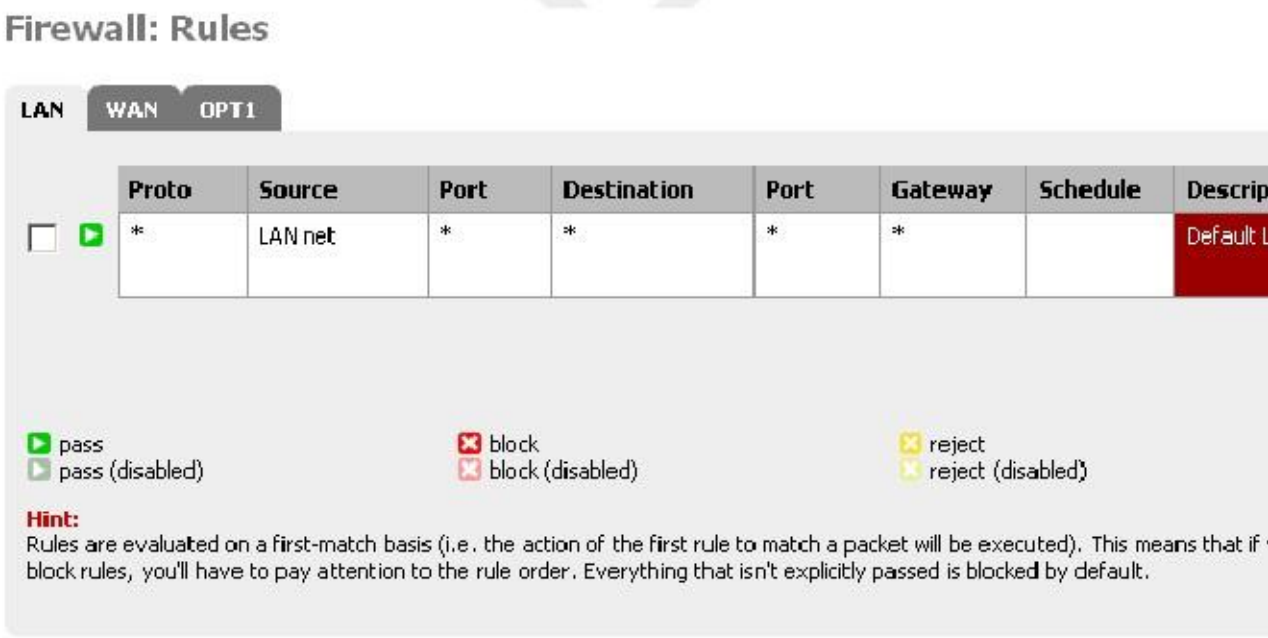
[1] http://tud.at/programm/fwanalog/
[2] http://www.dixongroup.net/hatchet/

Figura 10.2. Defecto reglas WAN



Haga clic en la ficha LAN para ver las reglas de LAN. Por defecto, este es sólo el Por defecto LAN -> cualquier gobernar como se ve en la Figura 10.3, "Default reglas LAN".

Figura 10.3. Por defecto las reglas de LAN



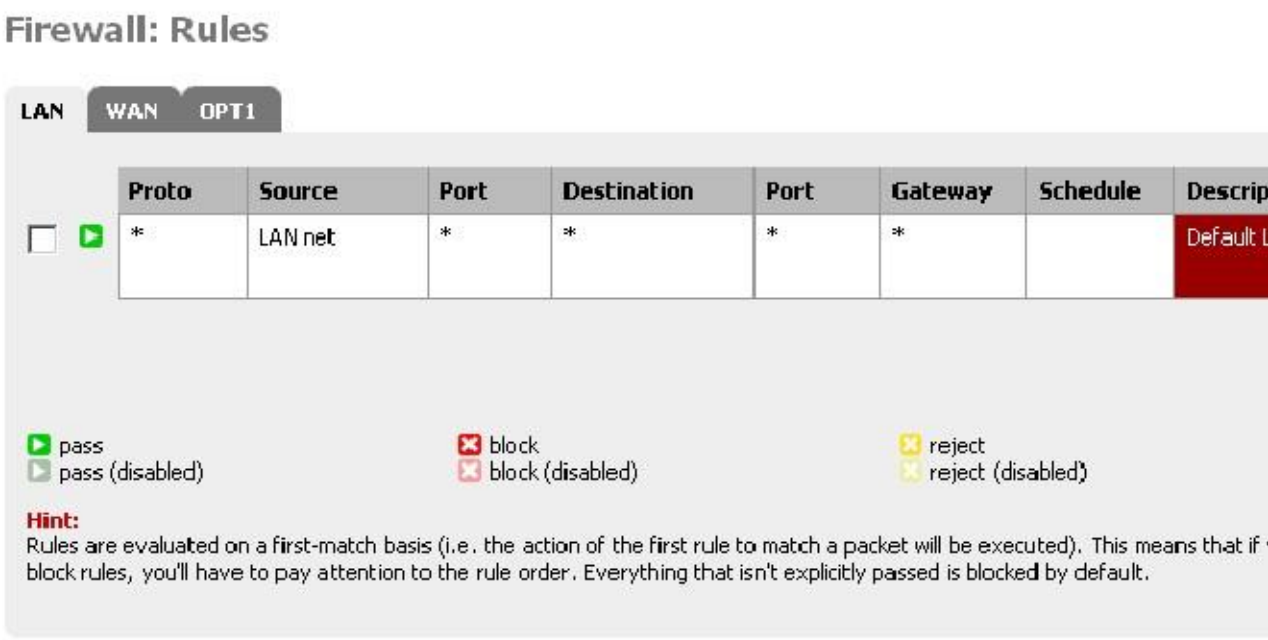
Reglas para otras interfaces se pueden ver haciendo clic en sus fichas respectivas. Aparecerán las interfaces OPT con sus nombres descriptivos, así que si usted designó a su interfaz DMZ OPT1, a continuación, en la ficha de su reglamento
También dirán DMZ.

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

Adición de una regla de firewall

Haga clic en cualquiera de los botones de la pantalla Firewall: Reglas para agregar una nueva regla. La parte superior e inferior botones, como se muestra en la Figura 10.4, "Añadir opciones de la regla LAN", se sumará una nueva añade una regla regla. La parte superior a la parte superior del conjunto de reglas, mientras que agrega la regla en la parte inferior. la parte inferior

Figura 10.4. Añadir opciones de la regla de LAN



Si usted desea hacer una nueva regla que es similar a una regla existente, haga clic en el al final de la fila. Aparecerá la pantalla de edición de la configuración de la regla existente precargadas, listas para ser ajustado. Para obtener más
información acerca de cómo configurar la regla de que se acaba de agregar, consulte la sección "Configuración de las reglas del cortafuegos ".

Edición de reglas de firewall

Para editar una regla de firewall, haga clic en theTo la derecha de la regla, o hacer doble clic en cualquier parte de la línea. Usted
luego será llevado a la pantalla de edición de esa norma, donde se pueden hacer los ajustes necesarios. Ver la sección llamada "Configuración de reglas del cortafuegos" para obtener más información sobre las opciones cuando esté disponible
la edición de una regla.

Mover reglas del cortafuegos

Las reglas pueden ser reordenados por su cuenta o en grupos. Para mover las reglas en la lista, seleccione la casilla junto a
las reglas que se deben mover o individuales haciendo clic en la regla verificará también el recuadro, a continuación, haga clic en el
botón en la fila que debe estar por debajo de las normas reubicados. Al pasar el puntero del ratón encima, una gruesa barra aparecerá para indicar dónde se insertarán las reglas. Después de hacer clic, el reglas serán luego insertadas encima de la fila seleccionada. También puede elegir las reglas para moverse por solo click en cualquier lugar dentro de la fila que desea seleccionar.

Eliminación de reglas de firewall

Para eliminar una sola regla, haga clic theTo 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 comienzo de las filas que deben ser eliminados, y luego haga clic en el en la parte inferior de la lista. Las reglas también se pueden seleccionar mediante un solo clic en cualquier parte de su línea.

Alias

Alias le permiten agrupar puertos, hosts o redes y se refieren a ellos por su nombre en las reglas del cortafuegos, Configuración de NAT y configuración regulador de trafico. Esto le permite crear significativamente más corto y más conjuntos de reglas manejables. Cualquier cuadro en la interfaz web con un fondo rojo es el alias de usar.

> **Nota**
>
> Los nombres en este contexto no se deben confundir con los alias IP de la interfaz, que son un medio de direcciones IP adicionales a una interfaz de red.

Configuración de los nombres

Para agregar un alias, vaya al Firewall □ Alias de la pantalla y haga clic en el botón. En las siguientes secciones describir cada tipo de alias que se puede utilizar.

En pfSense 1.2.x, cada alias se limita a 299 miembros.

Para añadir nuevos miembros a un alias, haga clic en el en la parte inferior de la lista de entradas en el Firewall □ Alias □ Pantalla Editar.

Anfitrión de los nombres

Alias de host permiten crear grupos de direcciones IP. Figura 10.5, "Ejemplo acoge alias" muestra un ejemplo de uso de un alias de hosts que contiene una lista de los servidores web públicos.

Los nombres de red

Alias de red le permiten crear grupos de redes, o rangos de IP mediante el uso de CIDR resumen. Anfitriones individuales también pueden ser incluidos en los alias de red mediante la selección de una máscara de red / 32.
Figura 10.6, "Ejemplo de alias de red" muestra un ejemplo de un alias de red que se utiliza más adelante en este capítulo.

Port de los nombres

Alias de puerto permiten la agrupación de puertos y rangos de puertos. El protocolo no está especificado en el alias, más bien la regla de firewall en el que utiliza el alias definirá el protocolo como TCP, UDP o ambos.
Figura 10.7, "Ejemplo puertos alias" muestra un ejemplo de un alias de puertos.

El uso de los nombres

Cualquier cuadro con un fondo rojo aceptará un alias. Al escribir la primera letra de un alias en Se muestra cualquier cuadro de entrada, una lista de alias coincidentes. Puede seleccionar el alias que desee, o tipo su nombre por completo.

> **Nota**
>
> Autocompletado Alias mayúsculas y minúsculas. Si usted tiene un alias llamado servidores web y escribe un minúscula "w", no aparecerá este alias. A "W" capital debe ser utilizado. Esto ya no ser el caso en 2.0.

Figura 10.8, "Autocompletado de los ejércitos alias" muestra como el alias de servidores web configuradas como se muestra
En la Figura 10.5, "Ejemplo acoge alias" puede ser utilizado en el campo Destino al añadir o editar una

regla de firewall. Seleccione "host individual o alias", a continuación, escriba la primera letra del alias deseado. Me acaba de escribir W
y el alias aparece como se muestra. Sólo se muestran los alias del tipo apropiado. Para los campos que requieren una dirección IP o subred, sólo se muestran los alias de host y de red. Para los campos que requieren puertos, sólo se muestran los puertos alias. Si hubiera varios alias que comienzan con "W", en la lista desplegable que Aparece mostrarían todos los alias determinadas.

Figura 10.8. Autocompletado de hosts alias

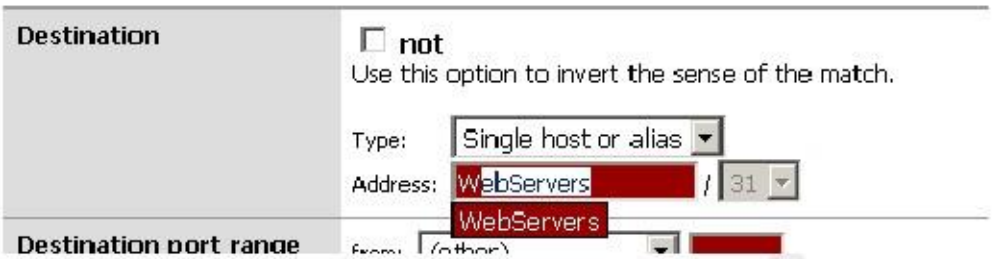


Figura 10.9, "Autocompletado de puertos alias" muestra el autocompletado de los alias de puertos configurados como se muestra en la Figura 10.7, "Ejemplo puertos alias". De nuevo, si múltiples alias coincide con la letra entró, todo alias coincidentes se enumeran. Puede hacer clic en el alias deseado para seleccionarlo.

Figura 10.9. Autocompletado de puertos alias

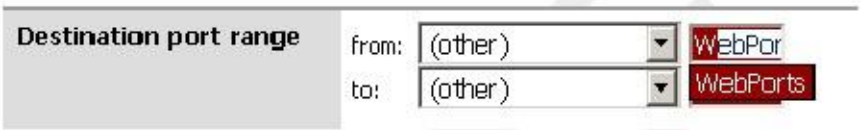


Figura 10.10, "Ejemplo Regla Utilizar alias" muestra la regla que creé usando los servidores web y Webports alias. Esta regla está en la WAN, y permite a cualquier fuente de las direcciones IP definidos en la Servidores web de alias cuando se utilizan los puertos definidos en el alias webports.

Figura 10.10. Ejemplo Regla Uso de alias

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

Si pasas el ratón por encima de un alias en el Firewall Reglas pantalla, aparece un cuadro que muestra la contenido del alias con las descripciones incluidas en el alias. Figura 10.11, "Suspendido en el aire muestra Hosts contenidos "muestra esto para el alias de servidores web y en la Figura 10.12," Suspendido en el aire muestra el contenido de Puertos "para
los alias de puertos.

Figura 10.11. Suspendido en el aire muestra el contenido de Hosts

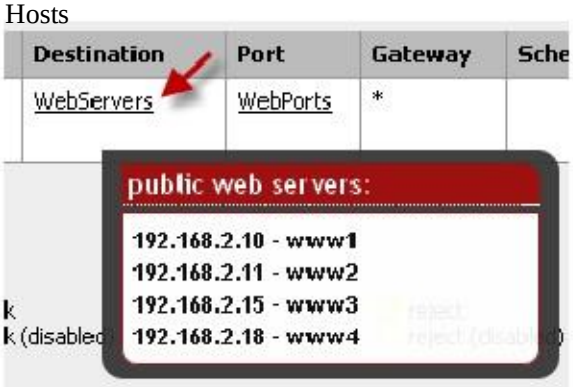


Figura 10.12. Suspendido en el aire muestra el contenido de Puertos

Mejoras alias en 2.0

pfSense 2.0 le permitirá alias anidar dentro de otros alias, e incluirá la posibilidad de introducir una Ubicación URL de un alias para su descarga.

pfSense 2.0 también incluye un gestor de usuarios de OpenVPN, y la posibilidad de crear alias de agrupación Usuarios de OpenVPN. Por ejemplo, los usuarios de TI pueden necesitar acceso a toda la red interna, pero otros usuarios sólo tienen acceso a un pequeño subconjunto de la red. Usuario alias OpenVPN harán de este fácil de lograr. OpenVPN se explica con más detalle en el Capítulo 19, OpenVPN.

Firewall Rule Mejores Prácticas

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

Denegar por defecto

Hay dos filosofías básicas de seguridad informática relacionados con el control de acceso - por defecto permitir y denegación predeterminada. Usted siempre debe seguir una estrategia de denegación predeterminada con las reglas del firewall. Configure
sus reglas para permitir sólo el mínimo requerido de tráfico para las necesidades de su red, y dejar que la caída de descanso con pfSense incorporado en mora regla de denegación. Siguiendo esta metodología, el número de negar
reglas en su conjunto de reglas deben ser mínimos. Ellos todavía tienen un lugar para algunos usos, pero se reducirán al mínimo
En la mayoría de los entornos, siguiendo una estrategia de denegación predeterminada.
En una forma predeterminada, las interfaces LAN y WAN de configuración, pfSense utiliza un defecto negar la filosofía en la
WAN y un defecto permiten en la LAN. Todo entrantes de Internet se niega, y todo
salir a Internet desde la LAN está permitido. Todos los routers de grado hogar utilizan esta metodología, como lo hacen todos
proyectos de código abierto similares y ofertas comerciales más similares. Es lo que quiere la mayoría de la gente - por lo tanto, es la configuración predeterminada. Sin embargo, no son los medios recomendados de operación.
pfSense usuarios a menudo preguntan "¿qué cosas malas Qué necesito para bloquear?" Esa es la pregunta equivocada, ya que se aplica a
una metodología de permiso de forma predeterminada. Seguridad señaló profesional Marcus Ranum incluye permiso de forma predeterminada en
su "Seis más mudos de Ideas en Seguridad Informática" papel, lo que se recomienda la lectura de ningún tipo de seguridad
professional.[3] permiso sólo lo que necesitan, y evitar dejar el valor por defecto permitir que todo dominio en la LAN y la adición de reglas de bloqueo de "cosas malas" por encima de la norma permitida.

Sea breve

Cuanto más corto sea su conjunto de reglas, más fácil es manejar. Conjuntos de reglas largas son difíciles de trabajar, aumentan la
posibilidades de error humano, tienden a ser excesivamente permisiva, y mucho más difícil de auditar.
Utilizar alias para ayudar a mantener su conjunto de reglas lo más corto posible.

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

Revise sus Reglas

Usted debe revisar manualmente las reglas de firewall y la configuración NAT de forma periódica para garantizar aún coinciden con los requisitos mínimos de su entorno de red actual. La recomendada frecuencia de esos exámenes varía de un entorno a otro. En redes que no cambian con frecuencia, con un pequeño número de administradores de firewall y buenos procedimientos de control de cambios, trimestral o semestralmente suele ser adecuada. Para cambiar rápidamente entornos o aquellos con problemas de control de cambios y varias personas con acceso firewall, la configuración debe ser revisado por lo menos sobre una base mensual.

Documentar su configuración

En todos menos en las redes más pequeñas, puede ser difícil recordar lo que se configura dónde y por qué. El uso de el campo Descripción de las reglas de firewall y NAT es siempre recomendable. En mayores o más complejas despliegues, también deben mantener un documento de configuración más detallada que describe su configuración pfSense entero. Al revisar su configuración en el futuro, esto le ayudará a determinar cuáles son necesarias reglas y por qué están allí. Esto también se aplica a cualquier otra área de la configuración.

También es importante mantener este documento hasta la fecha. Cuando se realiza la configuración de su periódico opiniones, es una buena idea revisar también este documento para asegurar que permanece al día con su actual configuración. Usted debe asegurarse de este documento se actualiza siempre que se hagan cambios de configuración.

La reducción de ruido Conectarse

El registro está habilitado en la denegación predeterminada regla en pfSense por defecto. Esto significa que todo el ruido recibiendo bloqueado a través de Internet va a ser registrados. A veces, usted no verá mucho ruido, pero en muchos ambientes que se encuentra algo spamming incesantemente sus registros. Con las conexiones utilizando gran dominios de difusión - una práctica comúnmente empleada por los ISP de cable - esto es lo más a menudo NetBIOS emisiones de los individuos-clue deficiente que se conectan las máquinas de Windows directamente a su banda ancha conexiones. Estas máquinas constantemente bombear solicitudes de difusión de navegación de la red, entre otras cosas. También puede ver el protocolo de enrutamiento de su ISP, o protocolos de redundancia de router tal como VRRP o HSRP. En entornos de co-ubicación, tales como centros de datos, a veces se ve una combinación de todas esas cosas.

Debido a que no hay ningún valor en conocer su firewall bloquea 14 millones de transmisiones de NetBIOS en el pasado días, y que el ruido podría encubriendo registros que son importantes, es una buena idea añadir una regla de bloqueo en la interfaz WAN para el tráfico ruido repetido. Mediante la adición de una regla de bloqueo sin registro habilitado en la interfaz WAN, este tráfico se seguirá bloqueado, pero ya no llena tus logs.

La regla se muestra en la Figura 10.13, "regla de cortafuegos para evitar la tala programas de radiodifusión" es que tengo configurado en uno de mis sistemas de prueba, donde el "WAN" está en una LAN. Para deshacerse de los ruidos de registro para
Puedo ver las cosas de interés, he añadido esta regla para bloquear pero no ingrese nada con el destino de la dirección de broadcast de la subred.

Figura 10.13. Regla de cortafuegos para prevenir emisiones de registro

Usted debe agregar reglas similares, haciendo coincidir los detalles de cualquier ruido de registro que está viendo en su medio ambiente. Compruebe los registros del firewall en Estado Registros del sistema Ficha Firewall para ver qué tipo de

tráfico están bloqueando y revisar su frecuencia. Si constantemente se está registrando todo el tráfico particular, más de 5 veces por minuto, probablemente debería agregar una regla de bloqueo para que pueda reducir el ruido de registro.

Prácticas de tala

Fuera de la caja, pfSense no registra cualquier tráfico pasado y registros de todas cayó tráfico. Este es el comportamiento por defecto típico de casi todos los de código abierto y firewall comercial. Es el más práctico, como el registro de todo el tráfico pasa rara vez se debe hacer debido a los niveles de carga y registro generados. Pero esta metodología es realmente un poco hacia atrás. Tráfico bloqueado no puede hacerte daño por lo que su valor de registro es
limitado, mientras que el tráfico que se pasa puede ser información de registro muy importante para tener si un sistema se ve comprometida. Después de eliminar cualquier ruido de bloque inútil como se describe en la sección anterior, la resto es de algún valor para fines de análisis de tendencias. Si usted está viendo significativamente más o menos log volumen de lo habitual, es probablemente bueno para investigar por qué es así. OSSEC, una fuente abierta basada en host sistema de detección de intrusos (IDS), es un sistema que puede recopilar registros de pfSense via syslog y alerta que inicie sesión volumen abnormalities.4

Regla Metodología

Reglas en pfSense se aplican en función de cada interfaz, siempre en la dirección de entrada de la interfaz. Esto significa que el tráfico iniciados desde la LAN se filtra utilizando las reglas de interfaz de LAN. Tráfico iniciado desde Internet se filtra con las normas de interfaz WAN. Debido a que todas las reglas de pfSense son stateful de forma predeterminada, se crea una entrada en la tabla de estado cuando el tráfico coincide con una regla de permiso. Todo el tráfico de respuesta es
permitida automáticamente por esta entrada de la tabla de estado.

En este momento, no hay manera para adaptarse a las reglas de salida en cualquier interfaz. Reglas de salida nunca se requiere, porque el filtrado se aplica en la dirección de entrada de cada interfaz. En algunos circunstancias limitadas, como un cortafuegos con numerosas interfaces internas, que tienen a disposición puede reducir significativamente el número de reglas de firewall requeridas. En tal caso, se podría aplicar a su normas de egreso para el tráfico de Internet como las reglas de salida de la WAN para evitar tener que duplicarlos para cada interfaz interna. El uso de filtros de entrada y salida hace las cosas más complejas y
más propenso a errores de los usuarios, pero entendemos que puede ser conveniente y esperamos dar cabida a esto de alguna
la moda en el futuro.

Reglas de cortafuegos añade automáticamente

pfSense agrega automáticamente algunas reglas de firewall, para una variedad de razones. En esta sección se describe cada
añade automáticamente regla y su propósito.

Regla Anti-bloqueo

Para prevenir mismo se quede fuera de la interfaz web, pfSense permite a una de las reglas anti-bloqueo por defecto.

Esto es configurable en el Sistema Página Avanzadas en Webgui Anti-bloqueo. Esto automáticamente regla añadida permite el tráfico procedente de cualquier fuente dentro de la red a todos los protocolos que escucha en la IP LAN.

En entornos de seguridad-consciente, debe deshabilitar esta regla, y configurar sus reglas LAN así
sólo un alias de host de confianza puede tener acceso a las interfaces de administración del servidor de seguridad.

Restringir el acceso a la interfaz de administración de LAN

En primer lugar es necesario configurar las reglas de firewall como se desee para restringir el acceso a las interfaces de administración.
Voy a caminar a través de un ejemplo de cómo normalmente configuro esto. Puedo utilizar SSH y HTTPS para gestión, por lo que crear un alias ManagementPorts contienen estos puertos (Figura 10.14, "Alias de puertos de administración ").

Entonces puedo crear un alias para hosts y / o redes que tendrán acceso a las interfaces de administración (Figura 10.15, "Alias de hosts de gestión").

[4] http://www.ossec.net

Los alias resultantes se muestran en la Figura 10.16, "Lista de Alias".

A continuación, las reglas de firewall de LAN deben estar configurados para permitir el acceso a los hosts definidos previamente, y
denegar el acceso a todo lo demás. Hay muchas maneras que usted puede lograr esto, en función de las características específicas de
su entorno y la forma de manejar filtrado de salida. Figura 10.17, "Ejemplo de gestión restringida
Reglas de LAN "y Figura 10.18," Administración restringido reglas LAN - ejemplo alternativo "muestran dos ejemplos. El primero permite las consultas DNS a la IP LAN, que es necesario si usted está utilizando el DNS promotor, y también permite a LAN alberga hacer ping a la IP LAN. A continuación, rechaza el resto del tráfico. El segundo
ejemplo permite el acceso desde los ordenadores de gestión de los puertos de administración, luego rechaza todas las demás
el tráfico a los puertos de gestión. Elija el método 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 se configuran las reglas del cortafuegos, es necesario deshabilitar la regla anti-bloqueo Webgui en el Sistema
 Página Avanzadas (Figura 10.19, "Anti-bloqueo regla discapacitados"). Marque la casilla y haga clic en Guardar.

> **Nota**
>
> Si ya no puede acceder a la interfaz de administración después de desactivar la regla anti-bloqueo, que no configurar las reglas de firewall de manera apropiada. Puede volver a activar el anti-bloqueo gobernar mediante la opción Set LAN IP en el menú de la consola. Sólo tienes que configurar a su IP actual, y la
> automáticamente se vuelve a activar la regla.

Reglas Anti-spoofing

pfSense utiliza la función antispoof PF para bloquear el tráfico falso. Esto proporciona Unicast Reverse Path Desviar (uRPF) funcionalidad que se define en el RFC 3704 [http://www.ietf.org/rfc/rfc3704.txt]. La
firewall comprueba cada paquete contra su tabla de enrutamiento, y si un intento de conexión proviene de una fuente IP en una interfaz donde el firewall sabe que la red no reside, se cae. Por ejemplo,
algo que viene en la WAN con una IP de origen de una red interna se cae. Todo inició en
la red interna con una IP de origen que no reside en la red interna se cae.

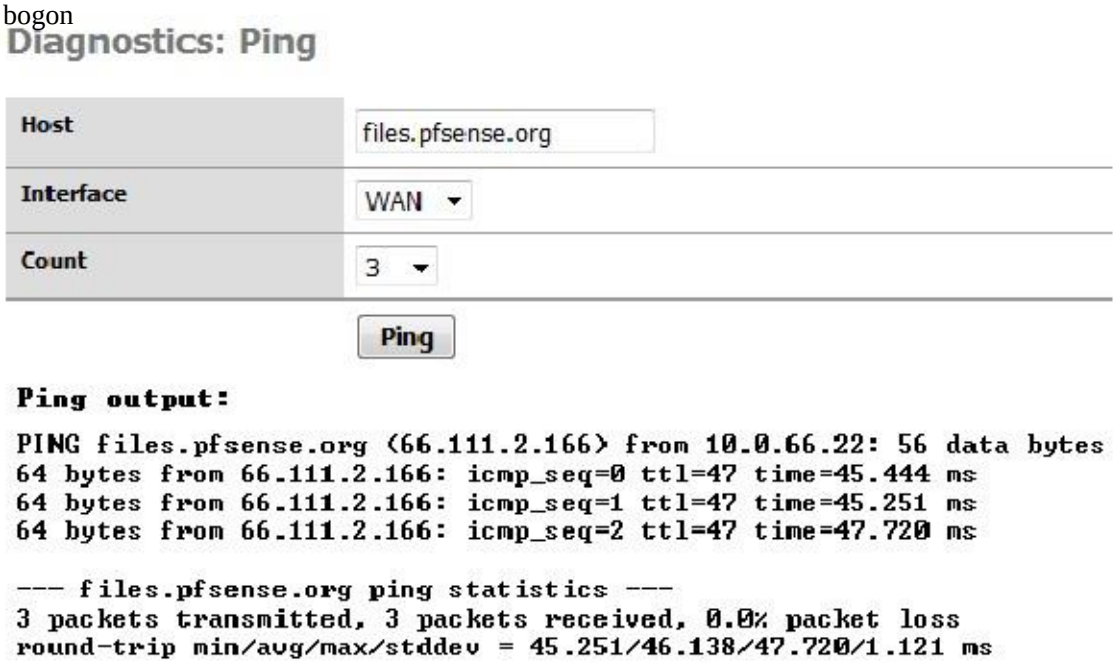
Bloque de Redes Privadas

La opción Bloquear las redes privadas en la interfaz WAN pone automáticamente en una regla de bloqueo de RFC 1918 subredes. A menos que tenga un espacio IP privado en su WAN, debería activar esto. Esto sólo
se aplica al tráfico iniciado en el lado WAN. Todavía se puede acceder a los hosts en redes privadas de la interior. Esta opción no está disponible para las interfaces WAN OPT en pfSense 1.2.x, pero está en 2,0. Usted puede añadir manualmente una regla para bloquear las redes privadas en sus interfaces de OPT WAN mediante la creación de un alias
que contiene el RFC 1918 subredes y añadiendo una regla de cortafuegos a la parte superior de su interfaz OPT WAN reglas para bloquear el tráfico con origen coincidente ese alias. (Vea la sección denominada "Direcciones IP privadas" para obtener más información acerca de las direcciones IP privadas.)

Bloque Bogon Redes

Redes Bogon son aquellos que nunca debe ser visto en Internet, incluyendo reservado y
espacio de direcciones IP sin asignar. Estas redes no deben ser vistos como IP de origen en Internet, y indicar tanto el tráfico falso, o una subred no utilizada que ha sido secuestrado por un uso malicioso. pfSense proporciona una lista bogons que se actualiza según sea necesario. Si tiene redes de bloque bogon habilitadas, su firewall obtendrá una lista bogons actualizado en el primer día de cada mes de `files.pfsense.org`.
El script se ejecuta a las 3:00 am, hora local, y tiene capacidad para una cantidad aleatoria de tiempo hasta 12 horas antes realizar la actualización. Esta lista no cambia con mucha frecuencia, y se eliminan las nuevas asignaciones de IP a partir de los meses de lista bogons antes de que realmente se usa, por lo que la actualización mensual es adecuado. Hacer
Asegúrese de que su firewall puede resolver nombres de host DNS, de lo contrario la actualización fallará. Para garantizar que pueda
resolver DNS, vaya a Diagnósticos Ping, y tratar de hacer ping files.pfsense.org como se demuestra
En la Figura 10.20, "Pruebas de resolución de nombres para las actualizaciones bogon".

Figura 10.20. Probando la resolución de nombres para las actualizaciones bogon



Forzar una actualización bogons

Con los cambios relativamente infrecuentes en la lista bogons y aviso anticipado de la nueva IP pública asignaciones, la actualización bogons mensual es adecuado. Sin embargo puede haber situaciones en las que querer forzar manualmente una actualización bogon, como si sus cambios bogon han estado fallando debido a

una configuración de DNS incorrecta. Puede ejecutar una actualización a través de diagnósticos de la interfaz web Pantalla de comandos, mediante la ejecución de / Etc / rc.update_bogons.sh ahora. La ahora argumento que sigue el guión
es importante porque le indica al guión para ejecutar de inmediato y no dormir.

IPsec

Al habilitar un sitio para localizar la conexión IPsec, las reglas se agregan automáticamente permitiendo el control remoto
acceso de direcciones IP del extremo del túnel al puerto UDP 500 y el protocolo ESP en la dirección IP de WAN utilizado
para la conexión. Cuando los clientes móviles IPsec está habilitado, el puerto UDP 500 y se permite el tráfico ESP de cualquier fuente.
Debido a las obras de encaminamiento de política así, todo el tráfico que coincide con una regla que especifica una puerta de entrada será
forzado a salir a Internet y pasará por alto el procesamiento IPsec. Cuando se tiene una regla de permiso que especifica un
puerta de enlace en la interfaz interna que contiene la subred utilizada por la conexión IPsec, y el destino
de la regla es "cualquiera", una regla se añade automáticamente a negar la política de enrutamiento para el tráfico destinado a la
subred VPN remoto.
Reglas de IPsec añadidos automáticamente se discuten en mayor detalle en el Capítulo 17, IPsec.

PPTP

Cuando se habilita el servidor PPTP, reglas ocultas son automáticamente añadidos permitir el puerto TCP 1723
y el protocolo GRE (Generic Routing Encapsulation) a su dirección IP de WAN desde cualquier fuente IP
Dirección. Más información acerca de estas reglas se pueden encontrar en la sección denominada "VPN y Firewall Reglas ".

Denegar por defecto Regla

Las reglas que no coincidan con las reglas definidas por el usuario ni ninguna de las otras reglas añadidas de forma automática están en silencio
bloqueada por la regla de denegación por defecto (como se explica en la sección llamada "Default Deny").

Configuración de reglas de firewall

Esta sección cubre cada opción individual disponible de Firewall Reglas Pantalla de edición cuando la configuración de reglas de firewall.

Acción

Aquí es donde se especifica si la regla va a pasar, bloquear o rechazar el tráfico. Cada uno de estos está cubierto anteriormente en este capítulo.

Discapacitado

Si desea desactivar una regla sin eliminarla de la lista de reglas, marque esta casilla. Todavía se mostrará en pantalla de las reglas del cortafuegos, pero estarán en gris para indicar el estado desactivado.

Interfaz

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

Protocolo

Aquí es donde se especifica el protocolo de esta regla será equivalente. La mayoría de estas opciones son fáciles de entender.
TCP / UDP coincidirá tráfico TCP y UDP. Especificando ICMP hará otro cuadro desplegable en la que podrá seleccionar el tipo de ICMP. Varios otros protocolos comunes también están disponibles.

Fuente

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

Para el tipo puede especificar: Any, que coincidirá con cualquier dirección; Host o alias único, que se coincidir con una única dirección IP / nombre de host o alias nombre; o red, que tendrá una dirección IP y la máscara de subred para que coincida con un rango de direcciones. Por último, hay varios presets disponibles que pueden ser
muy útil en lugar de introducir estas direcciones manualmente: la dirección de WAN, LAN dirección, la subred LAN, Usuarios clientes PPTP, PPPoE y.

Para conocer las reglas que utilizan TCP y / o UDP, también puede especificar el puerto de origen aquí haciendo clic en el Avanzada
botón. El puerto de origen está oculta detrás del botón Avanzada porque usted normalmente querrá abandonar el puerto de origen se establece en "cualquier", como TCP y UDP se obtienen de un puerto aleatorio en el rango de puerto efímero (entre 1024 y 65535, el rango exacto usado varía dependiendo de la versión del sistema operativo y el sistema operativo que inicia la conexión). El puerto de origen casi nunca es el mismo que
el puerto de destino, y nunca se debe configurar como tal a menos que sepa la aplicación que están utilizando emplea este comportamiento atípico. También es seguro para definir su puerto de origen como una amplia gama de
1.024 a 65.535.

Fuente OS

Una de las características más únicas de PF y por lo tanto pfSense es la capacidad de filtrar por el sistema operativo iniciar la conexión. Para conocer las reglas del PCT, pf permite pasiva fingerprinting sistema operativo que permite crear reglas basadas en el sistema operativo que inicia la conexión TCP. La característica de p0f
PF determina el sistema operativo en uso mediante la comparación de características del paquete TCP SYN que inicia TCP
conexiones con un archivo de huellas dactilares. Tenga en cuenta que es posible cambiar la huella digital de su operativo sistema para que parezca otro sistema operativo, sobre todo con los sistemas operativos de código abierto tales como los BSD y

Linux. Esto no es fácil, pero si usted tiene usuarios técnicamente competentes con el administrador o el nivel de la raíz acceso a los sistemas, es posible.

Destino

Aquí es donde se especifica la dirección IP de destino, subred o alias que coincida con esta regla. Consulte la descripción de la opción Fuente en la sección llamada "Fuente" para más detalles. Al igual que con la Fuente configuración de la dirección, es posible comprobar que no para negar el encuentro.

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

Iniciar sesión

Esta casilla determina si los paquetes que coincidan con esta regla se registrarán en el registro de servidor de seguridad. Logging
se discute con más detalle en la sección titulada "Prácticas de registro".

Opciones avanzadas

Esta sección le permite configurar poderosas habilidades de pf para limitar los estados de firewall en función de cada regla. Por
De forma predeterminada, no hay límites fijados para cualquiera de estos parámetros.

Límite de conexiones de cliente simultáneas

Esta opción especifica el número total de direcciones IP de origen pueden conectar simultáneamente a esta regla. Cada fuente
IP se permite un número ilimitado de conexiones, pero el número total de direcciones IP de origen permitida es restringido a este valor.

Entradas Máximo estatales por host

Si prefiere limitar basado en conexiones por host, este ajuste es lo que quieres. Utilizando este ajuste,
usted puede limitar una regla de 10 conexiones por host de origen, en lugar de 10 conexiones total.

Máximo nuevas conexiones por segundo /

Este método de limitación de velocidad puede ayudar a garantizar que un tipo 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 servidor de correo electrónico a reducir
la carga de la sobrecarga por contra spambots. También se puede utilizar en las normas de circulación de salida para establecer límites
que impida cualquier máquina solo desde la carga hasta su tabla de estado o hacer demasiados rápida
conexiones, los comportamientos que son comunes con los virus. Puede configurar tanto una cantidad de conexión y un número de segundos para el período de tiempo. Cualquier dirección IP superior a la cantidad de conexiones dentro de el marco de tiempo dado se bloqueará durante una hora. Detrás de las escenas, esto es manejado por el virusprot mesa, llamado así por su finalidad típica de la protección antivirus.

Tiempo de espera de Estado en segundos

Aquí se puede definir un tiempo de espera de estado para el tráfico coincidiendo esta regla, anulando el estado predeterminado del sistema
tiempo de espera. Las conexiones inactivas se cerrarán cuando la conexión ha estado inactiva durante esta cantidad de tiempo. El tiempo de espera de estado por defecto depende del algoritmo de optimización de servidor de seguridad en el uso. La optimización
opciones se tratan en la sección denominada "Opciones de optimización del servidor de seguridad"

Tipo Estado

Hay tres opciones para el seguimiento del estado de pfSense que pueden especificarse en función de cada regla.

mantener el estado

Este es el valor por defecto, y lo que casi siempre se debe utilizar.

Estado synproxy

Esta opción hace que pfSense a las conexiones TCP entrantes proxy. Conexiones TCP comienzan con un período de tres vías. El primer paquete de una conexión TCP es un SYN de la fuente, lo que provoca un SYN
Respuesta ACK desde el destino. Esto ayuda a proteger contra un tipo de ataque de denegación de servicio, Inundaciones SYN. Esto es típicamente utilizado con normas sobre interfaces WAN. Este tipo de ataque no es muy hoy común, y cada sistema operativo moderno principal incluye capacidades de manejo de este en su poseer. Podría ser útil cuando la apertura de puertos TCP para los hosts que no manejan bien el abuso de la red.

ninguno

Esta opción no mantener el estado de esta regla. Esto sólo es necesario en algunos avanzada altamente especializado escenarios, ninguno de los que se tratan en este libro, ya que son extremadamente raros. Usted nunca debe tener una necesidad de utilizar esta opción.

No XML-RPC Sync

Al marcar esta casilla evita que esta regla de sincronización con otros miembros de la carpa. Esto se trata en Capítulo 24, Firewall de redundancia / alta disponibilidad.

Horario

Aquí usted puede seleccionar una programación especifica los días y horas esta norma estará en vigencia. Selección "Ninguno" significa el gobierno siempre estará activado. Para obtener más información, consulte la sección "Tiempo de Reglas Internas "más adelante en este capítulo.

Entrada

Gateway le permite especificar una interfaz WAN o la piscina equilibrador de carga para la coincidencia de tráfico de esta regla
a utilizar. Esto se trata en el capítulo 15, Múltiples conexiones WAN.

Descripción

Escriba una descripción aquí para su referencia. Esto es opcional, y no afecta a la funcionalidad de la gobernar. Usted debe ingresar algo aquí que describe el objetivo de la norma. La longitud máxima es de 52 personajes.

Métodos de uso de IPs públicas adicionales

Si sólo tiene una única dirección IP pública, puede saltar a la siguiente sección. Los métodos de despliegue direcciones IP públicas adicionales variarán dependiendo de la forma en que se asignan, ¿cuántos tienes asignados, y las metas para su entorno de red. Para usar IPs públicas adicionales con NAT,
deberá configurar IPs virtuales. Usted también tiene dos opciones para asignar directamente IPs públicas a los anfitriones con enrutamiento subredes IP públicas y puente.

Elegir entre direccionamiento, puente, y NAT

Puede utilizar cualquiera de sus direcciones IP públicas adicionales asignando directamente en los sistemas que utilizarán ellos, o mediante el uso de NAT.

IP adicionales a través de DHCP

Algunos ISP 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, la deja con dos opciones viables.

Bridging

Si desea que las direcciones IP adicionales directamente asignados a los sistemas que van a utilizar, de puente es su única opción. Utilice una interfaz OPT puenteado con WAN para estos sistemas.

Pseudo multi-WAN

Su única opción para tener el firewall tire estas direcciones como arrendamientos es un pseudo multi-WAN despliegue. Instale una interfaz de red por IP pública, y configurarlos para DHCP. Conecte todos los interfaces en un interruptor entre el firewall y el módem o router. Ya que va a tener múltiples las interfaces que comparten un único dominio de difusión, tendrá que marcar la casilla al lado de "Esto suprimirá

Mensajes ARP cuando las interfaces comparten la misma red física "en el Sistema de Página Avanzadas para eliminar las advertencias ARP en sus registros que son normales en este tipo de despliegue.

El único uso de varias direcciones IP públicas asignadas de esta manera es para el reenvío de puertos. Puede configurar puerto remite en cada interfaz WAN que utilizará la IP asignada a la interfaz por sus ISP Servidor DHCP. NAT de salida a su OPT WAN no funcionará debido a la limitación de que cada WAN debe tener una puerta de enlace IP única para el tráfico adecuadamente directa de ese WAN. Esto se discute en el Capítulo 15, Múltiples conexiones WAN.

IPs estáticas adicionales

Métodos de uso de direcciones IP públicas estáticas adicionales variarán dependiendo del tipo de asignación. Cada uno de los escenarios más comunes se describen aquí.

Subred IP única

Con una única subred IP pública, una de las IPs públicas estarán en el router de salida, comúnmente perteneciente a su proveedor de Internet, con una de las IPs asignadas como la IP WAN en pfSense. Las IPs restantes pueden ser utilizado con cualquiera de NAT, de puente o una combinación de los dos. Para utilizarlos con NAT, Proxy ARP añadir o VIPs CARP. Para asignar IPs públicas directamente a los hosts detrás de su firewall, necesitará un dedicado interfaz para aquellas máquinas que se puentea a WAN. Cuando se utiliza con puente, los anfitriones con el público IPs directamente asignados deben usar la misma puerta de enlace predeterminada como la WAN del firewall, el ISP aguas arriba router. Esto creará dificultades si los hosts con direcciones IP públicas tienen que iniciar conexiones a hosts detrás de otras interfaces de su servidor de seguridad, ya que la puerta de enlace del ISP no distribuirá el tráfico para su interna subredes de nuevo a su servidor de seguridad. Figura 10.21, "Múltiples IPs públicas en uso - bloque de IP única" muestra un ejemplo del uso de varias direcciones IP públicas en un solo bloque con una combinación de NAT y de puente. Para información sobre la configuración de NAT, consulte el capítulo 11, Network Address Translation, y puente en el Capítulo 13, Tender un puente.

Pequeño subred IP WAN con mayor subred LAN IP

Algunos ISP le dará una pequeña subred IP que el "WAN" asignación, y la vía de una mayor "dentro" subred a su final de la subred WAN. Comúnmente se trata de un / 30 en el lado de la WAN, y un / 29 o mayor para el interior. El enrutador de proveedor se le asigna un extremo de la / 30, típicamente el IP más baja, y su firewall se le asigna el IP más alta. Luego, el proveedor rutas subred LAN a la WAN IP. Usted puede utilizar esas direcciones IP adicionales en una interfaz de enrutado con IPs públicas directamente asignado a los hosts, o con NAT Uso de otros VIPs, o una combinación de los dos. Dado que las IPs se enrutan a usted, ARP no es necesaria, y usted no necesita ninguna entrada VIP para el uso con NAT 1:1. Debido pfSense es la puerta de entrada en el OPT1 segmento, el enrutamiento de los hosts OPT1 a LAN es mucho más fácil que en el escenario de puente se requiere cuando utilizando un único bloque de IP pública. Figura 10.22, "Múltiples IPs públicas de uso - dos bloques IP" muestra un ejemplo que combina un bloque de enrutado IP y NAT. Enrutamiento IP pública se trata en la sección llamada "Enrutamiento IP Pública", y NAT en el Capítulo 11, La traducción de direcciones de red.

Si está utilizando CARP, la subred WAN tendrá que ser un / 29, por lo que cada uno tiene su propio firewall WAN IP, y usted tiene un IP CARP en que el proveedor le permitirá dirigir el más grande dentro del bloque. La subred IP dentro debe ser encaminado a una IP que está siempre disponible, independientemente del servidor de seguridad se ha terminado, y el más pequeño subred utilizable con CARP es un / 29. Una configuración de este tipo con CARP es el mismo que el ilustrado anteriormente, con la

Gateway OPT1 ser una IP CARP, y el encaminamiento a un proveedor de IP CARP en lugar de la IP WAN. CARP se trata en el capítulo 24, Firewall de redundancia / alta disponibilidad.

Subredes IP múltiples

En otros casos, usted puede tener varias subredes IP de su ISP. Por lo general se empieza con uno de los dos disposiciones descritas anteriormente, y más tarde al solicitar direcciones IP adicionales se le proporciona con una subred IP adicional. Esta subred adicional debe ser enviada a usted por su proveedor de Internet, ya sea para su WAN IP en el caso de un único servidor de seguridad o un IP CARP al utilizar CARP. Si su proveedor de se niega a dirigir la subred IP a usted, sino que la encamine a su enrutador y utiliza una de las IPs de la subred como una puerta de enlace IP, usted tendrá que usar proxy ARP VIPs para la subred adicional. Si en absoluto posible, su proveedor debe enrutar la subred IP a usted, ya que hace que sea más fácil trabajar con independencia de su firewall de elección.

Cuando la subred IP se enruta a usted, el escenario descrito en la sección llamada "Pequeña WAN IP subred con mayor subred IP LAN "se aplica, sólo por una subred dentro adicional. Puede asignar a un nueva interfaz OPT, usarlo con NAT, o una combinación de los dos.

IPs virtuales

pfSense permite el uso de múltiples direcciones IP públicas en combinación con NAT a través de direcciones IP virtuales (VIPs).

Hay tres tipos de direcciones IP virtuales disponibles en pfSense: Proxy ARP, la carpa, y Otros. Cada uno es útil en diferentes situaciones. En la mayoría de circunstancias, pfSense tendrá que proporcionar ARP en sus personalidades tan
debe utilizar proxy ARP o CARP. En situaciones donde no se requiere ARP, como cuando adicional IPs públicas son dirigidas por el proveedor a su WAN IP, use Otras personalidades de tipo.

Proxy ARP

Funciones de Proxy ARP estrictamente en la capa 2, simplemente proporcionar respuestas ARP para la dirección IP especificada o
CIDR rango de direcciones IP. Esto permite pfSense que transmita el tráfico destinado a esa dirección de acuerdo a la configuración de NAT. La dirección o rango de direcciones no están asignadas a ninguna interfaz en pfSense, ya que no es necesario ser. Esto significa que no hay servicios en pfSense sí puede responder en estos IPs. Esto es generalmente considerado un beneficio, ya que sus IPs públicas adicionales sólo deben utilizarse para NAT propósitos.

CARP

VIPs CARP se utilizan sobre todo con las implementaciones redundantes utilizando CARP. Para obtener información sobre el uso de
VIPs CARP, consulte el Capítulo 24, Firewall de redundancia / alta disponibilidad acerca de la redundancia de hardware.
Algunas personas prefieren usar VIPs CARP incluso cuando se utiliza un solo servidor de seguridad. Esto es generalmente porque
pfSense responderá a los pings de CARPA VIP si tus reglas del firewall permite este tráfico (las reglas predeterminadas No lo hagas, por VIPs sobre WAN). Otra situación en la que se deben utilizar VIPs carpa es para cualquier VIPs que será el anfitrión de un servidor FTP. El proxy FTP en pfSense debe ser capaz de unirse a la VIP a funcionar, y sólo VIP CARP permiten que.

pfSense no responderá a los pings destinados a Proxy ARP y otros VIPs, independientemente de su firewall descartar la configuración. Con Proxy ARP y otros VIPs, debe configurar NAT a un host interno para ping para funcionar. Consulte el Capítulo 11, Network Address Translation para más información.

Otro

"Otros" VIPs permiten definir direcciones IP adicionales para su uso cuando 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 la Pantallas de configuración de NAT. Esto es útil cuando se tiene un bloque de IP pública encaminada a su IP WAN dirección o un VIP CARP.

Reglas Internas de Tiempo

Normas basadas en el tiempo permiten aplicar reglas de firewall sólo en los días y / o intervalos de tiempo especificados. Tiempo
reglas basadas se implementan en 1.2.x utilizando el filtro ipfw, porque las dificultades con el estado de mantenimiento en el
tiempo esta funcionalidad fue escrito significaba que era la única posibilidad de desconectar adecuadamente activo sesiones cuando el horario expirado. Nueva funcionalidad en pfSense 2.0 permitió que esto puede integrar con el filtro pf, permitiendo reglas de tiempo basado funcionen igual que cualquier otra norma. Por el momento, no algunas advertencias para el uso de reglas de tiempo basada, y la lógica de estas reglas es un poco diferente. En esta sección
discutirá cómo utilizar reglas de tiempo basada, y las diferencias entre ellos y otras reglas de firewall.

Reglas basadas en el tiempo Lógica

Cuando se trate de normas basadas en el tiempo, el calendario determina cuándo aplicar la acción especificada en la regla de firewall. Cuando la hora o la fecha actual no está cubierto por el programa, la acción de la regla es invertido. Por ejemplo, una regla que pasa el tráfico los sábados lo bloqueará cada dos días, sin tener en cuenta de cualesquiera normas posteriores definidas en el firewall. Las reglas se procesan de arriba hacia abajo, lo mismo que otras reglas de firewall. Se utiliza el primer partido, y una vez que se encuentra una coincidencia, se adopten las medidas y no
se evalúan otras reglas. Si está trabajando con una regla de pase en un horario determinado, por ejemplo sábado y Domingo, y que no tiene el efecto que se pretende entonces es posible que en lugar de tratar una regla de bloqueo para el lunes
a viernes.

Es importante recordar siempre al usar los horarios que la norma va a tener algún efecto si
que está dentro del tiempo programado o no. La norma no sólo va a ser saltado porque el tiempo actual es no dentro de la hora programada. Tenga esto en cuenta para asegurarse de que usted no permite que accidentalmente más Acceso de lo previsto con una regla programada. Tome este otro ejemplo: Si usted tiene una salida restrictiva políticas para el tráfico HTTP y desea programar las normas de tráfico HTTP, entonces usted tendrá que programar las reglas restrictivas, y no sólo tener una regla de bloqueo programado para el tráfico HTTP. En este ejemplo, la regla de bloqueo programado, cuando fuera de la hora programada, se convertirá en una norma pase HTTP manta y ignorar las reglas HTTP egreso más restrictivas.

Tiempo reglas basadas Advertencias

Debido a las reglas basadas vez utilizan ipfw lugar de PF, son incompatibles con el portal cautivo. Para el misma razón, multi-WAN y algunas de las otras capacidades de reglas de firewall avanzado tampoco están disponibles con reglas de tiempo basado.

Configuración de Horarios para Tiempo reglas basadas

Los horarios se definen en Firewall Horarios y calendario de cada uno pueden contener múltiples veces rangos. Una vez que se define un horario, entonces se puede utilizar para una regla de cortafuegos. En el siguiente ejemplo,
una empresa quiere negar el acceso a HTTP en horario de oficina, y permitir que el resto del tiempo.

Definición de tiempos para una programación

Para añadir una programación de Firewall Horarios, haga clic en. Esto debería abrir el calendario de la edición pantalla, como se ve en la Figura 10.23, "Adición de un intervalo de tiempo". El primer campo de esta pantalla es para la Nombre de la programación. 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 números, y sin 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 Horas de operación. Desde un programa se compone de uno o más
definiciones de rango de tiempos, deberá próxima definir un rango de tiempo antes de poder guardar el horario.

Un programa se puede aplicar a días específicos, tales como el 2 de septiembre de 2009 o para los días de la semana, como
De lunes a miércoles. Para seleccionar un día cualquiera en el próximo año, elija el mes de la lista desplegable la lista desplegable, a continuación, haga clic en el día específico o día 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 el Lun, Mar, Mie, Jue y vie Esta voluntad

hacer que el programa activo para todos los lunes a viernes, con independencia del mes. Ahora seleccione el tiempo en que este programa debe ser activo, en formato de 24 horas. Nuestro horario de atención serán 09:00 a 17:00 (17:00). Todas las horas se muestran en la zona horaria local. Ahora entrar en un rango de tiempo Descripción, como Trabajo
Semana, a continuación, haga clic en Agregar Time.

Una vez que el rango de tiempo se ha definido, aparecerá en la lista al final de la edición de horario pantalla, como en la Figura 10.24, "Alta Gama de tiempo".

Si hay más veces para definir, repetir este proceso hasta que esté satisfecho con los resultados. Para ejemplo, para ampliar esta configuración, puede haber un medio día del sábado para definir, o tal vez la tienda abre a última hora del lunes. En ese caso, definir un intervalo de tiempo para los días idénticos, y luego otro rango para cada día con diferentes tiempos. Esta colección de rangos de tiempo será el calendario completo. Cuando todos los intervalos de tiempo necesarios se han definido, haga clic en Guardar. A continuación, volver a la lista de programación, y
aparecerá el nuevo horario, como en la Figura 10.25, "Lista de programación después de añadir". Este programa le ahora estará disponible para su uso en las reglas del cortafuegos.

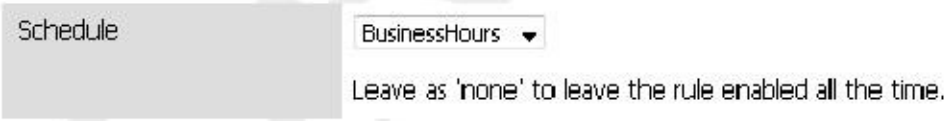
Figura 10.25. Programe lista después de agregar

Name	Time Range(s)			Description
BusinessHours	Mon - Fri	9:00-17:00	Work Week	Normal Business Hours

El uso de la Lista de que una regla de firewall

Para crear una regla de firewall que emplea este horario, debe agregar una regla en la interfaz deseada. Ver la sección "Adición de una regla de firewall" y la sección "Configuración de reglas del cortafuegos" para más información acerca de la adición y edición de reglas. Para nuestro ejemplo, agregar una regla para bloquear el tráfico TCP
en la interfaz LAN de la subred inalámbrica a internet, a cualquier destino en el puerto HTTP. Cuando se llega a el ajuste de Horario de elegir el horario que acabamos de definir, Businesshours, como en la figura 10.26, "La elección de un calendario para una regla de firewall".

Figura 10.26. La elección de un calendario para una regla de firewall



Después de guardar la regla, el programa le aparecerá en la lista de reglas de firewall, junto con una indicación de la estado activo de horario. Como se puede ver en la Figura 10.27, "Firewall Listado de reglas con el horario", se trata de una
bloquear regla, pero la columna de la agenda es lo que indica que la norma actualmente no se encuentra en su bloqueo activo
estado, ya que se está viendo en un momento en que está fuera de la gama prevista. Si pasa el ratón por encima del programar nombre, se mostrará las horas definidas para ese horario. Si se pasa sobre el estado horario indicador, le informará de manera descriptiva cómo la regla se está comportando en ese punto en el tiempo. Dado que este está siendo
visto fuera de los horarios definidos en nuestro programa businesshours, esta dirá "juego Traffic se está permitiendo actualmente esta regla. "Si hubiéramos utilizado una regla de pase, lo contrario sería cierto.

Figura 10.27. Firewall Listado de reglas con el Anexo

	Proto	Source	Port	Destination	Port	Gateway	Schedule	Descrip
	TCP	LAN net	*	*	80 (HTTP)	*	BusinessHours	Block We during B Hours

Ahora que la regla está definida, asegúrese de probarlo tanto dentro como fuera de las horas precisas para asegurar que el comportamiento deseado es promulgada. También hay que tener las advertencias de reglas basadas en el tiempo (la sección llamada "El tiempo
Basado en normas Advertencias ") en cuenta a la hora de artesanía estas reglas.

Ver los Registros del cortafuegos

Para cada regla que se establece para iniciar, y el valor predeterminado regla de rechazo, se realiza una entrada en el registro. Hay varias maneras
para ver estas entradas de registro, con diferentes niveles de detalle, y no hay un método claro "mejor".

Al igual que otros registros en pfSense, los registros del firewall sólo mantienen un cierto número de registros. Si las necesidades de los
su organización requiere que usted mantenga un registro permanente de los registros del firewall durante un período de tiempo
tiempo, ver la sección "Registros del sistema" para obtener información sobre la copia de estas entradas del registro a un syslog

Visualización de las WebGUI

Los registros del cortafuegos son visibles desde la WebGUI, y pueden encontrarse en Estado Registros del sistema, en la ficha Firewall. Puede consultar cualquiera de los registros analiza, que son más fáciles de leer, o los registros de primas, que tienen
más detalle si entiendes formato de registro de PF. También hay un ajuste para los registros del sistema que mostrará estas entradas en orden normal o inverso. Si no está seguro en el que ordenar las entradas del registro son que aparece, seleccione la fecha y hora de la primera y última líneas, o revise la sección titulada "Registros del sistema" para obtener información sobre cómo ver y cambiar estos valores.

Los registros WebGUI analizados, vistos en la Figura 10.28, "Ejemplo de las entradas del registro se ve desde la WebGUI", son
en 6 columnas: Acción, Tiempo, Interface, origen, destino, y el Protocolo. Acción muestra lo que sucedió al paquete que generó la entrada del registro, ya sea de paso, bloquear o rechazar. El tiempo es el tiempo que el paquete llegó. La interfaz es donde el paquete entró pfSense. La fuente es la dirección IP de origen y el puerto. Destino es la dirección IP de destino y el puerto. Protocolo es el protocolo del paquete, ya sea de ICMP, TCP, UDP, etc

Figura 10.28. Entradas del registro Ejemplo vistos desde los WebGUI

Act	Time	If	Source	Destination
⊠	Jul 16 20:54:05	WAN	0.0.0.0:68	255.255.255.255:67
⊠	Jul 16 20:56:05	WAN	0.0.0.0:68	255.255.255.255:67
⊠	Jul 16 21:05:05	WAN	0.0.0.0:68	255.255.255.255:67
⊠	Jul 16 21:06:05	WAN	0.0.0.0:68	255.255.255.255:67

El icono de acción es un vínculo que las operaciones de búsqueda y mostrar la regla que causó la entrada de registro. Más a menudo
que no, esto simplemente dice "Default Deny", pero al solucionar problemas de reglas que contribuyan a la reducción a los sospechosos.

Si el protocolo es TCP, también verá los campos extra aquí que representan indicadores TCP presentes en el paquete. Estos indican diversos estados de conexión o atributos de paquetes. Algunos de los más comunes son:

S - SYN	Sincronizar los números de secuencia. Indica un nuevo intento de conexión cuando sólo SYN está activado.
Un - ACK	Indica aceptación de los datos. Como se discutió anteriormente, estos son respuestas para que el remitente sepa los datos se recibieron en Aceptar.
F - FIN	Indica que no hay más datos del remitente, el cierre de una conexión.
R - RST	Conexión restablecida. El flag está puesto al responder a una solicitud para abrir una conexión en un puerto que no tiene un demonio que escucha. También puede ser establecido por el software de servidor de seguridad para rechazar las conexiones no deseadas.

Hay varias otras banderas y su significado se describen en muchos materiales en
el protocolo TCP. Como siempre, el artículo de Wikipedia sobre TCP [http://en.wikipedia.org/wiki/Transmission_Control_Protocol # TCP_segment_structure] tiene más información.

Viendo desde el Menú de consola

Los troncos sin procesar se pueden ver directamente en tiempo real desde la interfaz de registro de pf mediante la opción 10 desde
el menú de la consola. Un ejemplo sencillo es una entrada de registro al igual que la observada anteriormente en la Figura 10.28, "Ejemplo de sesión
Entradas vistos desde el WebGUI ":

```
000000 regla 54/0 (partido): bloquear en el vr1: 0.0.0.0.68> 255.255.255.255.67: BOOTP
```

Esto demuestra que la regla 54 fue igualado, lo que dio lugar a una acción de bloqueo en la `vr1` interfaz. La fuente y las direcciones IP de destino se muestran a continuación. Los paquetes de otros protocolos pueden mostrar de manera significativa
más datos.

Para ver imágenes de la Shell

Cuando se utiliza la cáscara sea desde SSH o desde la consola, hay numerosas opciones disponibles para ver los registros de filtro.

Al visualizar directamente los contenidos del archivo de obstrucción, las entradas del registro pueden ser bastante complejo y detallado.
Debería ser relativamente fácil seleccionar los distintos campos, pero en función del contexto del partido, puede ser más difícil.

Viendo el contenido actual del archivo de registro

El registro del filtro, como se discute en la apertura de este capítulo, está contenida en un fichero cíclico binario para que no puede utilizar las herramientas tradicionales como cat, grep, etc en el archivo directamente. El registro debe ser leído de nuevo con el
zueco programa, y luego pueden ser canalizado a través de cualquier programa que te gusta.

Para ver el contenido actual del archivo de registro, ejecute el siguiente comando:

```
#zueco / var / log / filter.log
```

Se mostrará todo el contenido del archivo de registro. Si usted está interesado sólo en las últimas líneas, usted puede él a través de la tubería cola de este modo:

```
#zueco / var / log / filter.log | cola
```

Tras la salida de registro en tiempo real

Para "seguir" a la salida del archivo de obstrucción, se debe utilizar el `-F` parámetro a obstruir. Este es el equivalente de tail-f para aquellos acostumbrados a trabajar con archivos normales de registro en los sistemas UNIX.

```
#obstruir-f / var / log / filter.log
```

Esta es la salida de todo el contenido del archivo de registro, pero no se cierra después. En su lugar, esperar a que más entradas y imprimirlos a medida que ocurren.

Viendo el resultado de registro analizado en la concha

Hay un analizador de registro sencillo escrito en PHP que puede ser utilizado a partir de la cáscara para producir una salida reducida
en lugar del registro prima completa. Para ver el contenido analizado de registro actual, ejecute:

```
#zueco / var / log / filter.log | php / usr / local / www / filterparser.php
```

Verá la salida de entradas una 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
```

Encontrar la regla que causó una entrada de registro

Cuando vea uno de los formatos de registro bruto, se muestra el número de la regla para una entrada. Usted puede utilizar esta
regla número para encontrar la regla que causó el choque. En el siguiente ejemplo, estamos tratando de encontrar lo que descartan es numerada 54.

#pfctl-vvsr | grep '^ @ 54'
```
@ 54 caída de bloques en el registro rápido todo etiqueta "Default
regla de rechazo"
```
Como puede ver, esta fue la denegación predeterminada
regla.

¿Por qué a veces veo bloqueado las entradas de registro para conexiones legítimas?

A veces, usted verá las entradas del registro que, si bien etiquetado con el "Default denegar" la regla, parece que pertenecer al tráfico legítimo. El ejemplo más común es ver una conexión bloqueada que implica una servidor web.

Esto es probable que ocurra cuando un paquete TCP FIN, que normalmente cerrar la conexión, llega después de que se ha eliminado el estado de la conexión. Esto sucede porque, en ocasiones, se pierde un paquete, y las retransmisiones serán bloqueados porque el servidor de seguridad ya ha cerrado la conexión.

Es inofensivo, y no indica una conexión bloqueada real. Todos los firewalls hacen esto, a pesar de algunos no se generan mensajes de registro para este tráfico bloqueado incluso si cierra la sesión todo el tráfico bloqueado.
Usted verá esto en alguna ocasión incluso si ha permitir que todas las reglas en todas las interfaces, como permitir a todos por
Conexiones TCP sólo permite que los paquetes TCP SYN. El resto del tráfico TCP o bien formar parte de una existente estado en la tabla de estado, o estarán paquetes con indicadores TCP falsificados.

Solución de problemas de reglas de firewall

En esta sección se proporciona orientación sobre qué hacer si las reglas del cortafuegos no se están comportando como usted desea
o esperar.

Revise sus registros

El primer paso para solucionar problemas de sospecha de tráfico bloqueado debe ser para revisar sus registros de cortafuegos
(Estado> Registros del sistema, en la ficha Firewall). Recuerde que, por defecto pfSense guardara todo el caído tráfico y no registrará ningún tráfico pasado. A menos que se agrega el bloque o rechazar las reglas que no utilizan la tala, todo el tráfico bloqueado siempre estará conectado. Si usted no ve el tráfico con una X roja junto a él en su los registros del firewall, pfSense no está disminuyendo el tráfico.

Parámetros de la regla de la opinión

Edite la regla en cuestión y revisar los parámetros que se han especificado para cada campo. Para TCP y Tráfico UDP, recuerda el puerto de origen es casi nunca el mismo que el puerto de destino, y deben suele ajustarse a cualquier. Si el defecto regla de rechazo es el culpable, puede ser necesario para elaborar una norma nueva que pase
coincidirá con el tráfico que necesita ser permitido.

Norma imperativa Comentario

Recuerde que los primeros triunfos de la regla coincidente - no se evalúan otras normas.

Normas e interfaces

Asegúrese de que sus normas están en la interfaz correcta de funcionar como es debido. Recuerde tráfico se filtra sólo por el conjunto de reglas configurado en la interfaz donde se inicia el tráfico. El tráfico procedente de un sistema de

en su LAN con destino a un sistema en cualquier otra interfaz se filtra por sólo las reglas de LAN. Lo mismo que es cierto para todas las demás interfaces.

Habilitar el registro de la regla

Puede ser útil para determinar qué regla se pongan en venta el tráfico en cuestión. Al habilitar el registro en sus reglas de paso, puede ver los registros del firewall y haga clic en una entrada individual para determinar qué norma aprobada el tráfico.

Solución de problemas con las capturas de paquetes

Capturas de paquetes puede ser muy valiosa para los problemas de tráfico de solución de problemas y la depuración. Usted puede saber si
el tráfico está llegando a la interfaz exterior en absoluto, o salir de la interfaz en el interior, entre muchos otros utiliza. Consulte el Capítulo 29, Captura de paquetes para más detalles sobre la solución de problemas con las capturas de paquetes y
tcpdump.

Capítulo 11. Network Address Traducción

En su uso más común, la traducción de direcciones de red (NAT) permite conectar múltiples ordenadores a Internet a través de una única dirección IP pública. pfSense permite estos despliegues simples, sino que también tiene capacidad para mucho más avanzado y configuraciones NAT complejas requeridas en las redes con múltiples direcciones IP públicas.

NAT se configura en dos direcciones - entrada y salida. NAT de salida define cómo el tráfico salga de la red destinado a Internet está traducido. Inbound NAT se refiere al tráfico que entra su red desde Internet. El tipo más común de NAT entrante y el más están familiarizados con es puerto remite.

Configuración de NAT por defecto

En esta sección se describe la configuración de NAT por defecto de pfSense. La frecuencia adecuada más Configuración de NAT se genera automáticamente. En algunos ambientes que se quiere modificar este configuración y pfSense permite totalmente a hacerlo - por completo de la interfaz web. Es un contraste de muchas otras distribuciones de servidor de seguridad de código abierto, que no permiten a las capacidades general, son necesarios en todo menos en las redes de pequeñas y sencillas.

Configuración predeterminada de NAT de salida

La configuración de NAT por defecto en pfSense con una interfaz de dos LAN y WAN despliegue traduce automáticamente el tráfico de Internet enlazado a la dirección IP de la WAN. Cuando múltiples interfaces WAN están configurados, el tráfico de dejar cualquier interfaz WAN se traduce automáticamente a la dirección de la Interfaz WAN está utilizando.

Puerto estático se configura automáticamente para IKE (parte de IPsec). Puerto estático se explica con más detalle en la sección llamada "salida NAT" sobre NAT Saliente.

Entrada predeterminado de configuración NAT

Por defecto, nada se deja en el Internet. Si usted necesita para permitir el tráfico iniciado en Internet a un host de la red interna, debe configurar forwards portuarias o NAT 1:1. Esto se trata en los próximos secciones.

Port Delanteros

Delante del puerto le permiten abrir un puerto, rango de puertos específico o protocolo para un tratado en privado dispositivo de la red interna. El nombre de "puerto hacia adelante" fue elegido porque es lo que la mayoría de la gente entender, y pasó a llamarse desde el más apropiado técnicamente "Inbound NAT" después de innumerables quejas de los usuarios confundidos. Sin embargo, es un poco de un nombre inapropiado, ya que se puede redirigir el GRE y Protocolos ESP, además de los puertos TCP y UDP. Esto es más comúnmente utilizado cuando se alojan los servidores, o el uso de aplicaciones que requieren conexiones entrantes de Internet.

Riesgos de Port Forwarding

En una configuración predeterminada, pfSense no deja en ningún tráfico iniciado en Internet. Esto proporciona la protección de nadie escanear el Internet en busca de sistemas para atacar. Cuando se agrega un puerto hacia adelante, pfSense permitirá que cualquier tráfico que coincide con la regla de firewall correspondiente. No conoce el diferencia de un paquete con una carga maliciosa y uno que es benigno. Si coincide con el firewall

regla general, está permitido. Usted necesita confiar en los controles host basado para asegurar cualquier servicio permitido a través de la
firewall.

Port Forwarding y Servicios Locales

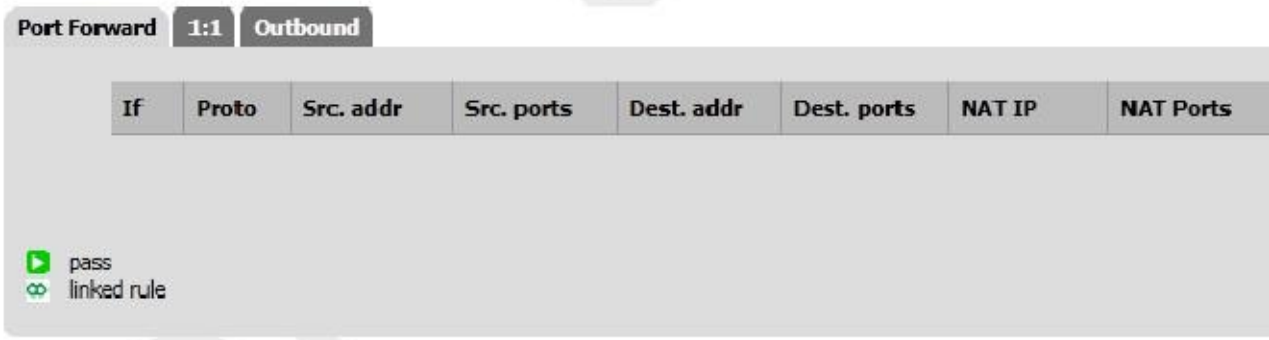
Delante del puerto tienen prioridad sobre cualquiera de los servicios que se ejecutan localmente en el servidor de seguridad, como por ejemplo la web
interfaz, SSH, y cualquier otro servicio que se esté ejecutando. Por ejemplo, esto significa que si usted permite que acceso a la interfaz web remota desde la WAN con HTTPS en el puerto TCP 443, si se agrega un puerto hacia adelante en WAN para TCP 443 que adelante el puerto va a funcionar y su acceso a la interfaz web de WAN
ya no funcionan. Esto no afecta el acceso a otras interfaces, sólo la interfaz que contiene la
puerto hacia adelante.

Adición de puertos Delanteros

Port Delanteros son gestionados en Firewall NAT, en la ficha Port Forward. Las reglas de esta pantalla
se manejen de la misma manera que las reglas del cortafuegos (ver la sección llamada "Introducción al Firewall Pantalla de las reglas ").

Para comenzar a agregar una entrada hacia delante del puerto, botón en la parte inferior muy superior o de la lista, como haga clic en el
indica en la Figura 11.1, "Añadir Port Forward".

Figura 11.1. Añadir Port Forward



Ahora va a estar mirando a la pantalla de edición Port Forward, que se muestra en la Figura 11.2, "Port Forward Ejemplo ", con las opciones por omisión elegidas. En primer lugar, seleccione la interfaz en la que desea agregar el puerto hacia adelante.
En la mayoría de los casos esto será WAN, pero si usted tiene un vínculo OPT WAN, o si esto será una redirección local puede ser otra interfaz. La interfaz es en la que se inicia el tráfico.

La selección del origen de su escondido detrás de un botón Opciones avanzadas por defecto, y ajustado a cualquier fuente. Este
le permite restringir el cual IP de origen pueden acceder a esta entrada delante del puerto. Si tiene que ser accesible desde cualquier lugar en Internet, la fuente debe ser cualquiera.

El destino se establece en la dirección IP en el que el tráfico que se remitirá está destinado inicialmente. Para el puerto hacia delante sobre la WAN, en la mayoría de los casos esto se debe establecer en WAN Dirección, o cuando usted tiene múltiples
IPs públicas, una IP virtual disponible (ver la sección llamada "IP virtual") en WAN.

El rango de puerto de destino es donde se especifica el puerto de destino original del tráfico, ya que es
Llegando por la Internet, antes de que sea redirigido al host de destino especificado. Si la transmisión de una sola puerto, introdúzcalo en el de: caja y dejar a: en blanco. También puede elegir entre una lista de los servicios comunes en el cuadro desplegable disponible.

Redireccionar target IP es la dirección IP en la que se remitió el tráfico, o técnicamente redirigido.

se establecería Protocolo TCP y el Margen de puertos externos para 5900. (Dado que este es un común puerto reenviado, que también está disponible en la lista desplegable de selección de puerto.)

La IP de destino de redireccionamiento es la dirección IP local a la que este puerto externo remitirá, y el redireccionamiento
puerto de destino es donde comenzará el rango de puertos reenviados. Si va a reenviar un rango de puertos, por ejemplo 19000-19100, sólo se especifica un punto de partida local, ya que los puertos deben coincidir uno a uno. Este campo le permite abrir un puerto diferente en el exterior que el anfitrión en el interior está escuchando en, por ejemplo de 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 sobre lo que el puerto hacia adelante hace o por qué existe.

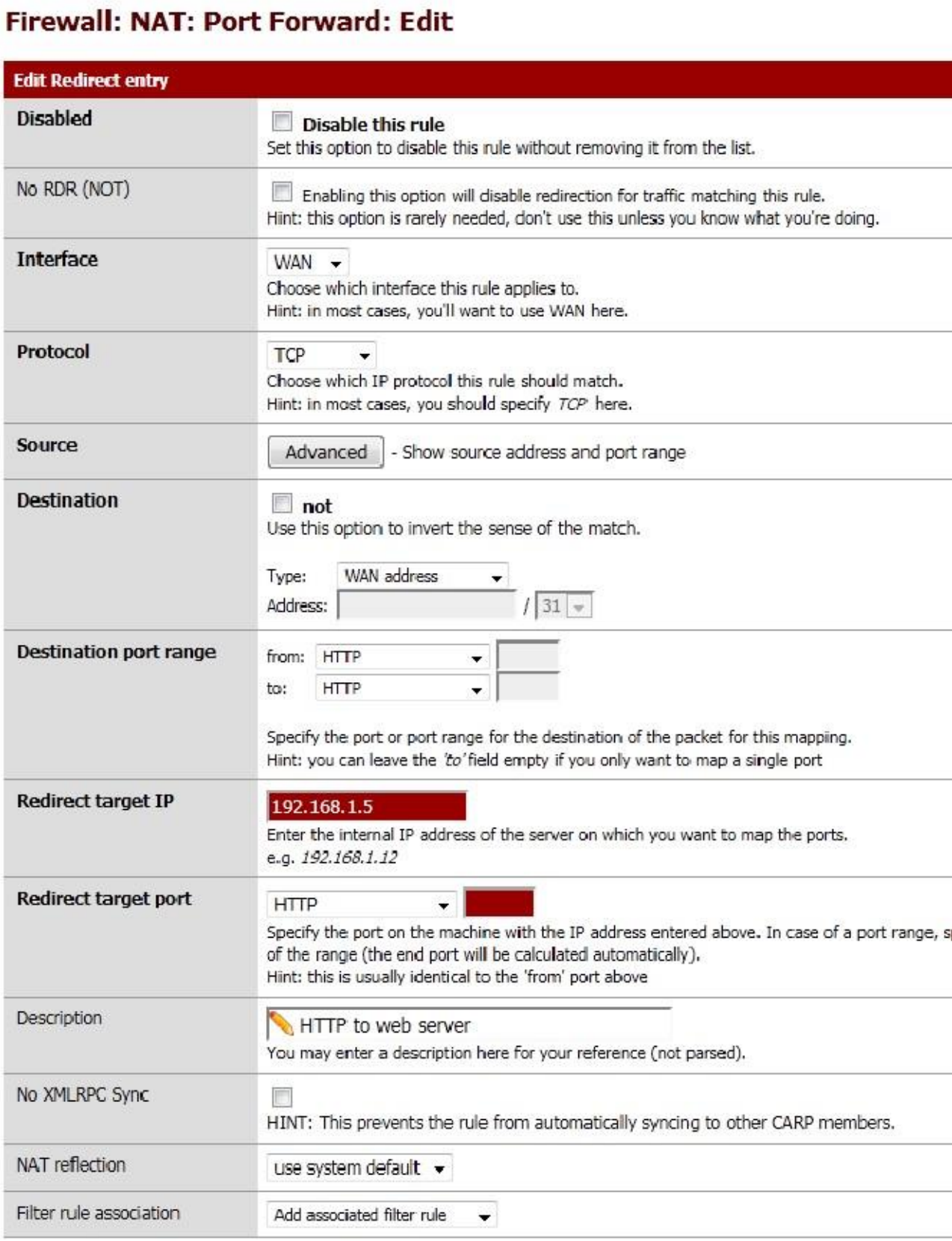
Si no está utilizando un clúster de conmutación por error CARP, saltar sobre la opción Sin XML-RPC Sync. Si es así, entonces
Marcando esta casilla evitará esta regla se sincronice con los otros miembros de una conmutación por error cluster (véase el Capítulo 24, Firewall de redundancia / alta disponibilidad), que es generalmente indeseable.

La última opción es muy importante. La entrada hacia adelante puerto simplemente define que el tráfico debe ser redirigida, se requiere una regla de firewall para pasar todo el tráfico a través de esa redirección.

Haga clic en Guardar cuando haya terminado, y luego en
Aplicar cambios.

En la Figura 11.2, "Ejemplo Port Forward" no es un ejemplo de la pantalla de edición de avance puerto lleno con la configuración adecuada para transmitir por HTTP entrante en WAN destinados a la IP WAN para interior 192.168.1.5 sistema.

Figura 11.2. Port Forward Ejemplo



Después de hacer clic en Guardar, se le llevará de nuevo a la lista delante del puerto, y verá la recién creada entrada como en la Figura 11.3, "Port Forward List".

Figura 11.3. Puerto Lista de reenvío

Es posible que desee volver a comprobar la regla de firewall, como se ve en Cortafuegos Normas sobre la ficha de la interfaz en la que se creó el delantero puerto. Se mostrará que el tráfico se permitirá en el
IP interna en el puerto adecuado, como se muestra en la Figura 11.4, "Port Forward Firewall Rule".

Figura 11.4. Port Forward Firewall Rule

Usted tendrá que restringir el Fuente de la norma genera automáticamente cuando sea posible. Para que las cosas tales como correo y servidores web que por lo general tienen que ser ampliamente accesible, esto no es práctico, pero para
servicios de gestión remota, como SSH, RDP y otros, es probable que sólo un número pequeño
de los ejércitos que deberían ser capaces de conectarse a través de los protocolos en un servidor de todo el Internet. Crear un alias de hosts autorizados, y el cambio de la fuente de cualquier al alias es mucho más seguro
de dejar la fuente abierta a toda la Internet. Es posible que desee probar primero con el irrestricto
fuente, y después de comprobar que funciona como se desea, restringir la fuente que se desee.

Si todo se ve bien, el delantero de puerto debe funcionar cuando se prueba fuera de su red. Si
algo salió mal, vea la sección llamada "Port Forward Solución de problemas" más adelante en este capítulo.

Port Forward Limitaciones

Sólo puede reenviar un único puerto a un host interno para cada dirección IP pública que tiene disponible. Por ejemplo, si sólo tiene una dirección IP pública, sólo puede tener un servidor web interno
que utiliza el puerto TCP 80 para garantizar el tráfico web. Cualquier servidor adicional tendrían que utilizar puertos alternativos
tales como 8080. Si usted tiene cinco direcciones IP públicas disponibles configurados como IPs virtuales, podría Tiene cinco servidores web internos que utilizan el puerto 80. Vea la sección llamada "IP virtual" para más información sobre
Las direcciones IP virtuales.
Hay un poco común, pero a veces es aplicable la excepción a esta regla. Si necesita enviar un
en particular el puerto a un host interno específico sólo para ciertas direcciones IP de origen y reenviar el mismo puerto a un
host diferente para otras direcciones IP de origen, esto es posible mediante la especificación de la dirección de origen en el puerto delantero
entradas.
Para que los forwards de puerto en WAN direcciones para ser accesible mediante el uso de sus respectivas IP WAN tratar de interfaces internas frente, usted tendrá que configurar NAT reflexión que se describe en
la sección llamada "Reflexión NAT". Usted siempre debe probar sus forwards puerto de un sistema en un diferente de conexión a Internet, y no desde dentro de su red.

Servicio de Auto-Configuración con UPnP

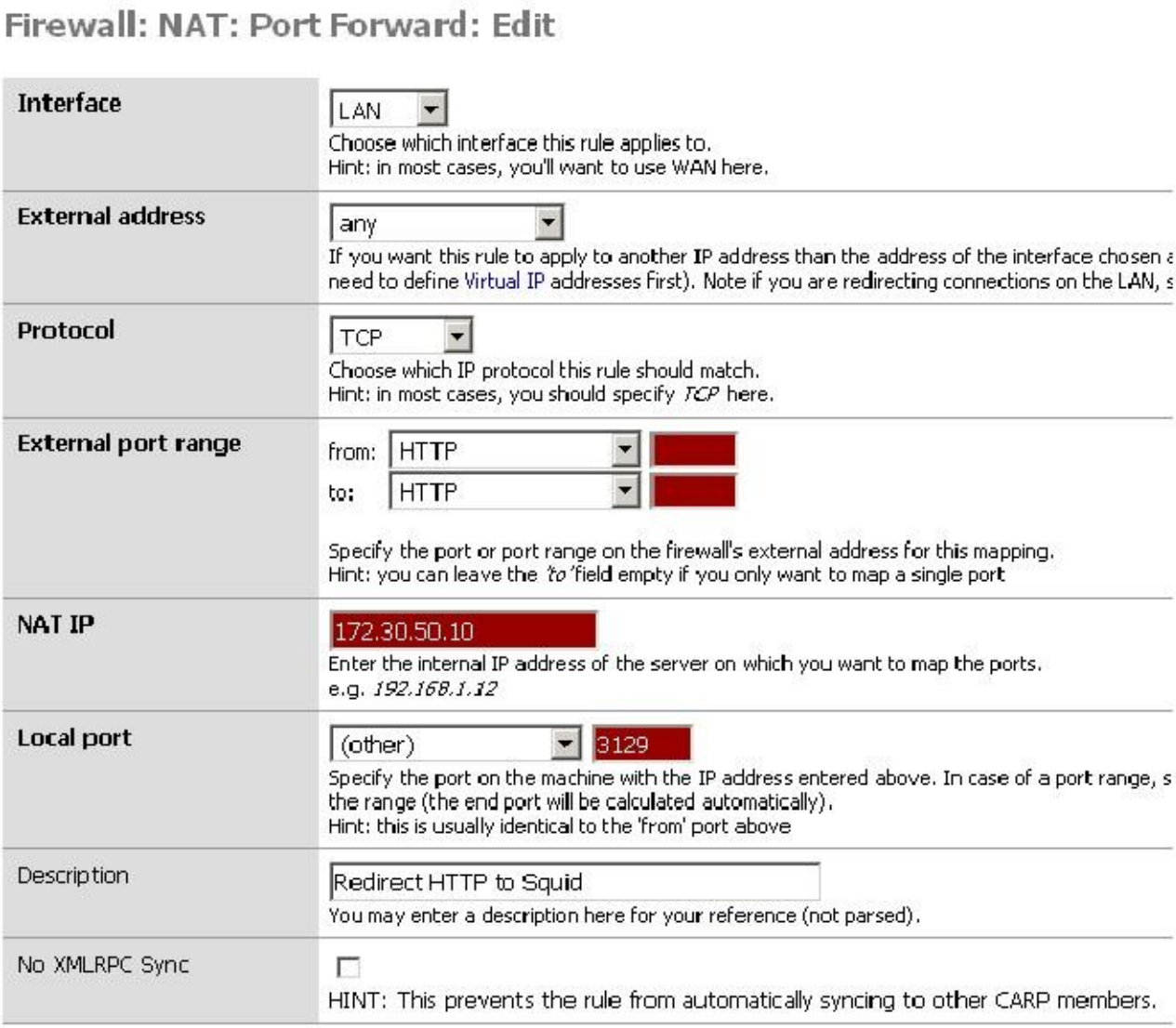
Algunos programas ahora son compatibles con Universal Plug-and-Play (UPnP) para configurar automáticamente los puertos NAT
forwards y reglas de firewall. Aún más problemas de seguridad se aplican allí, pero en casa utilizan los beneficios a menudo
superan cualquier preocupación potencial. Vea la sección "UPnP" para obtener más información sobre la configuración y el uso de UPnP.

La redirección de tráfico con puerto reenvía

Otro uso de los delanteros del puerto es para redirigir de forma transparente el tráfico desde la red interna. Puerto forwards que especifican la interfaz LAN u otra interfaz interna se redirigir el tráfico que coincide con el reenviar al destino especificado. Esto es más comúnmente utilizado para hacer proxy transparente HTTP tráfico a un servidor proxy, o redirigir todo SMTP saliente a un servidor.

La entrada NAT se muestra en la Figura 11.5, "Ejemplo de redirección del puerto hacia adelante" es un ejemplo de una configuración
que va a redirigir todo el tráfico HTTP que entra en la interfaz LAN en Squid (puerto 3129) en el host 172.30.50.10.

Figura 11.5. Ejemplo redirigir puerto delantero



NAT 01:01

01:01 (pronunciado uno a uno) NAT mapea una dirección IP pública a una dirección IP privada. Todo el tráfico desde ese privada
IP en Internet y se asigna a la dirección IP pública se define en el 1:01 asignación de NAT, anulando su Configuración de NAT Saliente. Todo el tráfico iniciado en Internet destinado al público especificada
IP será traducido a la IP privada, y luego evaluadas por el servidor de seguridad conjunto de reglas WAN. Si el tráfico es permitido por las reglas del cortafuegos, será pasado al host interno.

Los riesgos de la NAT 01:01

Los riesgos de NAT 1:01 son en gran parte los mismos que hacia delante del puerto, si permite que el tráfico a ese host en su
Reglas de firewall WAN. Cada vez que usted permite que el tráfico, usted está permitiendo el tráfico potencialmente perjudicial en
su red. Hay un riesgo añadido ligera cuando se utiliza NAT 1:01 en que los errores de reglas de cortafuegos puede tener consecuencias más nefastas. Con entradas de remitir el puerto, que está limitando el tráfico que se permitirá dentro de la regla de NAT, así como la regla de firewall. Si usted transfiere hacia adelante el puerto TCP 80, añadiendo además un permitir que todos
pronunciarse sobre la WAN, sólo TCP 80 en ese host interno será accesible. Si usted está usando NAT 1:1 y agregar un deje todo dominio sobre WAN, todo en ese host interno será accesible desde Internet.
Errores de configuración son siempre un peligro potencial, y esto por lo general no deben considerarse una razón para evitar NAT 01:01. Hemos de tener en cuenta este hecho cuando se configuran las reglas del cortafuegos, y como siempre,
[Illegible] evitar todo lo que no se requiere.

Configuración de NAT 01:01

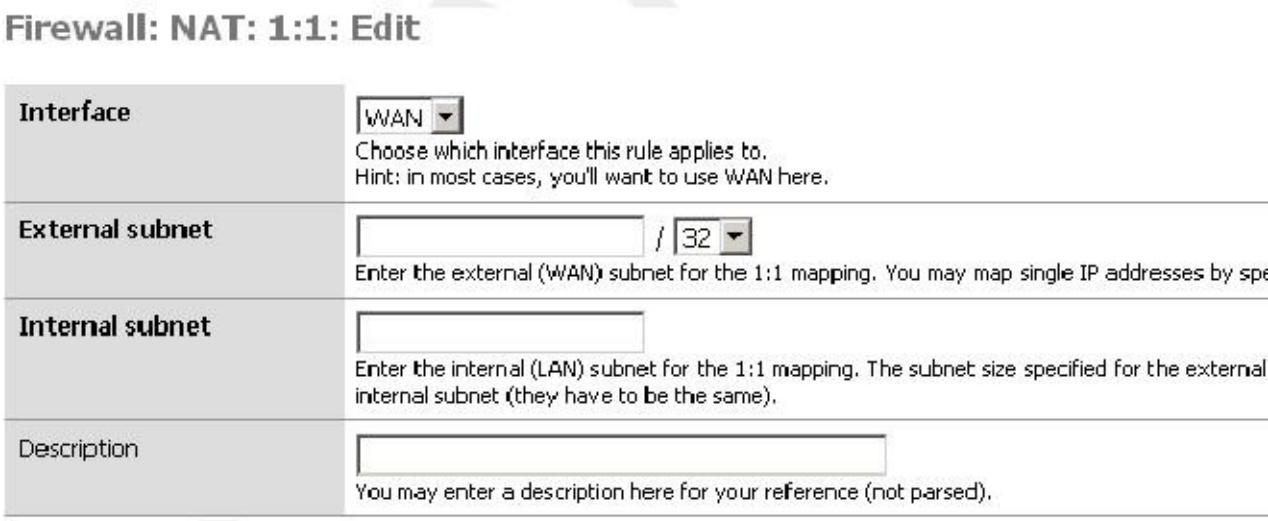
Para configurar NAT 1:1, primero agregar una IP virtual para la IP pública que se utilizará para la entrada NAT 1:1 como se describe en la sección llamada "IP virtual". Luego vaya a Firewall NAT y haga clic en la pestaña 01:01.

Clic  para añadir una entrada 01:01.

01:01 Campos de entrada de NAT

Figura 11.6, "01:01 de pantalla NAT Editar" muestra la pantalla NAT Edit 01:01, luego cada campo se detallará.

Figura 11.6. 01:01 pantalla NAT Editar



Interfaz

La caja de interfaz es donde se selecciona la ubicación de la subred externa. Esto es casi siempre su WAN o una interfaz OPT WAN en implementaciones multi-WAN.

Subred externa

La subred externa es donde se define la dirección IP pública o rango de direcciones IP para la asignación 1:1. Esto puede ser una única dirección IP mediante la especificación de una máscara / 32, o un rango CIDR seleccionando otra máscara.

Subred interna

La subred interna es donde se especifica la dirección IP interna o rango de direcciones IP para la asignación 1:1. Esta dirección IP o rango deben ser alcanzable en una de sus interfaces internas, ya sea directamente en una subred conectada, o una accesible a través de la ruta estática.

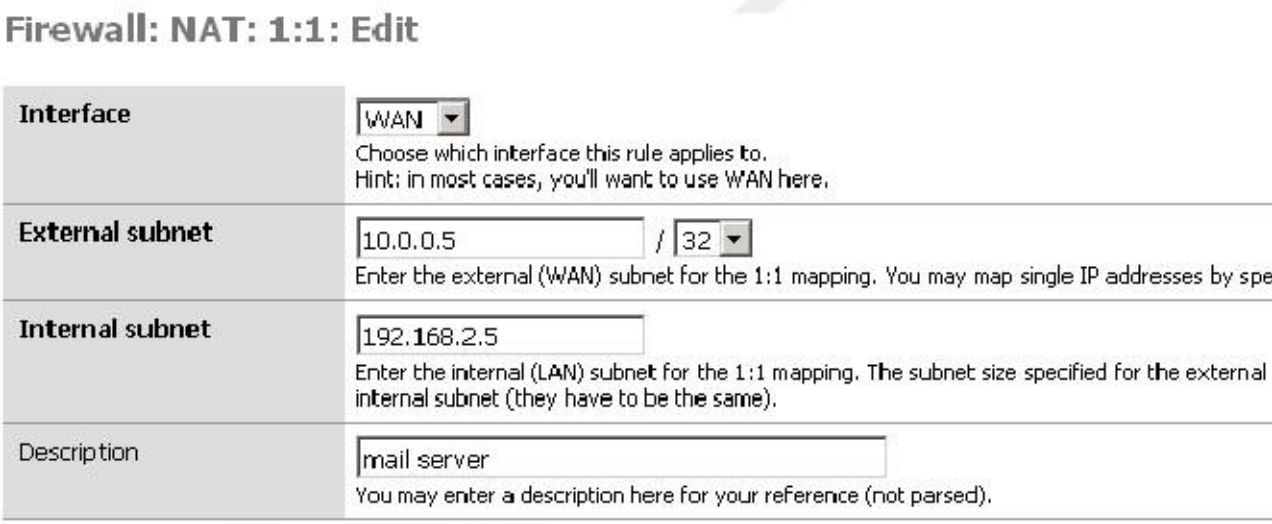
Descripción

Este es un campo opcional que no afecta el comportamiento de la entrada NAT 1:1. Rellena algo que le permitirá identificar fácilmente esta entrada cuando se trabaja con el servidor de seguridad en el futuro.

Ejemplo única configuración IP 01:01

Esta sección le mostrará cómo configurar una entrada de 01:01 NAT con una única IP interna y externa. En este ejemplo, 10.0.0.5 es una IP virtual en la WAN. En la mayoría de las implementaciones de este será sustituido por una de sus direcciones IP públicas. El servidor de correo está configurado para esta correspondencia se encuentra en un DMZ
segmento utilizando 192.168.2.5 IP interna. El 01:01 entrada NAT para mapear 10.0.0.5 a 192.168.2.5 se muestra en la Figura 11.7, "01:01 Entrada NAT". Un diagrama que representa esta configuración es en la Figura 11.8, "1:01 NAT Ejemplo - Single dentro y fuera de IP ".

Figura 11.7. 01:01 Entrada NAT



Ejemplo de configuración IP gama 01:01

NAT 01:01 se puede configurar para varias direcciones IP públicas mediante el uso de rangos CIDR. CIDR es el resumen cubierto en la sección llamada "CIDR Summarization". Esta sección cubre la configuración de NAT 01:01 para un rango CIDR / 30 de IPs.

Tabla 11.1. / 30 mapeo CIDR - juego octeto final

IPs externas	IPs internas
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

El último octeto de la dirección IP no es necesariamente el mismo en el interior y el exterior, pero yo recomiendo hacerlo siempre que sea posible. Por ejemplo, la Tabla 11.2, "/ 30 mapeo CIDR - no coincidentes definitiva octeto "también sería válido.

Tabla 11.2. / 30 mapeo CIDR - no coincidentes octeto final

IPs externas	IPs internas
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

Recomiendo elegir un esquema de direccionamiento en el que el último octeto coincide, porque hace que su la red más fácil de entender y por lo tanto mantener. Figura 11.9, "01:01 entrada NAT para / 30 rango CIDR" muestra cómo configurar NAT 1:01 para lograr la asignación que figuran en la Tabla 11.1, "/ 30 mapeo CIDR - A juego octeto final ".

NAT 01:01 en la IP WAN, también conocido como "zona de distensión" en Linksys

Algunos routers de consumo como los de Linksys tienen lo que llaman una función de "zona de distensión" que reenviará todos los puertos y protocolos destinados a la dirección IP de WAN a un sistema de la LAN. En efecto, este es 1:01 NAT entre la dirección IP de la WAN y la dirección IP del sistema interno. "DMZ" en ese contexto, sin embargo, no tiene nada que ver con lo que una red DMZ real es en la terminología de red real. En De hecho, es casi todo lo contrario. Un host en una verdadera zona de distensión está en una red aislada lejos de la otros equipos de una LAN, asegurados fuera de Internet y LAN acoge por igual. En contraste, un anfitrión "DMZ" en el significado de Linksys es no sólo en la misma red que los hosts de la LAN, pero completamente expuesto a tráfico entrante sin ninguna protección.

En pfSense, usted puede tener NAT activa en la IP WAN 01:01, con la advertencia de que dejará todos los servicios que se ejecuta en el servidor de seguridad en sí inaccesible desde el exterior. Entonces, ¿dónde está ejecutando VPNs de cualquier tipo, u otros servicios locales en el servidor de seguridad que deben ser accesibles externamente, no se puede utilizar NAT 01:01 con su WAN IP.

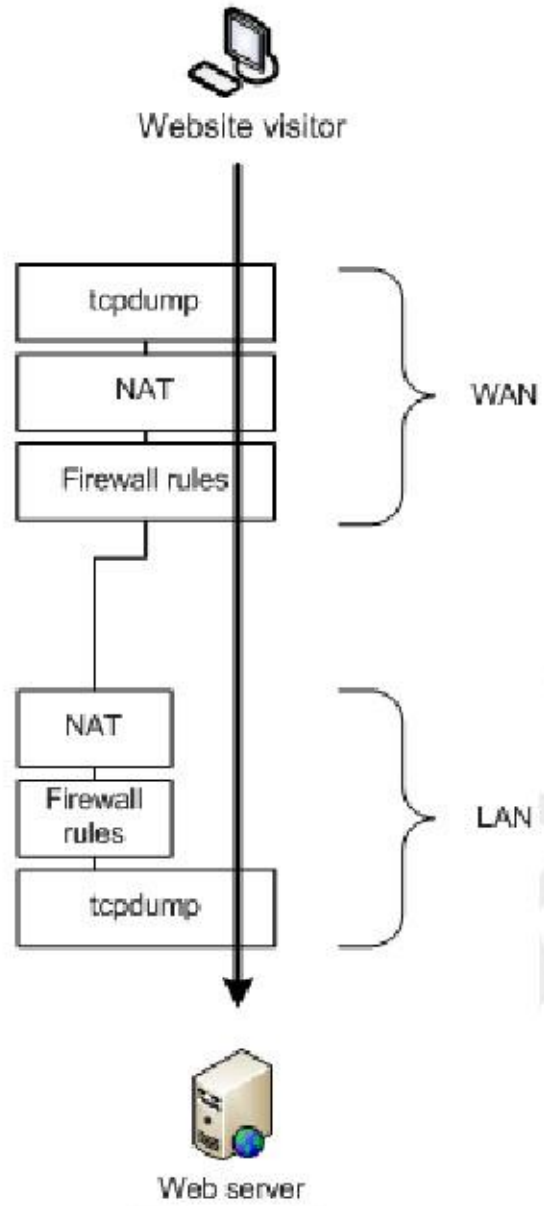
Ordenamiento de NAT y Procesamiento de Firewall

Entender el orden en que los cortafuegos y NAT se produce es importante si desea configurar NAT y las reglas del cortafuegos. La Figura 11.10, "Ordenamiento de NAT y Procesamiento Firewall" ilustra este ordenamiento. También representa donde tcpdump en lazos, ya que su uso como una herramienta de solución de problemas se describirá más adelante en este libro (véase el Capítulo 29, Captura de paquetes).

Cada capa no siempre es golpeado. Figura 11.11, "LAN a WAN Processing" y la Figura 11.12, "WAN a Procesamiento de LAN "ilustran que se aplican capas de tráfico iniciados desde la LAN va a la WAN, y también para el tráfico iniciado en la WAN va a LAN (cuando se permite este tipo de tráfico).

Para el tráfico de LAN a WAN, primero se evalúan las reglas del cortafuegos, a continuación, se aplica el NAT saliente si se permite el tráfico. La WAN, con NAT y reglas de firewall no se aplican al tráfico iniciado en la LAN.

Figura 11.12. WAN a LAN Procesamiento



Para el tráfico iniciado en la WAN, NAT se aplica en primer lugar, a continuación, las reglas de firewall.

Tenga en cuenta que tcpdump es siempre la primera y la última cosa a ver el tráfico - en primer lugar en la interfaz de entrada, antes de cualquier NAT y el procesamiento de firewall, y el último en la interfaz de salida. Muestra lo que está en la de alambre. (Consulte el Capítulo 29, Captura de paquetes)

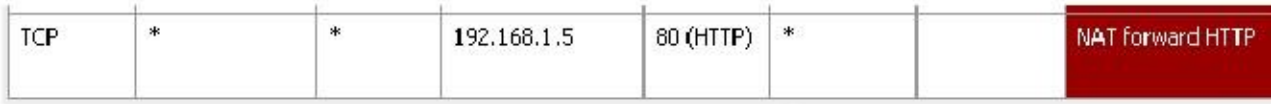
Extrapolando a interfaces adicionales

Los diagramas anteriores ilustran sólo un básico de dos interfaces LAN y WAN despliegue. ¿Cuándo trabajar con servidores de seguridad con OPT OPT WAN y las interfaces, se aplican las mismas reglas. Todas las interfaces OPT se comportan de la misma como Wi-Fi, y todas las interfaces WAN OPT se comportan de la misma como WAN. El tráfico entre dos interfaces internas se comporta igual que el tráfico de LAN a WAN, aunque las reglas de NAT por defecto no lo hará traducir el tráfico entre interfaces internas por lo que la capa de NAT no hace nada en esos casos. Si definir reglas de NAT salientes que coinciden con el tráfico entre interfaces internas, se aplicará como se muestra.

Las reglas para NAT

Para las reglas sobre interfaces WAN o OPT WAN, porque NAT traduce la IP de destino del tráfico antes de que las reglas de firewall evaluarlo, las reglas del firewall WAN siempre deben especificar la IP privada abordar como el destino. Por ejemplo, al agregar un puerto con interés para el puerto TCP 80 en WAN y marque la casilla Auto-añadir regla de firewall, esta es la regla de firewall que resulta en WAN. La IP interna en el delantero de puerto es 192.168.1.5. Si el uso de forwards portuarias o 1:01 NAT, las reglas de firewall en todos WAN interfaces deben utilizar la IP interna como dirección de destino. Consulte la Figura 11.13, "regla de cortafuegos para Port Forward para LAN Host "para un ejemplo de cómo debe aparecer una norma de este tipo.

Figura 11.13. Regla de Firewall de Port Forward para LAN Host



Reflexión NAT

NAT reflexión se refiere a la capacidad de acceder a los servicios externos de la red interna por el público IP, lo mismo que usted haría si estuviera en Internet. Muchos firewalls comerciales y de código abierto hacen no es compatible con esta funcionalidad en absoluto. pfSense tiene soporte tanto limitada para la reflexión NAT, aunque algunos entornos requieren una infraestructura DNS dividida para dar cabida a esta funcionalidad. División DNS se trata en la sección llamada "Split DNS".

Configuración y uso de Reflexión NAT

Para activar la reflexión NAT, busque el Sistema Página Avanzadas. Desplácese hacia abajo en Red Traducción de direcciones y desactive la casilla de Reflexión Desactivar NAT como se muestra en la Figura 11.14, "Habilitar
Reflexión NAT ". Haga clic en Guardar, y NAT reflexión se habilitará. No se necesita ninguna configuración adicional, va a trabajar de inmediato.

Figura 11.14. Habilitar Reflexión NAT

Advertencias Reflexión NAT

Reflexión NAT es siempre un poco de un truco, ya que los bucles de tráfico a través del firewall. Debido a la limitada Opciones pf prevé la adaptación de estos escenarios, hay algunas limitaciones en el NAT pfSense aplicación reflexión. Rangos de puertos de más de 500 puertos no tienen reflejo NAT habilitado y NAT 01:01 no es compatible. Dividir el DNS es el único medio para acoger grandes rangos de puertos y 01:01 NAT. Me encantaría decirte que esta situación mejore en pfSense 2.0, pero eso es poco probable debido a los retos de la manipulación de este dan los límites del software subyacente. El mantenimiento de un DNS dividido infraestructura es requerido por muchos servidores de seguridad comerciales, incluso, y por lo general no es un problema.

DNS de Split

Una alternativa preferible a la reflexión NAT está desplegando una infraestructura DNS dividida. Dividir el DNS se refiere
a una configuración de DNS en el DNS de Internet tiene sus IPs públicas y DNS en su red interna tiene por las IPs internas, privadas. Los medios para conseguir esto variará Dependiendo de las características específicas de su infraestructura de DNS, pero el resultado final es el mismo. Se omite la
necesidad de NAT reflexión mediante la resolución de nombres de host a las direcciones IP privadas dentro de su red.

DNS Forwarder anulaciones

Si utiliza pfSense como su servidor DNS para los hosts internos, puede utilizar las anulaciones de reenviador DNS lograr una implementación DNS dividido. Para agregar un reemplazo para el reenviador DNS, vaya a Servicios

 Forwarder DNS y haga clic theund "Usted puede entrar en los registros que anulan los resultados de la forwarders inferiores ", como se indica en la Figura 11.15," Añadir DNS Forwarder Override ".

Esto trae a colación el reenviador DNS: pantalla Editar host. La Figura 11.16, "Add DNS Forwarder Invalidar para example.com "y la Figura 11.17," Anulación de Forwarder DNS www.example.com " muestran ejemplos de DNS anula para example.com y www.example.com.

Usted tendrá que agregar un reemplazo para cada nombre de host en uso detrás de su firewall.

Los servidores DNS internos

Si utiliza otros servidores DNS de la red interna, como es común cuando se utiliza Microsoft Active Directory, tendrá que crear zonas para todos los dominios que organice dentro de su red, a lo largo de con todos los demás registros de los dominios (A, CNAME, MX, etc.)

En entornos que utilizan el servidor DNS BIND donde el DNS público está alojado en el mismo servidor como el DNS privada, vistas de BIND función se utiliza para resolver DNS diferente para hosts internos que los externos. Si está utilizando un servidor DNS diferente, puede soportar una funcionalidad similar. Revise su documentación para obtener información.

NAT Saliente

Controla NAT Saliente cómo se traduce el tráfico que sale de la red. Para configurarlo, visita el Firewall NAT página y elija la ficha de salida. Hay dos opciones de configuración para NAT Saliente en pfSense, la generación automática de reglas NAT saliente y saliente Manual NAT generación (Advanced Outbound NAT (AON)). En redes con una única dirección IP pública por la WAN, generalmente no hay razón para que AON. En entornos con múltiples direcciones IP públicas, esto puede ser deseable. Para entornos de uso de CARP, es importante para el tráfico de salida NAT para una dirección IP CARP dirección, como se discutió en el Capítulo 24, Firewall de redundancia / alta disponibilidad.

Por defecto salientes reglas NAT

Cuando se utiliza el valor por defecto de salida automática NAT, pfSense creará automáticamente las reglas de NAT la traducción de tráfico de dejar cualquier red interna a la dirección IP de la interfaz WAN que el tráfico deja.

Puerto estático

Por defecto, pfSense reescribe el puerto de origen en todos los paquetes salientes. Muchos sistemas operativos hacen un mal trabajo de la aleatorización de puerto de origen, si lo hacen en absoluto. Esto hace que la suplantación de IP más fácil, y marcas
Es posible tomar las huellas dactilares hosts detrás de su firewall de su tráfico saliente. La reescritura de la fuente puerto elimina estos potenciales (pero improbable) vulnerabilidades de seguridad.

Sin embargo, esto rompe algunas aplicaciones. No se construyen en las reglas cuando Advanced Outbound NAT es que personas con discapacidad, no hagas esto para UDP 500 (IKE para el tráfico VPN), ya que casi siempre se romperá reescribiendo el puerto de origen. El resto del tráfico tiene el puerto de origen reescrito por defecto.

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, es necesario utilizar la opción de puerto estático. Clic

Firewall NAT y la ficha de salida. Haga clic en Manual generación regla NAT saliente (avanzada Outbound NAT (AON)) y haga clic en Guardar. A continuación, verá una regla en la parte inferior de la página etiquetada
Auto creó regla para LAN. Haga clic en el botón a la derecha de esa norma para editarlo. Verifique la estática

Cuadro Puerto en esa página, y haga clic en Guardar. Aplicar cambios. Después de hacer ese cambio, el puerto de origen en
se conservará el tráfico saliente.

Desactivación de NAT de salida

Si está utilizando direcciones IP públicas en interfaces locales, y por lo tanto no es necesario aplicar NAT al tráfico que pasa a través del servidor de seguridad, debe desactivar NAT para esa interfaz. Para hacer esto, debe primero cambie la configuración de NAT de salida al Manual NAT de salida, y luego en Guardar. Después de hacer que cambian, aparecerán una o más reglas en la lista en la pantalla NAT Saliente. Eliminar la regla o reglas para las subredes IP públicas haciendo clic en cada línea una vez (o marque la casilla al comienzo de la línea) y luego

haga clic en  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 suprimido, NAT saliente ya no estará activo para esas direcciones, y pfSense entonces las direcciones IP públicas de ruta sin necesidad de traducción.

Para NAT saliente desactivar completamente, borrar todas las reglas que están presentes cuando se usa Manual NAT Saliente.

Elegir una configuración NAT

Su elección de la configuración NAT dependerá principalmente del número de direcciones IP públicas que tiene y número de sistemas que requieren acceso entrante desde Internet.

Soltero IP pública por WAN

Cuando sólo tiene una sola dirección IP pública por la WAN, las opciones de NAT son limitadas. Sólo se puede utilizar NAT 1:1 con IPs virtuales, no con IPs WAN. En este caso, sólo puede usar puerto remite.

Múltiples IPs públicas por WAN

Con varias direcciones IP públicas por WAN, tiene numerosas opciones para su NAT entrante y saliente configuración. Forwards portuarias, 01:01 NAT, y Advanced Outbound NAT pueden todos ser deseable en algunos circunstancias.

NAT y compatibilidad Protocolo

Algunos protocolos no funcionan bien y otras no en absoluto con NAT. Algunos protocolos de insertar direcciones IP dentro de paquetes, algunos no funcionan correctamente si el puerto de origen se vuelve a escribir, y algunos son difíciles porque
de limitaciones de PF. Esta sección cubre los protocolos que tienen dificultades con NAT en pfSense, y cómo evitar estos problemas cuando sea posible.

FTP

FTP plantea problemas tanto con NAT y servidores de seguridad debido al diseño del protocolo. FTP fue inicialmente diseñado en la década de 1970, y el estándar actual definición de las especificaciones del protocolo fue escrito en 1985. Desde FTP fue creada hace más de una década antes de la NAT, y mucho antes de que los servidores de seguridad
eran comunes, que hace algunas cosas que son muy NAT y firewall hostil. pfSense utiliza dos diferentes aplicaciones de proxy FTP, pftpx y ftpsesame. pftpx se utiliza para todos los escenarios de NAT, mientras ftpsesame Alojamiento para puente y el enrutamiento de IPs públicas.

FTP Limitaciones

Debido pf carece de la capacidad para manejar adecuadamente el tráfico FTP sin un proxy, y el proxy FTP pfSense aplicación es un poco deficiente, hay algunas restricciones en el uso de FTP.1

[1]En pfSense 2.0, el proxy ftp y ayudantes relacionadas han sido eliminados y todas estas funciones se manejan a la perfección en un más robusto camino en el interior del núcleo.

Conexiones de cliente FTP a Internet

Conexiones de cliente FTP siempre utilizarán la interfaz WAN principal y no pueden usar cualquier red WAN OPT interfaces. Más información sobre esto se puede encontrar en el capítulo 15, Múltiples conexiones WAN

Servidores FTP detrás de NAT

Servidores FTP detrás de NAT deben utilizar el puerto 21, como el proxy FTP sólo se iniciará cuando se especifica el puerto 21.

Modos de FTP

Modo Activo

Con Active Modo FTP, cuando se solicita una transferencia de archivos, la cliente escucha en un puerto local, y luego indica al servidor la dirección IP del cliente y el puerto. El servidor se conectará de nuevo a esa dirección IP y puerto con el fin de transferir los datos. Este es un problema para los cortafuegos porque el puerto es típicamente al azar, aunque los clientes modernos permiten la limitación de la gama que se utiliza. Como habrás adivinado, en el caso de un cliente detrás de NAT, la dirección IP dada sería una dirección local, inalcanzable desde el servidor. No sólo eso, sino una regla de firewall tendría que ser añadido y un puerto hacia adelante permitiendo que el tráfico en este puerto.

Cuando el proxy FTP está en uso, se trata de hacer tres cosas importantes. En primer lugar, se reescribirá el PORT de FTP
comandos para que la dirección IP es la dirección IP WAN del firewall, y un puerto elegido al azar
en esa dirección IP. A continuación, se añade un puerto delantero que conecta a la dirección IP traducida y puerto a la dirección IP original y el puerto especificados por el cliente FTP. Por último, se permite el tráfico desde el servidor FTP para conectarse a ese puerto "público".

Cuando todo está funcionando como debería, todo esto sucede de manera transparente. El servidor nunca sabe que es 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 es generalmente un problema ya que el servidor sólo estará escuchando las conexiones en los puertos estándar de FTP y luego hacer las conexiones de salida de nuevo a los clientes.

Modo pasivo

Modo pasivo (PASV) actúa un poco a la inversa. Para los clientes, es más de NAT y firewalls
porque el servidor escucha en un puerto cuando se solicita una transferencia de archivos, no el cliente. Típicamente, PASV
Modo de trabajo para los clientes FTP detrás de NAT sin usar ningún proxy o manejo especial en absoluto.

Si un servidor está detrás de NAT, sin embargo, el tráfico debe ser aproxima a la inversa cuando los clientes intentan utilizar el modo PASV. El proxy FTP puede manejar esta situación, pero todas las peticiones FTP entrante
parecen provenir del sistema de pfSense en lugar de los clientes. Similar a la situación en la anterior
sección, cuando un modo de solicitudes de cliente PASV al servidor tendrá que dar su dirección IP y un aleatorio puerto al que el cliente puede intentar conectarse. Puesto que el servidor se encuentra en una red privada, que la dirección IP
y tendrá que ser traducido y permitido a través del firewall de puerto.

Modo pasivo extendido

Modo pasivo extendido (EPSV) funciona de forma similar al modo PASV pero hace concesiones para el uso de IPv6. Cuando un cliente solicita una transferencia, el servidor responderá con el puerto al que el cliente debe conectarse. Las mismas advertencias para los servidores en modo PASV se aplican aquí.

Servidores FTP y el puerto Delanteros

Para asegurar el proxy FTP funciona correctamente para los delanteros del
puerto
- IP pública debe ser IP de la interfaz WAN o un tipo CARPA VIP porque el proxy FTP debe ser capaz de para que escuche en la dirección IP pública, y Proxy ARP y otras personalidades de tipo no permiten esto.

- FTP ayudante debe estar habilitado en la interfaz WAN en el que el puerto reside adelante.

- El servidor debe estar usando el puerto 21.

Servidores FTP y NAT 01:01

Al alojar un servidor FTP con NAT 01:01, debe hacer tres cosas para asegurarse de que el proxy FTP función, permitiendo FTP para que funcione correctamente.

• Utilice el tipo de VIPs CARP

Debido a que el proxy FTP debe ser capaz de escuchar en el VIP y Proxy ARP y otros VIPs Tipo hacer No permita que este, debe utilizar VIPs CARP con ningún 01:01 entradas NAT de hosting de servidores FTP.

• Habilitar el ayudante FTP en la WAN a la que se configura la entrada 01:01

Vaya a la interfaz donde reside el 01:01 subred externa, en el menú Interfaces. En un solo Despliegue de WAN, este es Interfaces WAN. Bajo Auxiliar de FTP, asegúrese de desactivar el FTP userland aplicación proxy está desactivada.

• Agregue una entrada hacia adelante puerto TCP 21

Esto no es exactamente en línea recta, pero la forma en que se activa el asistente para FTP para escuchar en un NAT 01:01 IP es mediante la adición de una entrada hacia delante del puerto con las mismas IPs internas y externas y puerto TCP 21. Este en realidad no añade la configuración de NAT se especifica, ya que el sistema reconoce el NAT 01:01 entrada, y simplemente lanza el proxy FTP en esa IP. Esto puede llegar a ser más recta hacia adelante en pfSense 2.0, pero el comportamiento existente se conserva por compatibilidad hacia atrás.

TFTP

Estándar tráfico TCP y UDP iniciar conexiones a hosts remotos utilizando un puerto de origen aleatorio en el intervalo de puertos efímeros (rango varía según el sistema operativo, pero cae dentro 1024-65535), y el puerto de destino del protocolo en uso. Respuestas desde el servidor al cliente que invierten - el puerto de origen es puerto de destino del cliente, y el puerto de destino es el puerto de origen del cliente. Así es como los asociados pf el tráfico de respuesta con las conexiones iniciadas desde la red.

TFTP (Trivial File Transfer Protocol) no se sigue de esto, sin embargo. La definición de TFTP estándar, RFC 1350, especifica la respuesta del servidor TFTP al cliente se obtiene de un puerto pseudoaleatoria número. Su cliente TFTP puede elegir un puerto de origen de 10 325 (como ejemplo) y utilizar el destino puerto para TFTP, puerto 69. El servidor para otros protocolos entonces enviaría la respuesta a través de puerto de origen 69 y 10325 puerto de destino. Desde TFTP en su lugar utiliza un puerto de origen pseudo-aleatorio, el tráfico de respuesta no coincidirá con el estado pf ha creado para este tráfico. De ahí que las respuestas serán bloqueados porque parece ser el tráfico no solicitado de Internet.

TFTP no es un protocolo que se utiliza a través de Internet. La única situación que viene de vez en cuando hasta donde esto es un problema es con algunos teléfonos IP que se conectan a los proveedores de VoIP externos en Internet usando TFTP para tirar de configuración y otra información. La mayoría de los proveedores de VoIP no lo requieren.

PPTP / GRE

Las limitaciones con PPTP en pfSense se deben a las limitaciones en la capacidad de pf de NAT el protocolo GRE. Por lo tanto, las limitaciones se aplican a cualquier uso del protocolo GRE, sin embargo PPTP es el más común utilizar de GRE en la mayoría de las redes de hoy en día.

El código de seguimiento de estado en pf para el protocolo GRE sólo se puede realizar un seguimiento de una única sesión por IP pública por un servidor externo. Esto significa que si usted utiliza conexiones PPTP VPN, sólo una máquina interna puede conectar simultáneamente a un servidor PPTP en Internet. Un millar de máquinas se pueden conectar simultáneamente a un millar de diferentes servidores PPTP, pero sólo uno a la vez en un solo servidor. Un solo cliente puede también conectarse a un número ilimitado de servidores PPTP externos.

El único trabajo disponible alrededor es utilizar varias direcciones IP públicas en el servidor de seguridad, uno por cada cliente a través de Outbound o NAT 1:1, o utilizar varias direcciones IP públicas en el servidor PPTP externo. Esto no es un problema con otros tipos de conexiones VPN.

Debido a las mismas limitaciones GRE se mencionó anteriormente, si se habilita el servidor PPTP en pfSense, que no se puede conectar a cualquier servidor PPTP en Internet de los clientes NAT a la IP WAN en pfSense. La para evitar esto también requiere el uso de más de una dirección IP pública. Puede NAT interno clientes a otra IP pública, y sólo estarán sujetos a las mismas restricciones de IP-per pública antes mencionados.

Ya que gran parte dependemos de la funcionalidad del sistema subyacente, y simplemente envolvemos un GUI alrededor esa funcionalidad, se trata de un problema difícil para nosotros resolvemos. Se investigaron las posibles soluciones para esta en pfSense 2.0, y tuvo temporalmente un arreglo en el lugar, pero mientras trabajaba para la mayoría es causado gran estabilidad problemas en otras circunstancias y la falta de tiempo estaba disponible para resolver lo que se revirtió. Nosotros Esperamos tener ese retorno funcionalidad en el futuro.

Juegos Online

Juegos normalmente son NAT amigable, aparte de un par de advertencias. Esta sección se refiere a los juegos de PC con capacidades en línea, así como sistemas de juegos de consola con capacidades en línea. Esta sección proporciona una visión general de las experiencias de numerosos usuarios pfSense. Recomiendo visitar el tablero de juego en el foro pfSense [http://forum.pfsense.org] para obtener más información.

Puerto estático

Algunos juegos no funcionan correctamente a menos que habilite puerto estático. Si usted está teniendo problemas con un juego, lo mejor que puede probar primero está permitiendo puerto estático. Vea la sección de puertos estáticos anteriormente en este capítulo para más información.

Múltiples jugadores o dispositivos detrás de un dispositivo NAT

Algunos juegos tienen temas en los que varios jugadores o dispositivos están detrás de un único dispositivo NAT. Estos cuestiones parecen ser específicos de NAT, no pfSense, ya que los usuarios que lo han intentado otras experiencias firewalls los mismos problemas con ellos también. Buscar en el tablero de juego en el foro pfSense para el juego o el sistema que está utilizando y es probable encontrar información de otras personas con experiencias similares en el pasado.

Superar los problemas de NAT con UPnP

Muchos sistemas de juego modernos soportan Universal Plug-and-Play (UPnP) para configurar automáticamente cualquier necesidades especiales en términos de forwards de puertos NAT y reglas de firewall. Usted puede encontrar que habilitar UPnP en su sistema pfSense se permitirá fácilmente juegos para trabajar con poca o ninguna intervención. Consulte la sección llamado "UPnP" para obtener más información sobre la configuración y el uso de UPnP.

Solución de problemas

NAT puede ser un animal complejo, y en todos menos en los ambientes más básicas, no es probable que haya algún problemas para conseguir una buena configuración de trabajo. Esta sección repasará algunos problemas comunes y algunas sugerencias sobre cómo podrían resolverse.

Port Forward Solución de problemas

Delante del puerto, en particular, puede ser complicado, 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 han sido resuelto por una o más de las siguientes sugerencias.

Entrada hacia delante Puerto incorrectas

Antes de cualquier otra tarea de resolución de problemas, asegúrese que las configuraciones para el futuro puerto son correctos. Ir sobre el proceso en la sección llamada "Adición de puertos Forwards" de nuevo y vuelve a comprobar que los valores son correctas. Recuerde, si usted cambia el IP NAT o los puertos, también se tendrá que ajustar el juego regla de firewall. Las cosas más comunes para verificar si hay:

• Interfaz correcta (por lo general debe ser 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.

• Rango de puerto correcto, que debe corresponder al servicio que está tratando de transmitir.

Regla de firewall que falta o incorrecta

Después de comprobar la configuración de reenvío de puerto, verifique que la regla de firewall tiene la configuración adecuada. Un
regla de firewall correctos también sería evidente al ver los logs del firewall (la sección llamada "Visualización
los registros de servidor de seguridad "). Recuerde, que el destino de la regla de firewall debe ser la interno IP
dirección del sistema de destino y no a la dirección de la interfaz que contiene el puerto hacia adelante. Consulte la
sección llamada "Reglas para NAT" para más detalles.

Firewall está habilitado en el equipo de destino

Otra cosa a considerar es que pfSense puede reenviando el puerto correctamente, pero un servidor de seguridad en el equipo de destino puede estar bloqueando el tráfico. Si hay un servidor de seguridad en el sistema de destino, tendrá que revisar sus registros y configuraciones para confirmar si el tráfico está bloqueado en ese punto.

pfSense no es la puerta de el sistema de destino

Para que pfSense que transmita correctamente un puerto para un sistema local, pfSense debe ser la puerta de enlace predeterminada
para el sistema de destino. Si pfSense no es la puerta de entrada, el sistema de destino intentará enviar respuestas a
puerto hacia adelante fuera del tráfico independientemente del sistema es la puerta de entrada, y luego una de las dos
cosas va a suceder: Se
será dado de baja en ese punto, ya no habría estado de conexión correspondiente ese router - o -
habría NAT aplicada por ese router y luego ser abandonado por el sistema que origina la solicitud
ya que la respuesta es de una dirección IP diferente de aquella a la que la solicitud fue enviada inicialmente.

La máquina de destino no está escuchando en el puerto reenviado

Si, cuando la conexión se prueba, se rechaza la solicitud en lugar de tiempo de espera, en todo pfSense probabilidad
es el reenvío de la conexión correcta y la conexión es rechazada por el sistema de destino. Esta lata
suceder cuando el sistema de destino no tiene servicio de escucha en el puerto en cuestión, o si el puerto es
transmitido 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 está escuchando las conexiones SSH, pero el puerto hacia adelante fue introducida por el puerto 23 en lugar de 22, la solicitud lo más probable sería rechazado. Normalmente se puede saber la diferencia al tratar de conectar con el puerto en cuestión utilizando telnet. Un mensaje como Conexión
negado indica algo, con frecuencia el anfitrión en el interior, se niega activamente la conexión.

ISP está bloqueando el puerto que está tratando de transmitir

En algunos casos, los ISP filtrar el tráfico entrante a los puertos conocidos. Compruebe de su ISP Condiciones Servicio (ToS), y ver si hay una cláusula sobre la ejecución de los servidores. Tales restricciones son más comunes en las conexiones residenciales que las conexiones comerciales. En caso de duda, una llamada al ISP puede borrar el asunto.

Si los puertos están siendo filtrados por el ISP, es posible que tenga que mover sus servicios a un puerto diferente para para evitar la filtración. Por ejemplo, si su ISP no permite los servidores en el puerto 80, intente 8080 o 8888.

Antes de intentar solucionar un filtro, consulte ToS de su ISP para asegurarse de que no está violando su normas.

Probando desde la red en lugar de fuera

Por defecto, puerto remite sólo funcionarán cuando las conexiones se realizan desde fuera de su red.
Esto es un error muy común cuando realice pruebas puerto remite.

Si usted requiere puerto remite a trabajar internamente, consulte la sección titulada "Reflexión NAT". Sin embargo, Dividir el DNS (la sección llamada "Split" DNS) es una solución más adecuada y elegante a este problema sin necesidad de recurrir a NAT reflexión o el puerto hacia delante, y que valdría la pena su tiempo para aplicar en su lugar.

Dirección IP virtual o es incorrecto

Al utilizar las direcciones IP que no son las direcciones IP reales asignados a una interfaz, debe utilizar IPs virtuales (VIP, ver la sección llamada "IP virtual"). Si un puerto de reenvío a una dirección IP alternativa es no funciona, puede que tenga que cambiar a un tipo diferente de VIP. Por ejemplo, es posible que tenga que utilizar un Tipo de proxy ARP en lugar de un tipo de "Otros" VIP.

Cuando se prueba, asegúrese también de que se está conectando a la VIP adecuado.

pfSense no es el router de borde / borde

En algunos escenarios, pfSense es un enrutador interno, y hay otros routers entre éste y el Internet También la realización de NAT. En tal caso, sería necesario un delantero de puerto que se ingresó en el router de borde reenvío de puerto para pfSense, que luego utilizar otro puerto hacia delante para conseguir que el sistema local.

La prueba adicional necesaria

Si ninguna de estas soluciones ha ayudado a obtener un puerto de trabajo hacia adelante, consulte el Capítulo 29, Paquete Captura para obtener información sobre el uso de paquetes de captura para diagnosticar problemas de reenvío de puertos.

NAT Solución de problemas Reflexión

Reflexión NAT (la sección llamada "Reflexión NAT") es más de una chapuza que una solución, y como tal, es propenso a no funcionar como se espera. No podemos recomendar lo suficiente que use DNS en lugar de Split (Ver la sección llamada "Split DNS"). Si Reflexión NAT no funciona correctamente, asegúrese de que se trataba habilitado el camino correcto, y asegúrese de que no está reenviando un gran rango de puertos.

Reglas Reflexión NAT también se duplican para cada interfaz presente en el sistema, por lo que si usted tiene un montón de delanteros portuarias e interfaces, el número de reflectores puede fácilmente superar los límites del sistema. Si esto sucede, una entrada se imprime en los registros del sistema.

Acceso Web se rompe con la reflexión NAT Activado

Si usted tiene una forma incorrecta especificada NAT Port Forward, puede causar problemas cuando NAT Reflexión está habilitado. La forma más común surge este problema es cuando se tiene un servidor web local, y el puerto 80 se remite allí con una dirección externa incorrectamente especificado.

Si Reflexión NAT está habilitada y la dirección externa está establecida en cualquier, cualquier conexión que hagas viene como su propio sitio web. Para solucionar este problema, edite el NAT Port Forward para el puerto de ofender, y el cambio
Dirección externa a Interfaz Dirección en su lugar.

Si realmente necesita una dirección externa de cualquier, entonces Reflexión NAT no funciona para usted, y usted que emplear Split DNS en su lugar.

Outbound NAT Solución de problemas

Cuando usted tiene el manual de salida habilitado NAT, y hay varias subredes locales, un saliente Será necesaria la entrada NAT para cada uno. Esto se aplica sobre todo si es su intención que la salida de tráfico 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 que falta sería ver los paquetes salen de la interfaz WAN con una dirección de origen de una red privada. Consulte el Capítulo 29, Captura de paquetes para más detalles sobre obtener e interpretar capturas de paquetes.

Capítulo 12. Enrutamiento

Una de las principales funciones de un servidor de seguridad es el enrutamiento de tráfico, además de la filtración y la realización de
NAT. Este capítulo trata varios temas relacionados con el enrutamiento, incluyendo pasarelas, las rutas estáticas de enrutamiento
protocolos de enrutamiento de direcciones IP públicas, y mostrar la información de enrutamiento.

Gateways

La clave para el enrutamiento es gateways y sistemas a través del cual otras redes pueden ser alcanzados. El tipo de gateway mayoría de la gente está familiarizada con una puerta de enlace predeterminada, que es el router a través de la cual
un sistema se conectará a Internet oa cualquier otra red no tiene una ruta más específica para
alcanzar. Gateways también se utilizan para el enrutamiento estático, donde otras redes deben llegar a través de locales específicos
routers. En la mayoría de las redes normales, puertas de enlace siempre residen en la misma subred que una de las interfaces
en un sistema. Por ejemplo, si tiene una dirección IP de 192.168.22.5 en un servidor de seguridad, a continuación, una puerta de enlace
a otra red tendría que ser en algún lugar dentro de 192.168.22.x Si la otra red es
accesible a través de esa interfaz. Una notable excepción a esto es las interfaces basadas en la PPA, que a menudo
tener direcciones IP de puerta de enlace en otra subred, y aún no se utilizan de la misma manera.

Familias Gateway Address (IPv4 e IPv6)

Cuando se trabaja con rutas y puertas de enlace, la funcionalidad y los procedimientos son los mismos para ambos
Las direcciones IPv4 e IPv6, sin embargo todas las direcciones para una ruta dada deben incluir direcciones de
la misma familia. Por ejemplo, para dirigir una red IPv6, debe hacerlo a través de una puerta de enlace IPv6 / router.
No se puede crear una ruta para una red IPv6 con una dirección de puerta de enlace IPv4. Cuando se trabaja con
grupos de puerta de enlace, se aplica la misma restricción; Todas las puertas de enlace en un grupo de puerta de enlace deben ser de la misma
familia de direcciones.

Gestión de Gateways

Si es necesario agregar una puerta de enlace predeterminada, una puerta de entrada adicional para una ruta estática, u otra puerta de entrada de multi-WAN, hay que añadir las pasarelas antes de que puedan ser utilizados. Si va a agregar una puerta de acceso para una interfaz de tipo WAN, puede hacerlo desde la interfaz (Vea la sección llamada "Interface Conceptos básicos de configuración "), o añadir la puerta de acceso y luego seleccione de la lista desplegable de la configuración de la interfaz.

Tipos de interfaces dinámicos como DHCP y PPPoE reciben una pasarela automática que se observa como
Dinámico en la lista de puerta de enlace. Los parámetros para este tipo de puertas de enlace se puede ajustar la misma que la
parámetros para una puerta de enlace estática, sino una puerta de enlace dinámico no se pueden eliminar.

Para añadir o director pasarelas, navegue a System Enrutamiento, en la ficha Puertas de enlace. Para agregar un nuevo puerta de entrada, haga clic en el botón en la parte superior o inferior de la lista. Para editar una puerta de entrada existente, haga clic en el botón al final de su fila. Para eliminar una entrada, haga clic en el botón al final de su fila.

Gateway Settings

Al agregar o editar una puerta de entrada, se le presentará una pantalla que muestra todas las opciones
para controlar el comportamiento de una puerta de enlace. Los únicos ajustes necesarios son la interfaz, el nombre y el Gateway (dirección IP).

Interfaz

Esta es la interfaz que la pasarela se llega a través de. Por ejemplo, si se trata de una puerta de enlace local en la subred LAN, usted elegiría la interfaz LAN aquí.

Nombre

El nombre de la puerta de entrada, como se indica en la lista de puerta de enlace, y varios desplegable y otros selectores para puertas de enlace. Sólo puede contener caracteres alfanuméricos, o un guión bajo, pero no espacios. Así que usted podría tener WANGW, GW_WAN, o WanGate, pero no WAN GW.

Entrada

Esta es la dirección IP de la puerta de enlace. Como se mencionó anteriormente, esto debe residir en la misma subred como la interfaz elegido.

Puerta de enlace predeterminada

Esta casilla de verificación controla si esta pasarela se trata como la puerta de enlace predeterminada para el sistema. La puerta de enlace predeterminada es el gateway de último recurso. Se utiliza cuando no hay otras rutas más específicas. Es posible que tenga una puerta de enlace predeterminada IPv4 y IPv6 una puerta de enlace predeterminada.

Desactivar Monitoreo de puerta de enlace

Por defecto, el sistema hará ping cada puerta de enlace una vez por segundo para controlar el estado de la puerta de entrada en términos
de latencia y pérdida de paquetes. Estos datos son utilizados para la información de estado de puerta de enlace y también para dibujar el
Gráfico de RRD Calidad. Si usted encuentra esta vigilancia no deseada por cualquier razón, puede ser desactivado comprobar Monitoreo Disable Gateway. Tenga en cuenta que si no se controla el estado de la puerta de enlace, y luego de múltiples
WAN no funcionará correctamente ya que no puede detectar este tipo de fallas.

IP Monitor

La opción IP Monitor le permite elegir la dirección IP para hacer ping para monitorear el estado de la puerta de enlace. Por defecto el sistema ping a la dirección IP de puerta de enlace para el seguimiento de la situación. Esto no es siempre deseable, especialmente en el caso de que la puerta de enlace IP es local para usted, como en un módem de cable o CPE DSL. En casos como el que tiene más sentido hacer ping a algo más lejos río arriba, como un
Servidor DNS del ISP o de un servidor en Internet. Otro caso es cuando un ISP es propenso a tener aguas arriba fracasos, así ping hacia una máquina en Internet es una prueba más precisa de la capacidad de uso de la WAN en lugar de probando el propio enlace. Algunas opciones populares incluyen servidores de OpenDNS, servidores DNS público de Google,
o en los sitios web más populares, como Google o Yahoo. Si la dirección IP especificada en este cuadro no es directamente
conectado, se agrega una ruta estática para asegurarse de que el tráfico a la IP Monitor se apaga la puerta de entrada se espera.
el servidor de seguridad mediante la comprobación de estado Gateways o mediante el uso de las puertas de enlace del widget en el tablero de instrumentos. Si
Cada puerta de enlace debe tener un monitor de IP única. Usted puede verificar si una puerta se percibe como en línea mediante
muestra en línea, entonces la IP del monitor regresa con éxito pings.

Avanzado

Hay varios parámetros que se pueden cambiar los que afectan a cómo se controla o se trata de una pasarela
en un escenario multi-WAN. La mayoría de los usuarios no tendrán que cambiar estos valores. Para acceder a la avanzada
opciones, haga clic en el botón Opciones avanzadas. Si alguna de las opciones avanzadas se establecen, esta sección es automáticamente
expandido. Para obtener más información sobre el uso de múltiples conexiones WAN, consulte el Capítulo 15, Múltiple WAN
Conexiones.

Peso

Cuando se utiliza multi-WAN, si dos redes WAN tienen diferentes cantidades de ancho de banda, el parámetro de Peso se puede utilizar para ajustar la forma en que se utilizan. Por ejemplo si usted tiene 5Mbit / s WAN y 10 Mbit / s WAN2, usted puede ponderar WAN como 1 y WAN2 como 2. Luego de cada tres conexiones que salen, lo hará
utilizar WAN y dos usará WAN2. Esto distribuir con mayor precisión el ancho de banda en este tipo
de configuración.

Umbrales de latencia

Los umbrales Latencia campos de control de la cantidad de latencia que se considera normal para esta pasarela. Este valor se expresa en milisegundos (ms). El valor en el campo es el límite inferior en que la puerta de entrada se considera en estado de alerta, pero no hacia abajo. Si la latencia excede el valor en el campo, se considera baja y retirarse del servicio. Los valores adecuados en estos los campos pueden variar dependiendo de qué tipo de conexión está en uso, y qué ISP o el equipo está entre el firewall y la IP del monitor. Los valores por defecto son de 300 y A 500.

Algunas otras situaciones comunes pueden requerir el ajuste de estos valores. Por ejemplo, algunas líneas DSL están bien incluso en una mayor latencia, lo que aumenta el parámetro TO 700 o más podría reducir el número de veces que el gateway se consideraría abajo cuando en realidad estaba trabajando bien. Otro ejemplo es un túnel GIF a un lugar como he.net para IPv6. Debido a la naturaleza de túneles GIF y carga en el túnel servidores, el túnel podría estar trabajando aceptablemente incluso con una latencia de hasta 900ms.

Los umbrales de pérdida de paquetes

Al igual que en los umbrales Latencia anteriores, los umbrales de pérdida de paquetes de control de la cantidad de pérdida de paquetes que el sistema puede ver a un IP monitor antes sería considerado inutilizable. Este valor se expresa como un porcentaje, siendo 0 la ausencia de pérdidas y 100 siendo la pérdida total. El valor en el campo es la más baja límite en el que la puerta de entrada se considera en estado de alerta, pero no hacia abajo. Si la cantidad de pérdida de paquetes excede el valor en el campo, se considera baja y retirarse del servicio. La valores propios de estos campos puede variar dependiendo de qué tipo de conexión está en uso, y qué ISP o el equipo se encuentra entre el firewall y el IP del monitor. Los valores por defecto son de 10 y A 20.

Al igual que con la latencia, las conexiones pueden ser propensos a diferentes cantidades de pérdida de paquetes y todavía funcionar en una manera útil, especialmente si la ruta de acceso a una IP Monitor gotas o retrasa ICMP a favor de otro tipo de tráfico. Hemos visto las conexiones sean inutilizables con pequeñas cantidades de pérdida, y algunos que son utilizables incluso cuando se muestra la pérdida del 45%. Si usted encuentra que usted está viendo alarmas de pérdida en una WAN funcione normalmente puerta de enlace, introduzca los valores más altos en el campos De y hasta que logre un buen equilibrio para ese circuito.

Frecuencia de la sonda

El valor en el campo de la sonda de frecuencia controla la frecuencia con la que se envía un ping al IP del monitor. El valor por defecto es hacer ping a cada segundo. En algunas situaciones, tales como enlaces que necesitan supervisado, pero que tienen datos de alta cargos, incluso una pequeña mesa de ping cada segundo puede sumar. Este valor puede ser aumentado de manera segura con tal de que la frecuencia se incrementa la exactitud de la gráfica de calidad se reduce.

Tenga en cuenta que la gráfica de calidad está promediado en segundos, no los intervalos, de manera que la sonda de frecuencia es menor que el valor en el campo de Down.

Abajo

El campo de Down especifica cuántos intervalos deben ser anormales antes de que se considera baja y fuera de servicio. Por defecto, este es 10 segundos. Algunos ajustes puede ser necesario para evitar falsas positivos (o falsos negativos), pero en términos generales el valor por defecto es suficiente.

El tiempo total antes de una puerta de enlace está abajo es el producto de la Frecuencia de la sonda y los campos de abajo. Por De forma predeterminada es 1 * 10 = 10 segundos. Si el aumento de la Frecuencia de la sonda a 7, entonces sería 7 * 10 = 70 segundos.

Descripción

Descripción de campo de la puerta de enlace es para su referencia. Una breve nota sobre la puerta de entrada o la interfaz es utilizado para puede ser útil, o se puede dejar en blanco si lo desea.

Portal de Grupos

Portal de Grupos de definir conjuntos de puertas de enlace que se utilizarán para la conmutación por error o el balanceo de carga. Para obtener información sobre el establecimiento de estas características, consulte el Capítulo 15, Múltiples conexiones WAN.

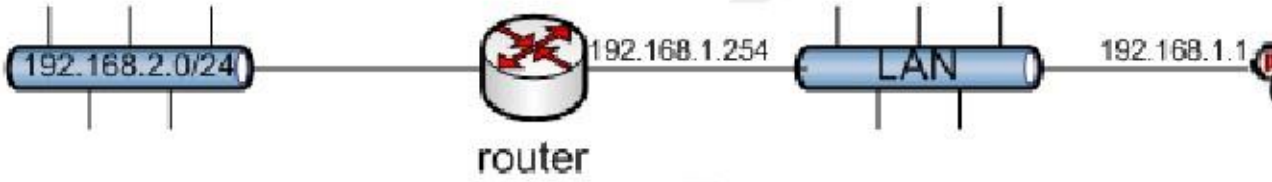
Rutas estáticas

Las rutas estáticas se utilizan cuando tiene hosts o redes accesibles a través de un router que no sea el predeterminado puerta de enlace. El servidor de seguridad o enrutador sabe acerca de las redes directamente conectadas a la misma, y alcanza todos los demás
redes según las indicaciones de su tabla de enrutamiento. En las redes donde usted tiene un router de conexión interna subredes internas adicionales, debe definir una ruta estática para esa red para ser alcanzable. Los routers
a través del cual se llega a estas otras redes primero hay que añadir como puertas de acceso. Vea la sección llamada "Gateways" para obtener información sobre la adición de gateways.

Ejemplo de ruta estática

Figura 12.1, "ruta estática" ilustra un escenario en el que se requiere una ruta estática.

Figura 12.1. Ruta estática



Debido a que la red 192.168.2.0/24 en la Figura 12.1, "ruta estática" no está en una conexión directa
interfaz de pfSense, necesita una ruta estática por lo que sabe como llegar a dicha red. Figura 12.2, "estático configuración de la ruta "muestra la ruta estática apropiada para el diagrama de arriba. Como se mencionó anteriormente, antes se puede agregar una ruta estática a la puerta de enlace debe estar definida.

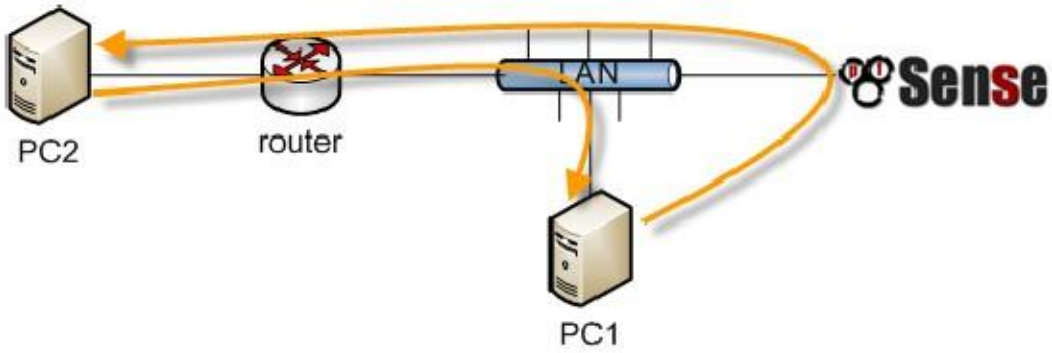
Figura 12.2. Configuración de rutas estáticas

La Red de destino especifica la subred accesible a través de esta ruta. Puerta de enlace selecciona el un router
a través del cual esta red es alcanzable. También pueden ser necesarios ajustes de reglas de firewall. El valor por defecto Regla LAN sólo permite el tráfico proviene de la subred LAN, por lo que si usted mantuvo esa regla, se le
que abrir la red de origen para incluir también las redes alcanzables a través de rutas estáticas en LAN.
La siguiente sección describe un escenario común con rutas estáticas que también se debe revisar.

Bypass de reglas de firewall para el tráfico sobre la misma interfaz

En muchas situaciones en las que el uso de rutas estáticas se termina con enrutamiento asimétrico. Esto significa que el tráfico
en una dirección se llevará a un camino diferente del tráfico en la dirección opuesta. Tome la Figura 12.3, "Encaminamiento asimétrico" por ejemplo.

Figura 12.3. Enrutamiento asimétrico



Tráfico de PC1 a PC2 pasará por pfSense, ya que es la puerta de enlace predeterminada del PC1, pero el tráfico en sentido contrario irá directamente desde el router al PC1. Desde pfSense es un firewall stateful, debe ver todas las de la conexión para poder filtrar el tráfico correctamente. Con el enrutamiento asimétrico como esto, cualquier firewall stateful acabará dejando caer el tráfico legítimo porque no puede mantener adecuadamente el estado sin ver el tráfico en ambas direcciones. Compruebe siempre las reglas de firewall de derivación para el tráfico en la misma caja de interfaz en el sistema Página Avanzadas en la pestaña Firewall / NAT asimétrica en escenarios de enrutamiento para prevenir el tráfico legítimo se caiga. Esto agrega reglas de firewall que permiten todo el tráfico entre redes definidas en las rutas estáticas que no utilizan la opción del estado de PF. Alternativamente, usted puede agregar reglas de firewall a ti mismo que especifican ninguno como el tipo de Estado, haciendo coincidir el tráfico entre el local y subredes remotas, sino que por lo general no se recomienda debido a la complejidad que pueden introducir y la aumento de la probabilidad de errores. Si necesita filtrar el tráfico entre subredes enrutadas estáticamente, se se debe hacer en el router y no el firewall ya que el firewall no está en una posición en la red donde se puede controlar de manera efectiva que el tráfico.

ICMP Redirecciones

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 reenviar el paquete como se ha configurado. La redirección de ICMP hace que una ruta para ese destino para ser añadido a la tabla de enrutamiento del dispositivo de envío, y el dispositivo utilizará posteriormente que más ruta directa a llegar a esa red. Esto no funcionará si su sistema operativo está configurado para no permitir redirecciones ICMP, que normalmente no es el caso por defecto.
Redirecciones ICMP son comunes cuando se tiene una ruta estática que apunta a un enrutador en la misma interfaz como las PC del cliente y otros dispositivos de red. El diagrama de enrutamiento asimétrico de la sección anterior es un ejemplo de esto.

Redirecciones ICMP han mayormente inmerecidamente conseguido una mala reputación de algunos en la seguridad comunidad, ya que permiten la modificación de la tabla de enrutamiento de un sistema. Sin embargo no son el riesgo que algunos implican, como para ser aceptado, el mensaje de redirección ICMP debe incluir los primeros 8 bytes del datos del datagrama original. Un huésped en condiciones de ver que los datos y por lo tanto ser capaces de forjar con éxito ICMP ilícito redirige está en una posición para conseguir el mismo resultado final en múltiples otras maneras.

Enrutamiento IP Pública

Esta sección cubre el enrutamiento de direcciones IP públicas, donde se tiene una subred IP pública asignada a un interno interfaz y único firewall despliegues. Si está utilizando CARP, consulte la sección "Proporcionar Redundancia Sin NAT ".

Asignación de IP

Usted necesita por lo menos dos subredes IP públicas asignadas a usted por su ISP. Uno es para la WAN de su servidor de seguridad, y una para la interfaz en el interior. Esto es comúnmente una subred / 30 de la WAN, con un segundo

subred asignada para la interfaz interna. En este ejemplo se utilizará un / 30 sobre la WAN tal como se muestra en la Tabla 12.1,
"WAN IP bloqueadas" y una subred pública / 29 en una interfaz OPT interno como se muestra en la Tabla 12.2, "Inside IP Block ".

Tabla 12.1. WAN IP bloqueadas

11.50.75.64/30	
Dirección IP	Asignado a
11.50.75.65	Router del ISP (default gateway IP de pfSense)
11.50.75.66	interfaz IP WAN pfSense

Tabla 12.2. Dentro de direcciones IP bloqueadas

192.0.2.128/29	
Dirección IP	Asignado a
192.0.2.129	interfaz OPT pfSense
192.0.2.130	Los hosts internos
192.0.2.131	
192.0.2.132	
192.0.2.133	
192.0.2.134	

Configuración de la interfaz

En primer lugar, configure las interfaces WAN y OPT. La interfaz de LAN también se puede utilizar para las direcciones IP públicas si
que usted desea. En este ejemplo, LAN es una subred IP privada y OPT1 es la subred IP pública.

Configurar WAN

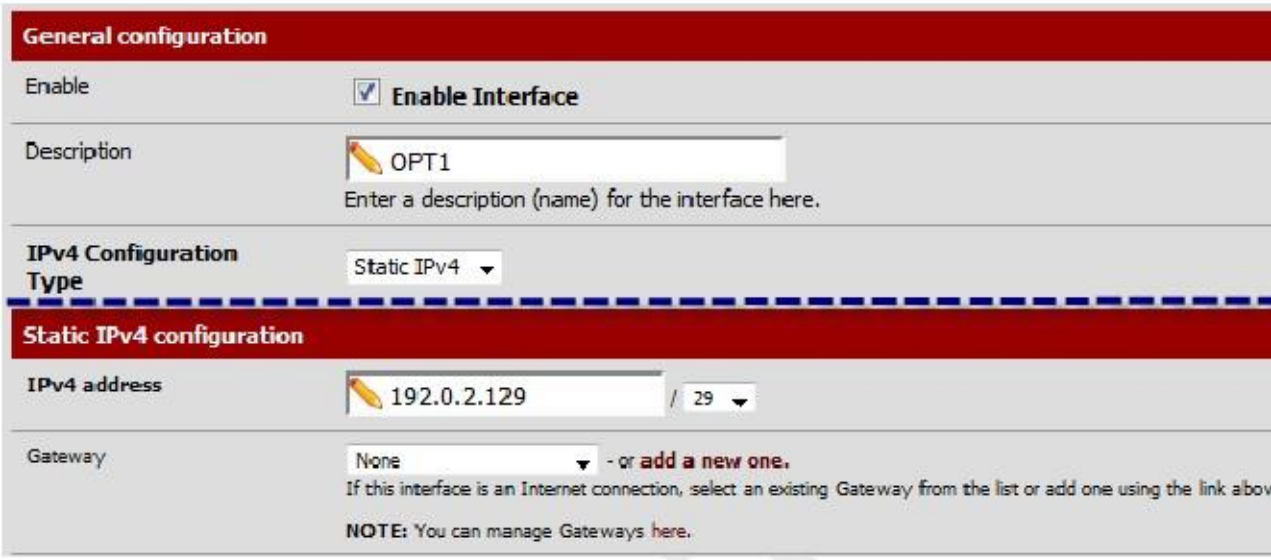
Agregue la dirección IP y el gateway en consecuencia. Figura 12.4, "WAN IP y la configuración de puerta de enlace" muestra la WAN configurada como se muestra en la Tabla 12.1, "WAN IP bloqueadas".

Figura 12.4. WAN IP y la configuración de puerta de enlace

Configure OPT1

Ahora permita OPT1, cambiar, opcionalmente, su nombre, y configurar la dirección IP y la máscara. La Figura 12.5, "Configuración OPT1 Routing" muestra OPT1 configurada como se muestra en la Tabla 12.2, "Dentro de direcciones IP bloqueadas".

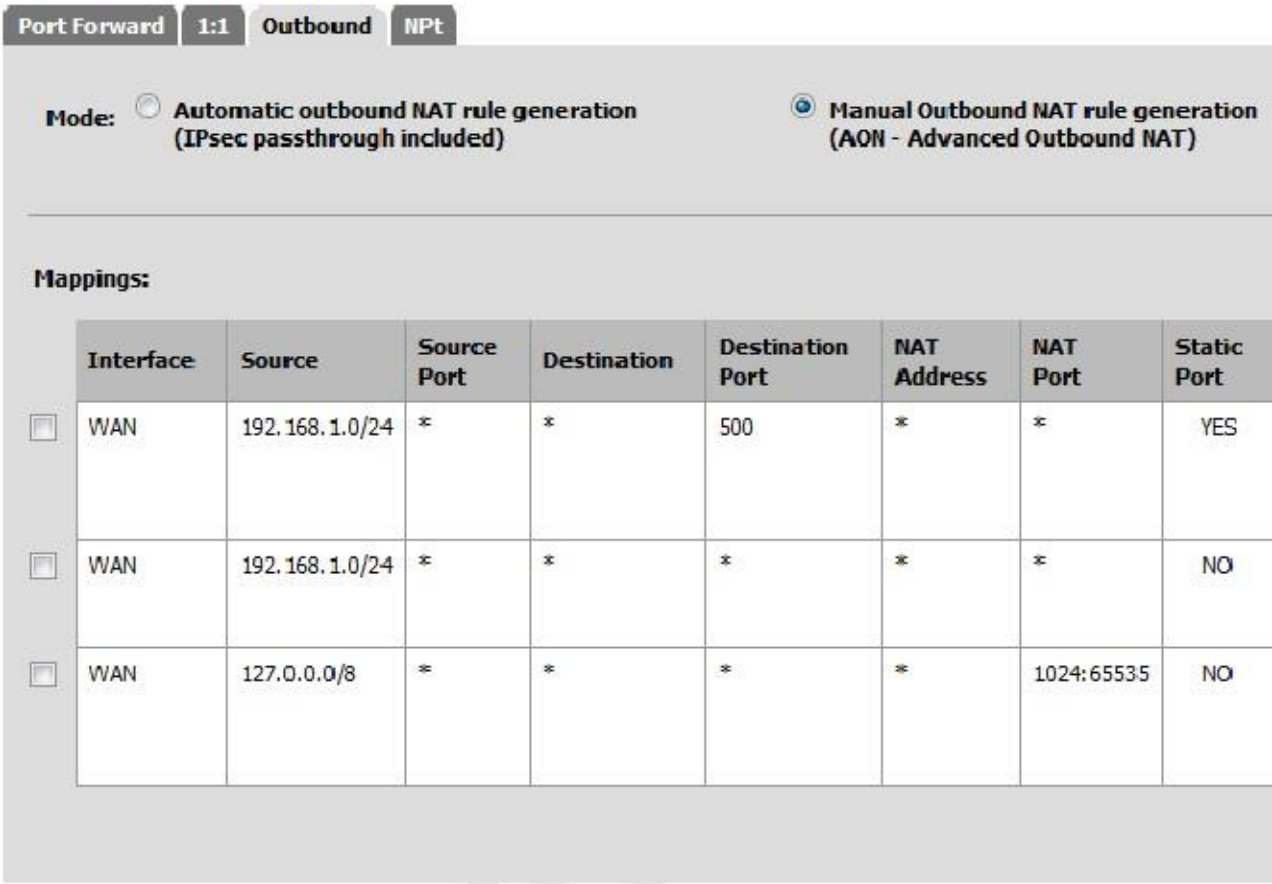
Figura 12.5. Configuración OPT1 Enrutamiento



Configuración de NAT

El valor por defecto de traducir el tráfico interno a la IP WAN debe ser anulado cuando se utilizan direcciones IP públicas en una interfaz interna. Vaya a Cortafuego NAT, y haga clic en la ficha de salida. Seleccione Manual Outbound generación regla NAT y haga clic en Guardar. Esto generará una regla por defecto traducir todo el tráfico de la subred LAN salir de la interfaz WAN a la IP WAN, el comportamiento predeterminado de pfSense. Si su LAN contiene una subred privada como en este ejemplo, se trata de la configuración exacta deseada. Tráfico procedente de la red de 192.0.2.128/29 OPT1 no se traduce porque la fuente se limita a 192.168.1.0/24. Esta configuración se muestra en la Figura 12.6, "configuración de NAT de salida". Si utilizar IPs públicas en su LAN, borrar esta entrada agregado automáticamente. Luego haga clic en Aplicar cambios.

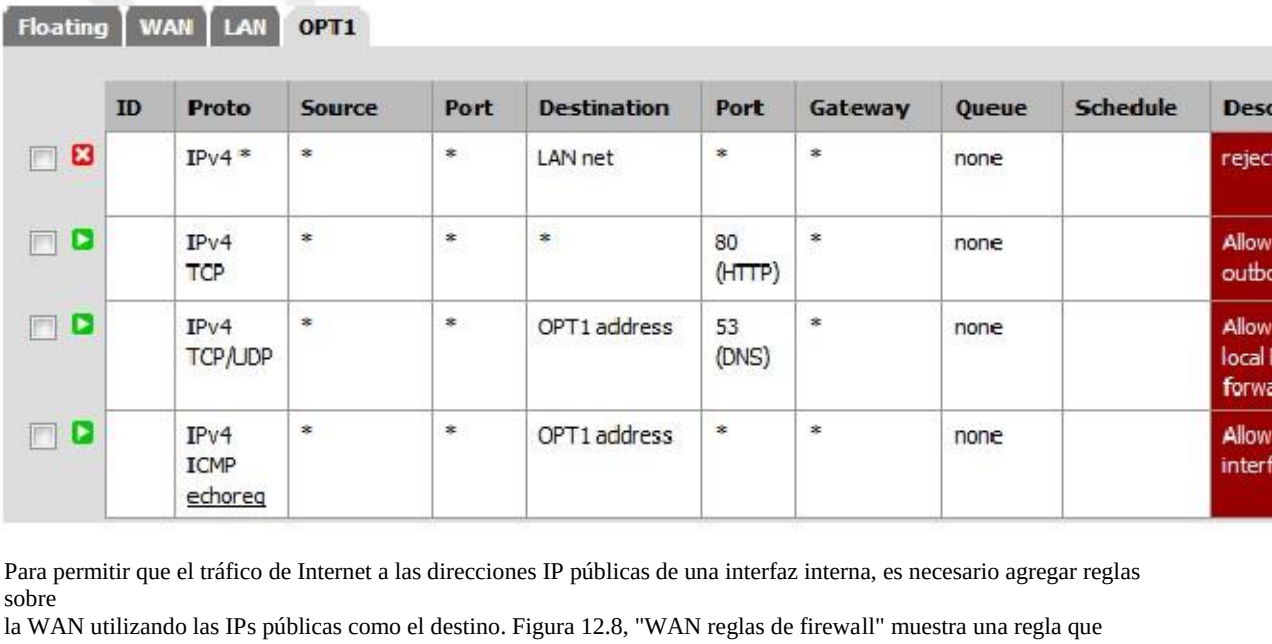
Figura 12.6. Configuración NAT de salida



Regla Configuración del cortafuegos

La configuración NAT e IP ya está completa. Tendrán que ser añadido para permitir reglas de firewall tráfico entrante y saliente. Figura 12.7, "las reglas del cortafuegos OPT1" muestra una configuración DMZ-como, donde se rechaza todo el tráfico destinado a la subred LAN, DNS y pings a la IP de la interfaz OPT1 son permitido, y HTTP está permitido saliente.

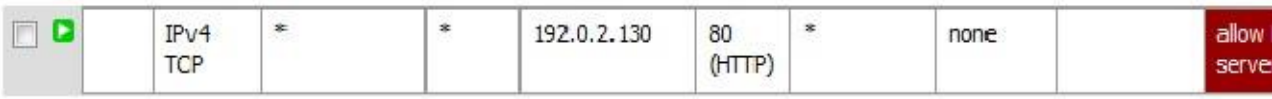
Figura 12.7. Reglas de firewall OPT1



Para permitir que el tráfico de Internet a las direcciones IP públicas de una interfaz interna, es necesario agregar reglas sobre
la WAN utilizando las IPs públicas como el destino. Figura 12.8, "WAN reglas de firewall" muestra una regla que

permite HTTP a 192.0.2.130, una de las IPs públicas en la interfaz interna, como se muestra en la Tabla 12.2, "Dentro de direcciones IP bloqueadas".

Figura 12.8. Reglas de firewall WAN



Después de configurar las reglas de firewall si lo desea, su configuración se ha completado.

Protocolos de enrutamiento

En el momento de escribir estas líneas, tres protocolos de enrutamiento son compatibles con pfSense, RIP (Routing Protocolo de información), BGP (Border Gateway Protocol) y OSPF (Open Shortest Path First). Este sección es la luz en los detalles, y supone la comprensión de los protocolos de enrutamiento, como requisito previo. Un en profundidad la discusión de los protocolos de enrutamiento está fuera del alcance de este libro.

RIP

RIP puede configurarse en Servicios RIP. Para utilizarlo:

1. Marque la casilla Habilitar RIP

2. Elija las interfaces RIP escucharán y enviar actualizaciones de enrutamiento en

3. Seleccione su versión de RIP

4. Cuando se usa RIPv2, introduzca una contraseña RIPv2 si se utiliza en la red.

5. Haga clic en Guardar

RIP se iniciará y comenzar a enviar y recibir las actualizaciones de enrutamiento en el especificado inmediatamente interfaces.

BGP

Un paquete BGP utilizando OpenBGPD de OpenBSD [http://www.openbgpd.org] está disponible. Para instalar ella, visita System Paquetes y haga clic en el signo más a la derecha de OpenBGPD. Haga clic en Aceptar para instalar el paquete. Usted encontrará OpenBGPD en el menú Servicios.

BGP es una bestia compleja, y describir en detalle está fuera del alcance de este libro. Configuración de OpenBGPD de pfSense es sencillo si se entiende BGP. Durante el desarrollo de este paquete, que se basó en BGP de O'Reilly reservar [http://www.amazon.com/gp/product/0596002548?ie = UTF8 & tag = pfSense-20 y linkCode = as2 y campo = 1,789 y = 9,325 y creativa creativeASIN = 0596002548] y se lo recomiendo a cualquiera que quiera implementar BGP.

OSPF

Un paquete OSPF utilizando el Quagga [http://www.nongnu.org/quagga/] daemon de encaminamiento es también disponible. Al igual que con BGP, para instalarlo visite System Paquetes y haga clic en el signo más a la derecha del Quagga OSPF. Haga clic en Aceptar para instalar el paquete. Usted encontrará Quagga ospfd en el menú Servicios.

OSPF es un protocolo de enrutamiento también bastante complejo, aunque no tan complejo para configurar como BGP puede ser. La detalles de cómo configurar ospfd son también fuera del alcance de este libro, aunque para alguien acostumbrado a OSPF las opciones de configuración se encuentran en la interfaz gráfica de usuario debe estar familiarizado. Las opciones para el Quagga Paquete OSPF son similares a los del antiguo paquete OpenOSPFD en versiones anteriores de pfSense,

sin embargo, hemos encontrado que la versión Quagga es mucho más comporta bien cuando se opera con otro equipo habilitado para OSPF.

Ruta de solución de problemas

Cuando el diagnóstico de problemas de flujo de tráfico, uno de los primero que debe verificar es de las rutas conocidas por pfSense.

Visualización de rutas

Hay dos maneras de ver las rutas: Via WebGUI, ya través de la línea de comandos.

Para ver las rutas en el WebGUI, visite Diagnóstico Rutas y podrás ver la salida de esa se muestra en la Figura 12.9, "Visualización de la Ruta".

Figura 12.9. Ruta Display

IPv4

Destination	Gateway	Flags	Refs	Use	Mtu	Netif
default	10.0.2.2	UGS	0	53	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
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

La salida de la línea de comandos es similar a la observada en el WebGUI:

#netstat-rn
Las tablas de enrutamiento

```
Internet:
Destino        Entrada             Banderas Refs      Uso  Netif de vencimiento
defecto        10.0.2.2            UGS         0       53    le0
10.0.2.0/24    enlace # 1          UC          0        0    le0
10.0.2.2       52:54:00:12:35:02   UHLW        2       35    le0
10.0.2.15      127.0.0.1           UGHS        0        0    le0796
127.0.0.1      127.0.0.1           UH          1        0    lo0
192.168.56.0/24 enlace # 2         UC          0        0    lo0
192.168.56.101 08:00:27:00: d4: 84 UHLW        1      590    LE1
                                                             le11197
```

Las columnas que se muestran en estas pantallas indican diversas propiedades de las rutas, y se explican a continuación.

Destino

El host de destino o de la red. La ruta por defecto para el sistema está simplemente aparece como "default".
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.

Entrada

Una puerta de enlace es el router por el cual los paquetes que van a una necesidad específica de destino para ser enviado. Si esta columna
muestra un vínculo, como el enlace # 1, luego de que la red es directamente accesible por esa interfaz y no especiales enrutamiento es necesario. Si un host es visible con una dirección MAC, entonces es un anfitrión local accesible con una entrada en la tabla ARP, y los paquetes son enviados allí directamente.

Banderas

Hay un buen número de banderas, todos los cuales están cubiertos en la página del manual de FreeBSD para `netstat (1)`,
reproducida en la Tabla 12.3, "Banderas y Significados tabla de rutas" con algunas modificaciones.

Tabla 12.3. Banderas y significados de la tabla de rutas

Carta	Bandera	Significado
1	RTF_PROTO1	Protocolo bandera de enrutamiento específica # 1
2	RTF_PROTO2	Protocolo bandera de enrutamiento específica # 2
3	RTF_PROTO3	Protocolo bandera de enrutamiento específica # 3
B	RTF_BLACKHOLE	Deseche los paquetes durante las actualizaciones
b	RTF_BROADCAST	Representa una dirección de difusión
C	RTF_CLONING	Generar nuevas rutas en el uso
c	RTF_PRCLONING	Especificado por el Protocolo de generar nuevos rutas de uso
D	RTF_DYNAMIC	Creado dinámicamente por redirección
T	RTF_GATEWAY	Destino requiere el reenvío por intermediario
H	RTF_HOST	Anfitrión entrada (neto de otro modo)
L	RTF_LLINFO	Válido protocolo para enlazar dirección traducción
M	RTF_MODIFIED	Modificado dinamicamente (Por redirigir)
R	RTF_REJECT	Host o red inalcanzable
S	RTF_STATIC	Agregado manualmente
U	RTF_UP	Ruta utilizable
W	RTF_WASCLONED	La ruta se generó como resultado de la clonación
X	RTF_XRESOLVE	Daemon externo se traduce proto vincular dirección

Por ejemplo, una ruta marcado como UGS es una ruta utilizable, los paquetes se envían a través de la puerta de entrada en la lista, y
se trata de una ruta estática.

Refs

En esta columna se cuenta el número actual de los usos activos de una ruta determinada.

Uso

Este contador es el número total de paquetes enviados a través de esta ruta. Esto es útil para determinar si una ruta en realidad se está utilizando, ya que continuamente incrementar como fluyen los paquetes si se ha utilizado esta ruta.

Netif

La interfaz de red utilizada para esta ruta.

Expirar

Para las entradas dinámicas, este campo muestra el tiempo hasta el vencimiento de esta ruta si no se utiliza de nuevo.

Usando traceroute

Traceroute es una herramienta útil para probar y verificar rutas y funcionalidad multi-WAN, entre otros utiliza. Esto le permitirá ver cada "salto" a lo largo de la ruta de un paquete a medida que viaja de un extremo al otro, junto con la latencia encontrado para llegar a ese punto intermedio. En pfSense, puede realizar una

traceroute, vaya a Diagnósticos Traceroute, o mediante el uso traceroute en la línea de comandos. Desde los clientes que ejecutan Windows, el programa está disponible bajo el nombre tracert.

Cada paquete IP contiene un tiempo de vida (TTL). Cuando un router pasa un paquete, se decrementa el TTL por uno. Cuando un router recibe un paquete con un TTL de 1 y el destino no es un localmente conectado a la red, el router devuelve un mensaje de error ICMP - Time-to-live superado - y las gotas el paquete. Esto es para limitar el impacto de los bucles de enrutamiento, que de otro modo causar cada paquete a bucle indefinidamente.

Traceroute utiliza esta TTL a su ventaja para trazar la ruta a un destino de red específica. Comienza por enviando el primer paquete con un TTL de 1. El primer router (normalmente puerta de enlace predeterminada del sistema) se
devolver el time-to-live error ICMP superado. El tiempo entre el envío del paquete y recibir el error ICMP es la hora que se muestra, que se enumeran junto con la IP que envió el error y su DNS inversa, si cualquier. Tras el envío de tres paquetes con un TTL de 1 y mostrar sus tiempos de respuesta, se incrementará el TTL a 2 y envía tres paquetes más, teniendo en cuenta la misma información para el segundo salto. Se mantiene incrementando el TTL hasta que alcanza el destino especificado, o excede el número máximo de lúpulo.

Funciones de encaminamiento de rastreo de forma ligeramente diferente en los sistemas operativos de tipo Unix (BSD, Windows y Linux,
Mac OS X, Unix, etc.) Windows utiliza los paquetes de solicitud de eco ICMP (pings), mientras que los sistemas de tipo Unix utilizan
Paquetes UDP. ICMP y UDP son protocolos de capa 4, y traceroute se realiza en la capa 3, por lo que el protocolo utilizado es en gran medida irrelevante, excepto cuando se considera la configuración de la política de enrutamiento. Traceroute desde
Los clientes de Windows será la política de enrutado basado en la regla que permite las solicitudes de eco ICMP, Enestejemplo,Unix
como clientes serán enviados por la regla que coincide con los puertos UDP en uso.

#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 hops max, 40 byte packets
 1 núcleo (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
 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 se puede ver, se tardó 10 saltos para llegar allí, y la latencia generalmente aumenta con cada salto.

Rutas y VPNs

Dependiendo de la VPN está usando, puede o no puede ver una demostración de ruta en la tabla para el extremo lado. IPsec no utiliza la tabla de enrutamiento, en su lugar se controla internamente en el núcleo usando la IPsec SPD. Las rutas estáticas nunca causarán el tráfico que se dirige a través de una conexión IPsec. Usos OpenVPN la tabla de enrutamiento del sistema y, como tal, usted verá las entradas para las redes alcanzables a través de una OpenVPN
túnel, como en el siguiente ejemplo:

#netstat-rn
Las tablas de enrutamiento

Internet:

Destino	Entrada	Banderas	Refs	Use	Netif de vencimiento
defecto	10.34.29.1	UGS	0	19693837	ng0
10.34.29.1	72.69.77.6	UH	1205590		ng0
72.69.77.6	lo0	UHS	00		lo0
172.17.212.0/22	192.168.100.1	UGS	0617		tun0
127.0.0.1	127.0.0.1	UH	00		lo0
192.168.10.0/24	enlace # 2	UC	00		em0
192.168.100.1	192.168.100.2	UH	30		tun0
192.168.130.0/24	192.168.100.1	UGS	0144143		tun0
192.168.140.0/24	192.168.100.1	UGS	00		tun0

La interfaz OpenVPN es 192.168.100.2, con una pasarela de 192.168.100.1 y la interfaz es tun0. Hay tres redes con rutas OpenVPN empujadas 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 enrutados como OpenVPN, porque el túnel de IPsec en sí no tiene IPs. Cuando se ejecuta traceroute a un destino a través de IPsec, verá un tiempo de espera para el salto que es el túnel de IPsec por esta razón.

Capítulo 13. Bridging

Normalmente cada interfaz en pfSense representa su propio dominio de difusión con una subred IP única, actuando de la misma como interruptores separados. En algunas circunstancias es deseable o necesario combinar múltiples interfaces en un único dominio de difusión, donde dos puertos en el firewall actuarán como si se están en el mismo switch, excepto el tráfico entre las interfases se puede controlar con las reglas del cortafuegos. Este que comúnmente se conoce como un cortafuegos transparente.

Tender un puente y bucles de Capa 2

Al puente, es necesario tener cuidado para evitar bucles de Capa 2, o tener una configuración del switch en el lugar que les maneja como usted desea. Un bucle de capa 2 es cuando se crea el mismo efecto que si se ha conectado ambos extremos de un cable de conexión en el mismo interruptor. Si usted tiene un pfSense instalar con dos interfaces, colmar esas interfaces juntas, a continuación, conecte ambas interfaces en el mismo interruptor se ha creado un la capa 2 de bucle. La conexión de dos cables de conexión entre dos switches también hace esto. Switches gestionados emplear Spanning Tree Protocol (STP) para manejar este tipo de situaciones, ya que a menudo es deseable tener varios enlaces entre los switches, y usted no quiere que su red sea expuesto para completar Meltdown por alguien de conectar un puerto de red en otro puerto de red. STP no está habilitado defecto en todos los switches gestionados embargo, y casi nunca es disponible con switches no administrados. Sin STP, el resultado de un bucle de capa 2 es marcos de la red se encierre en un círculo sin fin y la red cesará por completo de funcionar hasta que se retira el bucle.

En pocas palabras - puente tiene el potencial de fundir completamente la red a la que está conectando en si usted no ve lo que usted está conectando dónde.

Bridging y cortafuegos

Filtrar con funciones de interfaces puenteadas manera diferente que con interfaces enrutadas. Las reglas de firewall se aplican en cada interfaz miembro del puente en forma de entrada. Los que han sido utilizando pfSense desde hace bastante tiempo una casilla de verificación Habilitar el filtrado de puente sobre el sistema recordará
 Página Avanzadas. Hay información obsoleta en numerosos lugares referenciar esta casilla de verificación. Lo fue heredada de m0n0wall, cosa que salvar de una manera diferente. Desde pfSense utiliza un diferente puente metodología de esta caja es innecesaria, y con la forma en que la metodología de puente en el más reciente Versiones de FreeBSD trabaja que es imposible tener un puente no filtrado a menos que deshabilite pf completo.

Tender un puente dos redes internas

Se puede acortar dos interfaces internas para combinarlos en el mismo dominio de difusión y permitir filtrado en el tráfico entre las dos interfaces. Esto se hace comúnmente con interfaces inalámbricas se configura 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 de LAN y OPT se utilizará en lugar de un interruptor
en las redes de las que se necesitan sólo dos sistemas internos. Usted puede encontrar escenarios donde dos interfaces del firewall deben estar en el mismo dominio de difusión por otra razón.

> Nota
>
> Existen requisitos adicionales y restricciones al puente interfaces inalámbricas porque de la manera 802.11 funciones. Vea la sección llamada "Bridging e inalámbrico" para obtener más información.

DHCP y Puentes Internos

Si a salvar una red interna a otra, dos cosas deben hacerse. En primer lugar, asegúrese de que DHCP sólo se ejecuta en la interfaz principal (la que tiene la dirección IP) y no la que se está puenteado.

En segundo lugar, se necesita una regla de firewall adicional en la parte superior de sus reglas en esta interfaz OPT para permitir el tráfico DHCP.

Normalmente, al crear una regla para permitir el tráfico en una interfaz, se especifica la fuente similar a "OPT1 Subred ", por lo que sólo se permite el tráfico desde la subred de ese segmento. Con DHCP, que no es suficiente. Debido a que un cliente no cuenta aún con una dirección IP, una solicitud DHCP se realiza como una emisión. Para dar cabida a estas solicitudes, debe crear una regla en la interfaz de puente con el conjunto de Protocolo a UDP, la fuente es 0.0.0.0, puerto de origen 68, Destino 255.255.255.255, puerto de destino 67. Añadir una descripción que indica esta voluntad Permitir DHCP, a continuación, haga clic en Guardar y Aplicar cambios. Lo harás terminar con una norma que se parece a la Figura 13.1, "regla de cortafuegos para permitir el DHCP".

Figura 13.1. Regla para permitir DHCP Firewall

Después de añadir esa regla, los clientes en el segmento de puente debe ser capaz de realizar con éxito las solicitudes de el daemon de DHCP que escucha en la interfaz a la que está puenteado.

Bridging OPT para WAN

Superar una interfaz OPT con WAN permite utilizar direcciones IP públicas de la red interna que tener una puerta de enlace IP que reside en la red WAN. Una situación en la que esto es común es para DHCP asignado direcciones IP públicas. Usted puede utilizar pfSense para proteger los sistemas que obtienen directamente IPs públicas desde un servidor DHCP de su ISP mediante el uso de una interfaz de puente. Esto también es útil en escenarios con bloque de IP pública única, donde usted necesita IPs públicas directamente asignados a los hosts, tal como se describe en la sección llamado "subred IP única."

Cerrando la interoperabilidad

Dado que las interfaces con puente se comportan de manera diferente que las interfaces normales en algunos aspectos, hay algunos cosas que son incompatibles con el puente, y otros donde se deben hacer consideraciones adicionales para acomodar puente. En esta sección se describen las funciones que funcionan de manera diferente con puente que con interfaces no puenteado.

Portal Cautivo

Portal Cautivo (capítulo 23, Portal Cautivo) no es compatible con puente, ya que requiere una IP al ser un puente de la interfaz, utilizado para servir a los contenidos del portal. Las interfaces puenteadas no tienen un IP asignada.

CARP

CARP (capítulo 24, Firewall de redundancia / alta disponibilidad) no es compatible con puente en este tiempo - pero, hay algunos hacks manuales. El uso de la carpa con redes que implican puente no es generalmente se recomienda, pero este tipo de configuración ha trabajado para un número de individuos. Mucho cuidado se debe tomar para manejar la capa 2 bucles, que son inevitables en un escenario CARP + Bridge. Cuando dos segmentos de red están puenteados, que son en efecto fundido en una sola red más grande, como se discutió anteriormente

en este capítulo. Cuando se añade CARP en la mezcla, lo que significa que habrá dos caminos entre la interruptores para cada interfaz respectiva, creando un bucle.

Switches administrados pueden manejar esto con Spanning Tree Protocol (STP), pero los switches no gestionables tener defensas contra looping. Si no se controla, un bucle puede aportar una red de rodillas y hacerlo imposible pasar todo el tráfico. Si STP no está disponible, hay otros dos enfoques para el manejo de un tender un puente en este escenario, similar pero no tan elegante como STP. Ambos métodos requieren el cambio de archivos en el sistema de pfSense, y no sobreviviría una copia de seguridad / restaurar sin consideración especial. Estos técnicas son un cron secuencia de comandos para administrar el puente, o una DEVD gancho para gestionar el puente. Ambos de estos métodos se describen en un post sticky en el foro CARP / VIP [http://forum.pfsense.org/index.php/tema, 4984.0.html] 0.1

Configurar los servidores de seguridad principal y de respaldo

Configurar los servidores de seguridad principal y de respaldo como lo haría con cualquier implementación de CARP, como cubiertos en el capítulo 24, Firewall de redundancia / alta disponibilidad. Configurar la interfaz de puente tanto en el primaria y secundaria, usando la misma descripción de la interfaz. Si el puente es OPT1 en la primaria, hacen OPT1 en el secundario. No conecte los dos puentes a la vez hasta el final. Lo harás tenga que ser capaz de acceder a la pfSense WebGUI desde una interfaz de servidor de seguridad distinta de la interfaz de puente.
Usted tendrá que realizar todos estos pasos, tanto para los servidores de seguridad primaria y secundaria.

Configuración STP

Incluso con STP activo, será necesaria alguna configuración en el switch con el fin de empujar a STP en tomar la decisión correcta sobre qué puerto debe mantenerse abierta y que debe ser bloqueado. De otra manera usted podría terminar con una situación en la que el tráfico es fluido en realidad a través de la copia de seguridad de enrutador tender un puente en lugar del router primario, lo que lleva a un comportamiento impredecible. Puerto de bloqueo en esta situación se controla mediante el establecimiento de las prioridades de puertos y costes de la ruta.
En un interruptor de Cisco, la configuración sería algo como esto:

```
interfaz FastEthernet0 / 1
  Descripción Firewall - Tel - Puerto DMZ
  switchport access vlan 20
  spanning-tree vlan 20 port-priority 64
  no cdp permitir


interfaz FastEthernet0 / 2
  Descripción Firewall - Copia de seguridad - Puerto
DMZ
  switchport access vlan 20
  vlan spanning-tree 20 costó 500
  no cdp permitir
```

Al dar el puerto de la primaria una prioridad más baja que lo normal (64 vs el predeterminado 128), será más probable para ser utilizado, especialmente teniendo en cuenta el coste de la ruta más alta (500 vs el valor predeterminado 19) del otro puerto. Estos valores se puede comprobar de la siguiente manera (en el interruptor):

#show spanning-tree interface FastEthernet0 / 1

```
Interfaz FastEthernet0 / 1 (puerto 13) en el árbol de expansión 20 es EXPEDICION
Ruta Puerto costó 19, la prioridad de puerto 64
Raíz Designada tiene prioridad 32768, dirección 0002.4b6e.xxxx
Puente Designado tiene prioridad 32768, dirección 0002.b324.xxxx
Puerto designado es 3, camino cuesta 131
Timers: mensaje de la edad 6, dilación 0, tecla 0
BPDU: 18411032 enviado, recibido 16199798
```

#show spanning-tree interface FastEthernet0 / 2

[1] http://forum.pfsense.org/index.php/topic, 4984.0.html

```
Interfaz FastEthernet0 / 2 (puerto 14) en el árbol de expansión 20 es BLOQUEO
Ruta Puerto costó 500, la prioridad de puerto 128
Raíz Designada tiene prioridad 32768, dirección 0002.4b6e.xxxx
Puente Designado tiene prioridad 32768, dirección 0002.b324.xxxx
Puerto designado es 4, camino cuesta 131
Timers: mensaje de la edad 6, dilación 0, tecla 0
BPDU: envió 434174, recibido 15.750.118
```

Como puede ver, puerto del switch del sistema primario es el reenvío es que debería ser, y el puerto de copia de seguridad es
bloqueo. Si el tráfico deja de fluir a través del puerto principal, la copia de seguridad debe cambiar a un desvío estado.

Interruptores de otros proveedores admiten la funcionalidad similar. Consulte la documentación del conmutador para información sobre la configuración de STP.

En pfSense 2.0, STP puede ser configurado y realiza directamente en una interfaz de puente.

Secuencia check CARP para cron

En este método, una secuencia de comandos se ejecuta desde cron cada minuto y comprueba si el sistema está o MAESTRO
RESPALDO del clúster CARP. Si el sistema está MAESTRO, el puente es criado, si el sistema es
COPIA DE SEGURIDAD, el puente es bajado. Evita que el bucle por sólo tener un puente activo en un momento dado tiempo, pero como usted puede decir probablemente por la frecuencia con la cron script se ejecuta, puede ser tanto como un minuto
del tiempo de inactividad de los sistemas de puente antes de que el script detecta el interruptor y activa el puente de copia de seguridad.

Agregue la secuencia de comandos

En primer lugar es necesario agregar una secuencia de comandos para comprobar el estado de su CARP y modificar el estado de su puente en consecuencia.
A continuación se proporciona un ejemplo que se puede utilizar. También está disponible para su descarga [http:// files.pfsense.org / misc / bridgecheck.sh].

```
#! / Bin / sh
#
Secuencia check # CARP para puentear
#
# De eblevins del foro
#
si carp0 ifconfig | grep RESPALDO> / dev / null 2> & 1; entonces
        / Sbin / ifconfig bridge0 abajo
más
        / Sbin / ifconfig bridge0 hasta
fi
```

Copie ese script en alguna parte, por ejemplo, `/ Usr / bin / bridgecheck.sh`. La siguiente comando descargar este archivo desde files.pfsense.org y guardarlo como `/ Usr / bin / bridgecheck.sh`.

```
#buscar-o / usr / bin / bridgecheck.sh \
   http://files.pfsense.org/misc/bridgecheck.sh
```

Entonces usted necesita para hacer el script ejecutable mediante la ejecución del siguiente comando.

```
#chmod + x / usr / bin / bridgecheck.sh
```

Programe la secuencia de comandos

Ahora lo que necesita para programar la secuencia de comandos para ejecutar. Descarga una copia de seguridad de su configuración en el
Diagnóstico Pantalla Copia de seguridad / Restaurar. Abra la configuración en un editor de texto, y la búsqueda de <cron>. Va a encontrar la sección de la configuración que contiene todas las tareas programadas que cron carreras.

```
<cron>
 <item>
  <minuto> 0 </ minuto>
  <hora> * </ hora>
  <mday> * </ mday>
  <mes> * </ mes>
  <wday> * </ wday>
  raíz <quién> </ who>
  <comando> / usr / bin / newsyslog </ command> nice-n20
 </ Item>
 <item>
  <minuto> 1,31 </ minuto>
  <hora> 0-5 </ hora>
  <mday> * </ mday>
  <mes> * </ mes>
  <wday> * </ wday>
  raíz <quién> </ who>
  <comando> / usr / bin / adjkerntz-a </ command> nice-n20
 </ Item>
```

Añadir bridgecheck.sh como un cron entrada. Agregando la siguiente ejecutará el script cada minuto.

```
 <item>
  <minuto> * / 1 </ minuto>
  <hora> * </ hora>
  <mday> * </ mday>
  <mes> * </ mes>
  <wday> * </ wday>
  raíz <quién> </ who>
  <comando> / usr / bin / bridgecheck.sh </ command>
 </ Item>
```

Asegúrese de cambiar tanto el primario y el secundario.

Desactivar puente en el arranque

Usted tendrá que añadir un comando a la configuración para bajar el puente en el momento del arranque. Esto le ayudará a
prevenir bucles de Capa 2, como bridgecheck.sh traerá puente del maestro CARP en línea dentro de 1 minuto.
Por encima de la línea que dice `</ Sistema>`, añadir la siguiente línea.

<shellcmd> / sbin / ifconfig bridge0 abajo </ shellcmd>

Guarde los cambios en ambos archivos de configuración. Ahora restaurar las configuraciones modificadas tanto a la primaria y la secundaria. Los cortafuegos se reiniciará después de la restauración de la configuración, y cuando se iniciar una copia de seguridad que debe ser completamente funcional.

DEVD Ganchos

Esta solución sólo es posible en pfSense 1.2.3 o posterior, e implica el uso de DEVD para coger el real
Transición de estado CARP como sucede. Editar `/ Etc / devd.conf` en la copia de seguridad y señor, y añade estas líneas:

```
notificar 100 {
             partido "sistema" "IFNet";
             partido "tipo" "LINK_UP";
             igualar "subsistema" "carpa";
             acción "/ usr / local / bin / carpup";

};
notificar 100 {
```

```
                partido "sistema" "IFNet";
                partido "tipo" "LINK_DOWN";
                igualar "subsistema" "carpa";
                acción "/ usr / local / bin / carpdown";

};
```

A continuación, cree dos nuevos archivos: `/ Usr / local / bin / carpup`

```
#! / Bin / sh
/ Sbin / ifconfig bridge0 hasta
```

Y: `/ Usr / local / bin / carpdown`

```
#! / Bin / sh
/ Sbin / ifconfig bridge0 abajo
```

A continuación, hacer esos scripts ejecutables:

```
#chmod a + x / usr / local / bin / carpup
#chmod a + x / usr / local / bin / carpdown
```

Eso hará que automáticamente el puente arriba y hacia abajo cada vez que se detecta un cambio de estado CARP.

Solución de problemas de conmutación por error de puente

Si algo no está funcionando como se pretendía, compruebe el estado Página Interfaces en ambos sistemas para revisar la `bridge0` interfaz, y la página de estado CARP para verificar la maestría CARP o el estado de copia de seguridad. Usted
puede ejecutar bridgecheck.sh desde la línea de comandos, así como comprobar el estado de la interfaz utilizando ifconfig.
La comprensión de la FreeBSD OS subyacente puede ser necesario solucionar con éxito cualquier problemas con este tipo de despliegue.
Muchos problemas con CARP y Bridging surgirán de bucles de conmutación y cuestiones de STP. Cruce el sección llamada "CARP" otra vez, y compruebe también la configuración del interruptor para ver el estado del puerto para su
puenteado interfaces. Si los puertos están bloqueando cuando deberían estar expedición, es probable que necesites para ajustar la configuración de STP o emplear una de las técnicas alternativas para apagar un puente de respaldo.

Multi-WAN

Tender un puente por su naturaleza es incompatible con multi-WAN en muchos de sus usos. Cuando se utiliza de puente, comúnmente algo distinto de pfSense será la puerta de enlace predeterminada para los hosts de la puenteado interfaz, y que el router es el único que puede dirigir el tráfico desde esos hosts. Esto no impide que que el uso de multi-WAN con otras interfaces en el mismo servidor de seguridad que no están puenteados, sólo impactos de los anfitriones en las interfaces de puente donde utilizan algo más que pfSense como su defecto puerta de enlace. Si a salvar múltiples interfaces internas juntos y pfSense es la puerta de enlace predeterminada para su hosts en una interfaz de puente, entonces usted puede utilizar multi-WAN el mismo que con las interfaces no puenteados.

Capítulo 14. LANs virtuales (VLANs)

VLANs proporcionan un mecanismo de segmentación de un solo interruptor en múltiples dominios de difusión, lo que permite
un solo interruptor para funcionar las mismas en forma de múltiples switches. Esto es comúnmente utilizado para la red segmentación de la misma manera que múltiples interruptores podrían ser utilizados, para colocar hosts en un segmento específico
como se ha configurado en el conmutador. Cuando se emplea concentración de enlaces entre conmutadores, dispositivos en el mismo
segmento no tiene por qué residir en el mismo switch. Los conceptos, la terminología y la configuración de las VLAN están todos cubiertos en este capítulo.

Requerimientos

Hay dos requisitos, los cuales se deben cumplir para implementar las VLAN.

. 1 VLAN 802.1Q interruptor que pueda - cada switch gestionado decente fabricado desde aproximadamente el año 2000 admite 802.1Q VLAN trunking. No se puede utilizar VLAN de un conmutador no administrado.

2 Adaptador de red capaz de etiquetado VLAN -. Usted necesitará una tarjeta de red que soporte VLAN hardware etiquetado o tiene la ayuda del marco de largo. Debido a que cada cuadro tiene una etiqueta 802.1Q 4 byte añadido en la cabecera,
el tamaño del marco puede ser de hasta 1522 bytes. Un NIC apoyar el etiquetado VLAN hardware o marcos largos se requiere debido a que otros adaptadores no funcionarán con los marcos más grandes que el 1518 bytes normalidad máximo con 1500 MTU de Ethernet. Esto causará grandes marcos que se retiren, lo que provoca problemas de rendimiento y estancamiento de conexión.

> **Nota**
>
> El hecho de que un adaptador aparece como teniendo la ayuda del marco de largo no garantiza sus Nic implementación específica de ese chipset soporta adecuadamente marcos largos. Realtek `rl (4)` NIC son los mayores infractores. Muchos no tendrán ningún problema, pero algunos no apoyar adecuadamente marcos largos,
> y algunos no aceptan 802.1Q tramas etiquetadas en absoluto. Si tiene algún problema usando uno de las tarjetas de red que figuran en la ayuda del marco de largo, tratando de una interfaz con el etiquetado VLAN hardware
> Se recomienda apoyo. No tenemos conocimiento de algún problema semejante con tarjetas de red que figuran en
> Soporte de hardware VLAN

Interfaces Ethernet con soporte de hardware VLAN:

```
bce (4), bge (4), cxgb (4), em (4), ixgb (4), msk (4), ESN (4), re (4), stge (4),
ti (4),
TXP (4), vge (4).
```

Interfaces Ethernet con soporte de marco de largo:

```
bfe (4), dc (4), fxp (4), joya (4), hme (4), le (4), nfe (4), nve (4), rl (4),
hermana (4),
sk (4), ste (4), tl (4), tx (4), vr (4), xl (4)
```

Terminología

Esta sección cubre la terminología que usted tendrá que entender para implementar correctamente las VLAN.

Canalizaciones

Trunking se refiere a un medio de llevar a varias VLAN en el mismo puerto del switch. Los marcos que salen de un puerto de líneas externas están marcados con una etiqueta 802.1Q en la cabecera, lo que permite que el dispositivo conectado para diferenciar
entre varias VLAN. Puertos troncales se utilizan para conectar varios switches, y para conectar cualquier dispositivos que son capaces de etiquetado 802.1Q y que requieren el acceso a múltiples VLANs. Esto es comúnmente limitado a sólo el router proporcionar conectividad entre las VLAN, en este caso, pfSense, así
como las conexiones a otros conmutadores que contienen múltiples VLANs.

VLAN ID

Cada VLAN tiene un identificador asociado con ella que se utiliza para la identificación de tráfico etiquetado. Este es un número entre 1 y 4094. La VLAN por defecto en los switches es VLAN 1, VLAN y esto no debería usarse al implementar VLAN trunking. Esto se discute en la sección llamada "VLANs y Seguridad ". Además de evitar el uso de VLAN 1, puede elegir qué números de las VLAN que desea a utilizar. Algunos comienzan con VLAN 2 y el incremento por uno hasta el número requerido de VLAN es alcanzado. Otra práctica común es usar el tercer octeto de la subred IP de la VLAN como la VLAN ID. Por ejemplo, si utiliza 10.0.10.0/24, 10.0.20.0/24 y 10.0.30.0/24, es lógico utilizar VLANs 10, 20, y 30 respectivamente. Elija un esquema de asignación de VLAN ID que tenga sentido para usted.

Interfaz de Padres

La interfaz de matriz se refiere a la interfaz física donde residen las VLAN, tales como `em0` o `bge0`. Al configurar las VLAN en pfSense o FreeBSD, cada uno se le asigna una interfaz virtual, a partir de `vlan0` e incrementar en uno por cada VLAN adicional configurado. En pfSense 1.2.x, el número de la interfaz de VLAN no tiene correlación con el ID de VLAN. Usted no debe asignar a su interfaz de padres a cualquier interfaz en pfSense - su única función debe ser como el padre de las VLAN definidas. En algunos situaciones esto va a funcionar, pero pueden causar problemas con la configuración del switch, puede causar problemas con
usando portal cautivo, y te obliga a utilizar VLAN predeterminado del puerto de línea externa, que deben evitarse como se analiza en la sección llamada "VLANs y la seguridad".

Puerto de acceso

Un orificio de acceso se refiere a un puerto del conmutador proporcionar acceso a una única VLAN, donde las tramas no se
etiquetados con una cabecera 802.1Q. Se conecta todos los dispositivos que residen en una sola VLAN a un puerto de acceso.
La mayoría de los puertos del switch se puede configurar como puertos de acceso. Los dispositivos en los puertos de acceso no son conscientes de
cualquier VLAN en la red. Ellos ven cada VLAN lo mismo que si fuera un interruptor sin VLANs.

Doble etiquetado (QinQ)

También es posible duplicar tráfico de etiqueta, usando tanto una etiqueta de 802.1Q exterior e interior. Esto se conoce como QinQ. Esto puede ser útil en grandes entornos de ISP y algunas otras redes muy grandes. Triple etiquetado también es posible. pfSense no es compatible con QinQ en este momento, pero lo hará en 2,0. Estos tipos de ambientes generalmente necesitan el tipo de poder de enrutamiento que sólo un enrutador basado en ASIC de gama alta puede
apoyo y QinQ agrega un nivel de complejidad que no es necesaria en la mayoría de entornos.

VLAN privada (PVLAN)

PVLAN se refiere a la capacidad de algunos interruptores a los hosts del segmento dentro de una sola VLAN. Normalmente
Las máquinas de una sola función VLAN lo mismo que las máquinas de un solo interruptor sin VLANs configuradas. PVLAN proporciona un medio para prevenir los anfitriones en una VLAN de hablar con cualquier otro host en el que VLAN, sólo permite la comunicación entre la central y de su puerta de enlace predeterminada. Esto no es directamente pertinentes para pfSense, pero es una pregunta común tienen los usuarios. Interruptor de funcionalidad como este es el único
manera de evitar la comunicación entre hosts de la misma subred. Sin una función como PVLAN, sin cortafuegos de red puede controlar el tráfico dentro de una subred, ya que nunca toca la puerta de enlace predeterminada.

VLANs y Seguridad

Las VLAN ofrecen un gran medio para segmentar la red y aíslan subredes, pero hay algunos los problemas de seguridad que deben tenerse en cuenta en el diseño e implementación de una solución involucrando las VLAN. VLANs no son inherentemente inseguro, pero pueden dejar una mala configuración de su red vulnerable. También ha habido problemas de seguridad en las implementaciones de VLAN fabricantes de switches ' en el pasado.

La segregación de zonas de confianza

Debido a la posibilidad de una mala configuración, usted debe separar las redes de forma considerable diferentes niveles de confianza en sus propios switches físicos. Por ejemplo, aunque se puede utilizar técnicamente el mismo switch con VLAN para todas sus redes internas, así como la red fuera de la cortafuegos, que se deben evitar como una simple mala configuración del interruptor podría llevar a filtrar El tráfico de Internet en su red interna. Como mínimo, usted debe utilizar dos interruptores de tal escenarios, uno por fuera del firewall y uno interior. En muchos entornos, los segmentos DMZ son también tratada por separado, en un tercer interruptor además de los interruptores de WAN y LAN. En otros, la WAN lado está en su propio interruptor, mientras que todas las redes detrás del servidor de seguridad están en los mismos interruptores utilizando VLANs. ¿Qué escenario es el más apropiado para su red depende de sus circunstancias específicas, y el nivel de riesgo y la paranoia.

Uso de la VLAN1 defecto

Debido VLAN1 es el predeterminado, o "nativo", VLAN, puede ser utilizado de manera inesperada por el conmutador. Es similar al uso de una política por defecto-permitirá en las reglas del firewall en lugar de denegación predeterminada y seleccionar lo que necesita. Siempre es mejor usar una VLAN diferente, y asegurarse de que sólo selecciona los puertos que quiere en su grupo de interruptores para estar en esa VLAN, para limitar un mejor acceso. Interruptores enviarán interna protocolos como STP (Spanning Tree Protocol), VTP (VLAN Trunking Protocol) y CDP (Cisco Protocolo Discover) sin etiqueta sobre la VLAN nativa, donde sus switches utilizan estos protocolos. Es Generalmente es mejor mantener ese tráfico interno aislado de su tráfico de datos.

Si tiene que usar VLAN1, debe tener mucho cuidado para asignar a cada puerto único en cada cambio a una diferentes VLAN, excepto las que desee en VLAN1, y no se crea una interfaz de gestión de el interruptor de VLAN1. También debe cambiar la VLAN nativa del grupo de cambio a una diferente, sin usar, VLAN. Algunos interruptores pueden no apoyan ninguna de estas soluciones, por lo que es típicamente más fácil para mover los datos a una VLAN diferente en lugar de quejarse con la fabricación de VLAN1 disponible. Con VLAN ID del 2 al 4094 para elegir, que es, sin duda, mejor que simplemente ignorar VLAN1 la hora de diseñar su esquema de VLAN.

El uso de VLAN predeterminado del puerto de línea externa

Cuando VLAN etiquetada tráfico se envía a través de un tronco en la VLAN nativa, las etiquetas en los paquetes que coincidan con la VLAN nativa puede ser despojado por el interruptor para preservar la compatibilidad con las redes más antiguas. Peor sin embargo, los paquetes que se doble etiquetado con la VLAN nativa y una VLAN diferente sólo tendrán la etiqueta VLAN nativa eliminado cuando trunking de esta manera y cuando se procesan más tarde, que el tráfico puede terminar en una VLAN diferente. Esto también se conoce como "salto de VLAN".

Como se mencionó en la sección anterior, cualquier tráfico no etiquetado en un puerto de enlace troncal se supone que es el VLAN nativa, que también podría solaparse con una interfaz de VLAN asignada. Dependiendo de cómo el interruptor maneja este tipo de tráfico y cómo es visto por pfSense, utilizando la interfaz directa podría dar lugar a dos interfaces de estar en la misma VLAN.

Limitar el acceso a los puertos de troncales

Debido a un puerto troncal puede hablar con cualquier VLAN en un grupo de interruptores de concentración de enlaces, posiblemente, incluso los no presente en el interruptor de corriente en función de sus configuraciones de conmutación, es importante físicamente asegurar los puertos troncales. También asegúrese de que no hay puertos configurados para trunking que quedan desconectados donde alguien podría enganchar en una sola, accidentalmente o de otra manera. Dependiendo de su interruptor, puede soportan la negociación dinámica de concentración de enlaces. Usted debe asegurarse de esta funcionalidad está deshabilitado o bien restringida.

Otros problemas con los interruptores

Ha habido informes de que algunos switches VLAN basada tendrán fugas tráfico a través de redes VLAN cuando vienen con cargas pesadas, o si una dirección MAC de un PC en una VLAN se ve en otra VLAN.

Estos problemas tienden a estar en los conmutadores más antiguos con firmware anticuado o muy bajo de calidad gestionados
interruptores. Estos tipos de problemas se resolvieron en gran parte, hace muchos años, cuando este tipo de problemas de seguridad
eran comunes. No importa lo que el interruptor de la marca que tiene, hacer algunas investigaciones en línea para ver si es
ha sido sometido a ningún tipo de pruebas de seguridad, y asegurarse de que está utilizando la última versión del firmware. Si bien estos
Muchas de las cosas aquí son específicos de las marcas y modelos particulares de interruptores. Puede haber diferentes consideraciones de seguridad específicas para el interruptor que está utilizando. Consulte su documentación para
problemas son un problema con el cambio, y no pfSense, que son parte de la seguridad general.
recomendaciones sobre la seguridad de VLAN.

Configuración pfSense

En esta sección se explica la configuración de VLAN en el lado pfSense.

Configuración de la Consola de VLAN

Puede configurar las VLAN en la consola usando la función Asignar Interfaces. El ejemplo siguiente muestra cómo configurar dos VLAN, ID 10 y 20, con `le2` como la interfaz principal. La VLAN interfaces se asignan como OPT1 y OPT2.

```
 configuración de la consola pfSense
**********************
 0) Salir (SSH solamente)
 1) Asignar Interfaces
 2) Establezca la dirección IP de la LAN
 3) Restablecer contraseña webConfigurator
 4) Restablecer los valores predeterminados de fábrica
 5) Reinicie el sistema
 6) Sistema de Halt
 7) anfitrión Ping
 8) de Shell
 9) PFtop
10) Registros de filtro
11) Reiniciar webConfigurator
12) pfSense desarrollador Shell
13) Actualización de la consola
14) Desactivar Secure Shell (sshd)
98) Mueva el archivo de configuración de dispositivo
extraíble



Introduzca una opción: 1

Las interfaces válidas son:

le0      00:0 c: 29: d6: e7: dc(Hasta)
LE1      00:0 c: 29: d6: e7: e6(Hasta)
le2      00:0 c: 29: d6: e7: f0(Hasta)
plip0    0


¿Quieres configurar VLANs primero?
Si no va a utilizar las VLAN, o sólo para interfaces opcionales, debe
decir no aquí y utilizar el webConfigurator para configurar VLANs más tarde, si es neces


¿Quieres configurar VLANs ahora [y | n]? y

Capaz interfaces de VLAN:

le0      00:0 c: 29: d6: e7: dc(Hasta)
LE1      00:0 c: 29: d6: e7: e6(Hasta)
```

```
le2      00:0 c: 29: d6: e7: f0 (Hasta)

Introduzca el nombre de la interfaz principal para la nueva VLAN (o nada si terminó): le2
Introduzca la etiqueta de VLAN (1-4094): 10

Capaz interfaces de VLAN:

le0      00:0 c: 29: d6: e7: dc (Hasta)
LE1      00:0 c: 29: d6: e7: e6 (Hasta)
le2      00:0 c: 29: d6: e7: f0 (Hasta)


Introduzca el nombre de la interfaz principal para la nueva VLAN (o nada si terminó): le2
Introduzca la etiqueta de VLAN (1-4094): 20

Capaz interfaces de VLAN:

le0      00:0 c: 29: d6: e7: dc (Hasta)
LE1      00:0 c: 29: d6: e7: e6 (Hasta)
le2      00:0 c: 29: d6: e7: f0 (Hasta)


Introduzca el nombre de la interfaz principal para la nueva VLAN (o nada si terminó): <E


Interfaces VLAN:

vlan0    Etiqueta VLAN 10, le2 interfaz
vlan1    Etiqueta VLAN 20, le2 interfaz


Si no conoce los nombres de las interfaces, puede optar por utilizar
detección automática. En ese caso, desconecte todos los interfaces de ahora antes
golpear 'a' para iniciar la detección automática.


Introduzca el nombre de la interfaz LAN o 'a' para la detección
automática: LE1
Introduzca el nombre de la interfaz WAN o 'a' para la detección
automática: le0
Introduzca el nombre de la interfaz opcional 1 o 'a' para la detección
automática
(O nada si terminó): vlan0
Introduzca el nombre de la interfaz opcional de 2 o 'a' para la detección
automática
(O nada si terminó): vlan1
Introduzca el nombre de la interfaz 3 Opcional o 'a' para la detección
automática
(O nada si terminó): <enter>
Las interfaces se asignan de la siguiente manera:

LAN  -> LE1
WAN  -> le0
OPT1 -> vlan0
OPT2 -> vlan1


¿Quieres continuar [y | n]? y

Un momento mientras recargamos la configuración ...
```

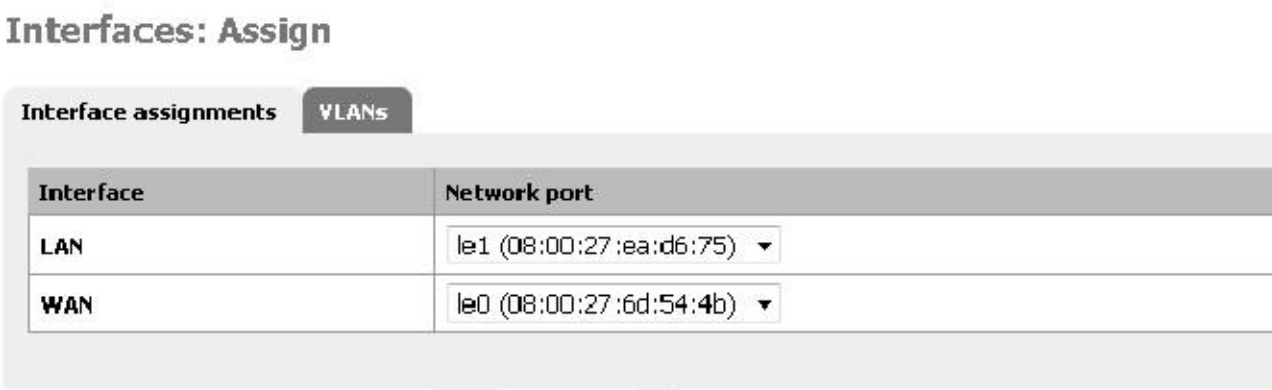
Después de unos segundos, la configuración se recarga y se le devolverá al menú de la consola. ¿Cuándo configurar las interfaces de VLAN en la consola, que no le advierte sobre el reinicio que puede ser necesario

antes de VLAN funcionarán. Algunos adaptadores de red o controladores no funcionan correctamente con las VLAN hasta que se reinicie el sistema. Esto no siempre es necesario, pero no hemos sido capaces de encontrar un medio de detectar cuando esto es necesario. Para estar en el lado seguro, reiniciar después de la instalación inicial de VLAN se recomienda. Para las futuras incorporaciones de VLAN VLAN vez ya están configurados, el reinicio no es requerida.

Configuración de VLAN Interfaz Web

Busque Interfaces Asignar. Figura 14.1, "Interfaces: Asignar" muestra el sistema que se utiliza para este ejemplo. WAN y LAN son asignados como `le0` y `LE1` respectivamente. También es un `le2` interfaz que se utilizará como la interfaz primaria de VLAN.

Figura 14.1. Interfaces: Asignar

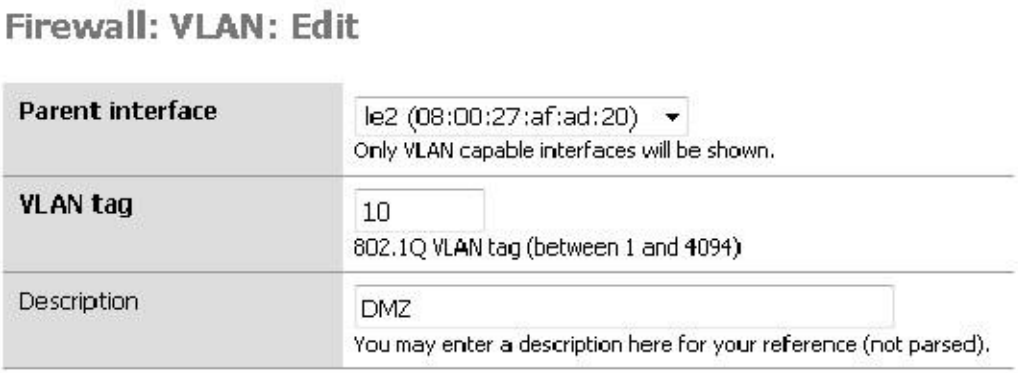


Haga clic en la ficha VLAN. Luego, haga clic para agregar una nueva VLAN, como se muestra en la Figura 14.2, "Lista de VLAN".

Figura 14.2. Lista de VLAN

La pantalla de edición de VLAN ahora se debe mostrar, como en la Figura 14.3, "Edit VLAN". Desde aquí, elige un Interfaz de Padres, le2. A continuación, introduzca una etiqueta VLAN, 10, e introduzca una descripción, por ejemplo, lo que la red es
en esa VLAN (DMZ, Bases de datos, pruebas, etc.)

Figura 14.3. Editar VLAN

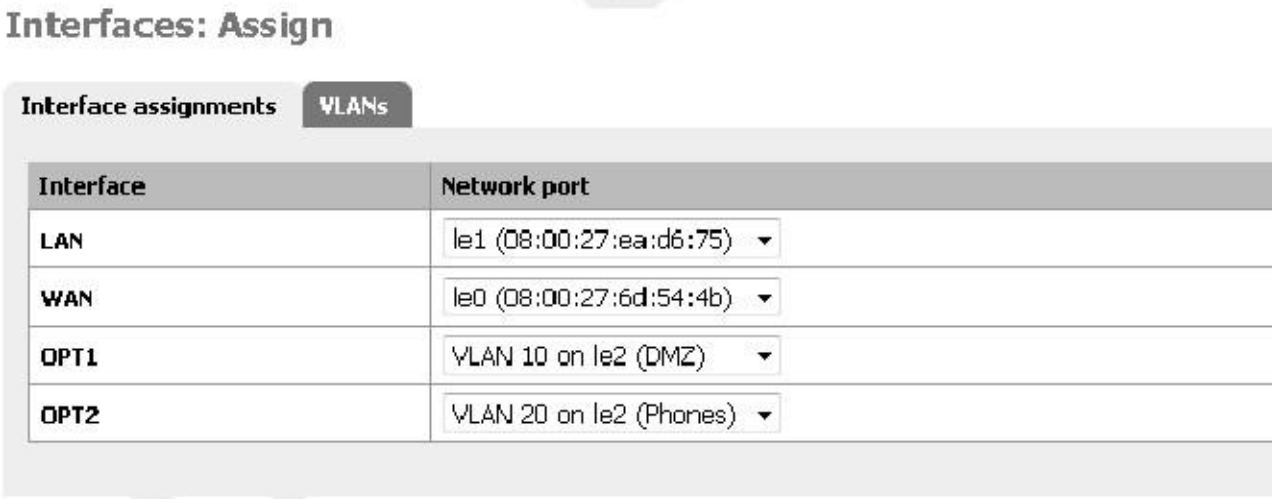


Una vez que se hace clic en Guardar, volverá a la lista de disponibles VLANs, que ahora debe incluir la acaba de agregar VLAN 10. Repita este proceso para agregar redes VLAN adicionales, tales como VLAN 20. Estos pueden
verse en la Figura 14.4, "Lista de VLAN"

Figura 14.4. Lista de VLAN

Ahora, para asignar las VLAN a las interfaces, haga clic en la pestaña de la interfaz de misiones, a continuación, haga clic en, y en el
lista desplegable de asignación de las interfaces disponibles, debería ver las nuevas VLAN. Para OPT1, recoger la interfaz con el ID de VLAN 10. Clickagain, y por OPT2, escoja la interfaz con el ID de VLAN 20.
Cuando termine, se verá algo como la Figura 14.5, "lista Interfaz con VLANs"

Figura 14.5. Lista Interfaz con VLAN



Las interfaces OPT basados en VLAN se comportan como cualquier otra interfaz OPT hacen, lo que significa que deben ser
habilitada, configurado, tendrá que ser configurado reglas de firewall añadidos, y servicios como el servidor DHCP si es necesario. Vea la sección llamada "Fundamentos de configuración Interface" para obtener más información sobre la configuración
interfaces opcionales.

Configuración de conmutación

Esta sección proporciona una guía sobre cómo configurar el switch. Esto ofrece una guía genérica que se aplicará a la mayoría, si no todos los 802.1Q conmutadores con capacidad, luego pasa a cubrir configuración en específico
conmutadores de Cisco, HP, Netgear, y Dell. Tenga en cuenta esta es la configuración mínima expresión se quiere necesidad de VLAN a la función, y no muestra necesariamente la configuración del switch segura ideales para su entorno. Una discusión en profundidad de la seguridad del conmutador está fuera del alcance de este libro.

Cambie Introducción a la configuración

En general, usted tendrá que configurar tres o cuatro cosas en conmutadores con capacidad de VLAN.

. 1 Añadir / define las VLAN - la mayoría de conmutadores tienen un medio de la adición de VLAN, y deben añadirse antes de que se pueden configurar en cualquier puerto.

. 2 Configure el puerto de líneas externas - configurar el pfSense puerto se conecta a un puerto troncal, etiquetado todas las VLAN en la interfaz.

. 3 Configure los puertos de acceso - configurar los puertos de su servidor interno va a utilizar como puertos de acceso en las VLAN deseadas, con VLAN sin etiqueta.

. 4 Configure el puerto VLAN ID (PVID) - algunas de las opciones necesitan configurar el PVID de un puerto. Especifica qué VLAN a utilizar para el tráfico de entrada que puerto del switch. Para algunos interruptores este es un proceso paso a uno, mediante la configuración del puerto como un puerto de acceso en una VLAN particular, automáticamente
el tráfico que viene en las etiquetas en ese puerto. Otras de las opciones necesitan configurar esto en dos lugares. Comprobar
documentación del conmutador para obtener más información si no es que se detalla en este capítulo.

Conmutadores basados Cisco IOS

Configuración y uso de redes VLAN en los switches Cisco con IOS es un proceso bastante sencillo, teniendo sólo un algunos 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 casi la misma sintaxis si no idéntico para configuración.

Crear las VLAN

Las VLAN se pueden crear de forma independiente, o utilizando el protocolo VLAN Trunk (VTP). El uso de VTP puede ser más conveniente, ya que se propagará automáticamente la configuración de la VLAN a todos los interruptores en un dominio VTP, aunque también puede crear sus propios problemas de seguridad y abrir posibilidades para inadvertidamente acabando con su configuración de VLAN. Con VTP, si usted decide que necesita otra VLAN Sólo se necesita agregar a un solo interruptor, y luego todos los demás conmutadores de concentración de enlaces en el grupo puede asignar
puertos a esa VLAN. Si VLAN se configuran de forma independiente, debe agregarlos a cada interruptor por mano. Consulte la documentación de Cisco en VTP para asegurarse de tener una configuración segura no es propenso a destrucción accidental. En una red con sólo unos detectores en ambientes donde las VLAN no cambian con frecuencia, usted es por lo general mejor que no usar VTP para evitar sus posibles caídas.

Standalone VLANs

Para crear VLANs independientes:

```
sw # vlan database
sw (vlan) # vlan 10 nombre "DMZ Servidores "
sw (vlan) # vlan 20 nombrar "Teléfonos"
sw (vlan) # salida
```

VTP VLAN

Para configurar el conmutador para VTP y las VLAN, crear una base de datos VTP en el interruptor principal y luego crear dos VLAN:

```
sw # vlan database
sw (vlan) # servidor VTP
sw (vlan) # dominio VTP example.com
sw (vlan) # VTP contraseña SuperSecret
sw (vlan) # vlan 10 nombre "DMZ Servidores "
sw (vlan) # vlan 20 nombrar "Teléfonos"
sw (vlan) # salida
```

Configurar puerto Trunk

Para pfSense, un puerto de switch no sólo tiene que estar en modo de tronco, pero también debe ser el uso de etiquetado 802.1Q.
Esto se puede hacer de esta manera:

```
sw # configure terminal
sw (config) # interfaz FastEthernet0/24
sw (config-if) # switchport mode trunk
sw (config-if) # switchport dot1q encapsulación del tronco
```

> **Nota**
>
> En algunos switches Cisco IOS más recientes, el método de encapsulación ISL VLAN Cisco-propietario está en desuso y ya no es compatible. Si el interruptor no permite la encapsulación dot1q opción de configuración, sólo es compatible con 802.1Q y usted no necesita preocuparse por la especificación de la encapsulación.

Agregar puertos a la VLAN

Para agregar puertos para estas VLAN, es necesario asignar de la siguiente manera:

```
sw # configure terminal
sw (config) # interfaz FastEthernet0/12
sw (config-if) # switchport mode access
sw (config-if) # switchport access vlan 10
```

Conmutadores basados Cisco CatOS

Crear las VLAN en CatOS es un poco diferente, aunque la terminología es lo mismo que usar VLANs bajo IOS. Usted todavía tiene la opción de utilizar VLAN independientes o VTP o para mantener la VLAN base de datos:

```
# conjunto ejemplo de dominio del servidor de modo VTP
# conjunto VTP passwd SuperSecret
# conjunto vlan 10 nombre dmz
# conjunto vlan 20 nombre teléfonos
```

Y configurar un puerto troncal para manejar automáticamente cada VLAN:

```
#establecer tronco 5/24 en dot1q 1-4094
```

A continuación, añada los puertos a la VLAN:

```
#establecer vlan 10 5/1-8
#establecer vlan 20 5/9-15
```

Switches HP ProCurve

HP ProCurve cambia sólo admiten enlaces troncales 802.1q, por lo que no se necesita ningún examen allí. En primer lugar, telnet en el interruptor y abrir el menú de administración.

Habilitar el soporte VLAN

En primer lugar, soporte VLAN se debe activar el interruptor, si no lo está ya.

1. Elija la configuración de interruptor

2. Seleccione Funciones avanzadas

3. Elija Menú VLAN ...

4. Elija Soporte VLAN

5. Set Enable VLAN a Sí si no lo 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 soportar la mayor cantidad de VLAN
   como se le ha ocurrido que necesitan.

6. Reinicie el interruptor para aplicar los cambios.

Crear las VLAN

Antes de que las VLAN se pueden asignar a los puertos, lo que necesita para crear las VLAN. En la configuración del switch
Menú:

1. Elija la configuración de interruptor

2. Seleccione Funciones avanzadas

3. Elija Menú VLAN ...

4. Elija VLAN Nombres

5. Seleccione Agregar

6. Introduzca el ID de VLAN, 10

7. Introduzca el nombre, LAN

8. Seleccione Guardar

9. Repita los pasos desde Agregar ahorrar para cualquier VLAN restantes

Asignación de troncales de puertos a las VLAN

A continuación, configure el puerto de línea externa para el servidor de seguridad, así como los puertos troncales que van a otros switches
que contiene múltiples VLANs.

1. Elija la configuración de interruptor

2. Elija Menú VLAN ...

3. Elija VLAN Asignación de puerto

4. Seleccione Editar

5. Encuentra el puerto que desea asignar

6. Pulse espacio en defecto VLAN hasta que diga No

7. Hazte a un lado a la columna para cada una de las VLAN en el puerto de línea externa y Prensa espacio hasta que dice
   Etiquetado. Cada VLAN en uso debe ser tocado en el puerto de enlace troncal.

Asignación de puertos de acceso a las VLAN

1. Elija la configuración de interruptor

2. Elija Menú VLAN ...

3. Elija VLAN Asignación de puerto

4. Seleccione Editar

5. Encuentra el puerto que desea asignar

6. Pulse espacio en defecto VLAN hasta que diga No

7. Hazte a un lado a la columna de la VLAN a la que se asignará este puerto

8. Pulse espacio hasta que diga No etiquetado.

Netgear switches gestionados

Este ejemplo se encuentra en una GS108T, pero otros modelos de Netgear que hemos visto son todos muy similares, si no
idéntica. También hay varios otros proveedores, incluyendo Zyxel que venden conmutadores realizados por el mismo fabricante, utilizando la misma interfaz web con un logotipo diferente. Inicie sesión en la interfaz web de su conmutador para comenzar.

Planificación de la configuración de la VLAN

Antes de configurar el switch, lo que necesita saber cuántos VLAN va a configurar, lo que IDS
utilizará y cómo necesita cada puerto de switch que desea configurar. Para este ejemplo, estamos usando un puerto de 8 GS108T, y se configura como se muestra en la Tabla 14.1, "Configuración de VLAN Netgear GS108T".

Tabla 14.1. Netgear configuración VLAN GS108T

Cambie el puerto	Modo VLAN	VLAN asignada
1	tronco	10 y 20, etiquetado
2	acceso	10 sin etiquetar
3	acceso	10 sin etiquetar
4	acceso	10 sin etiquetar
5	acceso	20 sin etiquetar
6	acceso	20 sin etiquetar
7	acceso	20 sin etiquetar
8	acceso	20 sin etiquetar

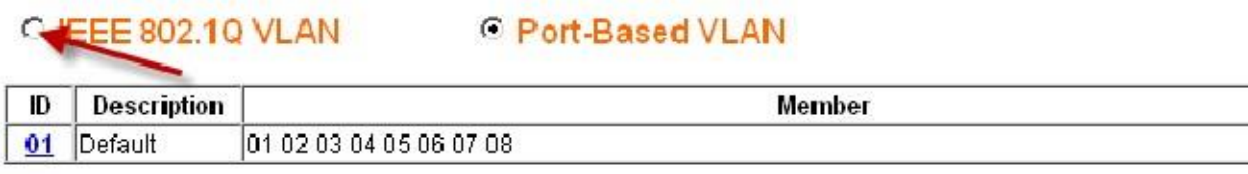
Habilitar 802.1Q VLANs

En el menú del sistema en el lado izquierdo de la página, haga clic en un grupo VLAN Configuración, como se indica en la figura 14.6,
"Grupo VLAN Setting".

Figura 14.6. VLAN Ajuste de grupo

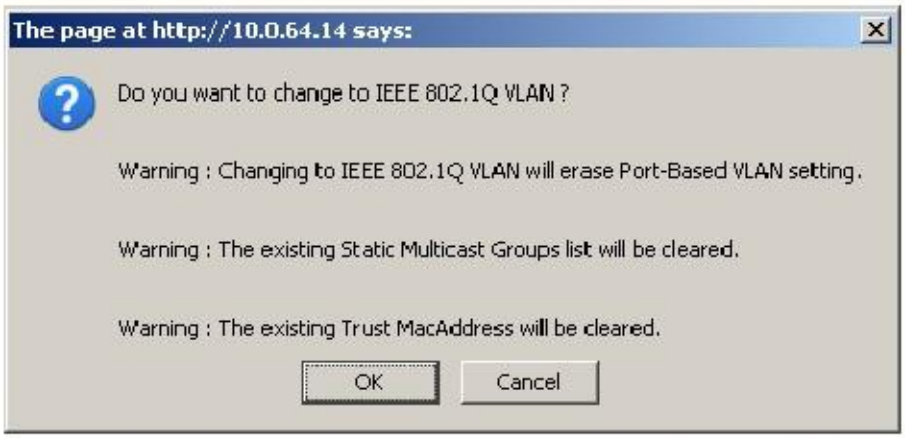
Seleccione IEEE 802.1Q VLAN (Figura 14.7, "Habilitar 802.1Q VLANs").

Figura 14.7. Habilitar 802.1Q VLANs



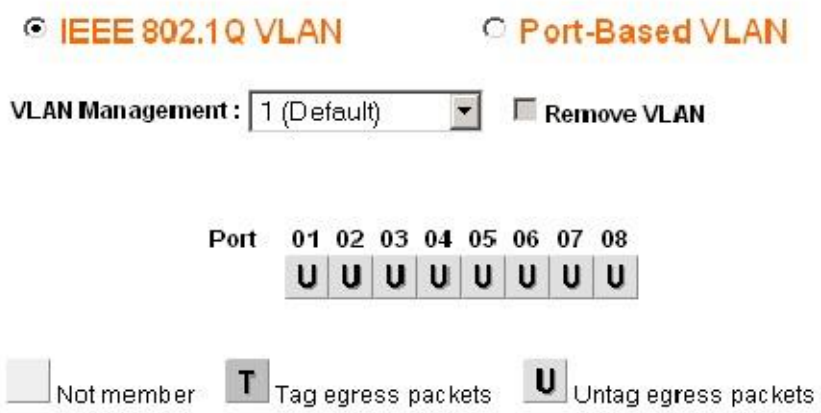
Nos pedirá con una ventana emergente que le preguntará si realmente desea cambiar, y una lista de algunos de los consecuencias, como se muestra en la Figura 14.8, "Confirmar cambio de 802.1Q VLAN". Si desea tronco VLAN, debe utilizar 802.1Q. Haga clic en Aceptar.

Figura 14.8. Confirmar cambio de VLAN 802.1Q



Después de hacer clic en Aceptar, la página se actualizará con la configuración de VLAN 802.1Q como se muestra en Figura 14.9, "Configuración estándar 802.1Q".

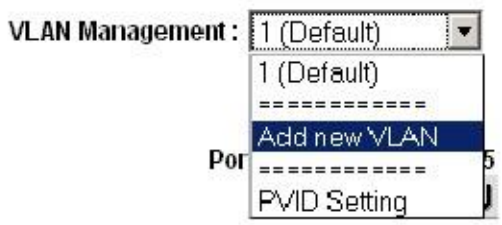
Figura 14.9. Configuración estándar 802.1Q



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 la Figura 14.10, "Add new VLAN".

Figura 14.10. Añadir nueva VLAN



Introduzca la ID de VLAN para esta nueva VLAN, haga clic en Aplicar. La pantalla VLAN ahora le permitirá configurar VLAN 10 (Figura 14.11, "Add VLAN 10"). Antes de configurar, lo haré de nuevo, haga clic en Agregar

nueva VLAN como se muestra en la Figura 14.10, "Add new VLAN" para añadir VLAN 20 (Figura 14.12, "Añadir VLAN 20 ").

Figura 14.11. Añadir VLAN 10

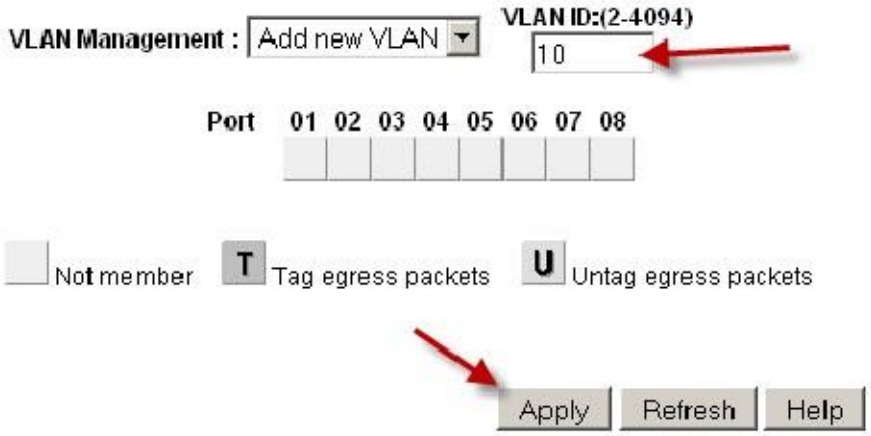
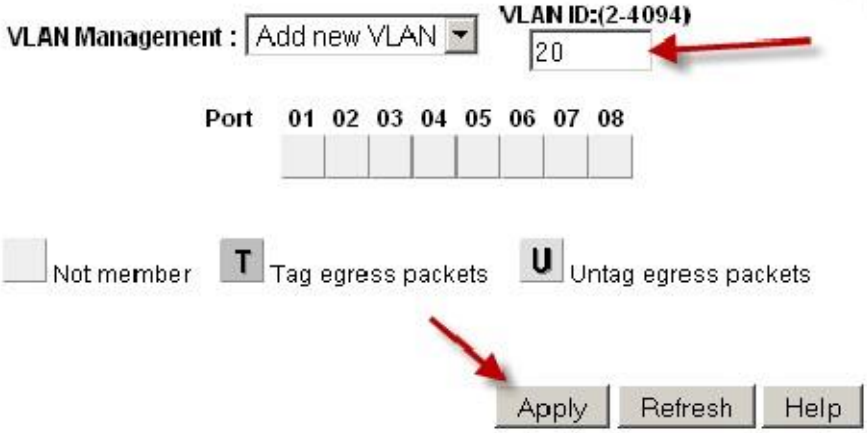


Figura 14.12. Añadir VLAN 20



Añadir tantas VLANs como necesite, y luego continuar con la siguiente sección.

Configure el etiquetado VLAN

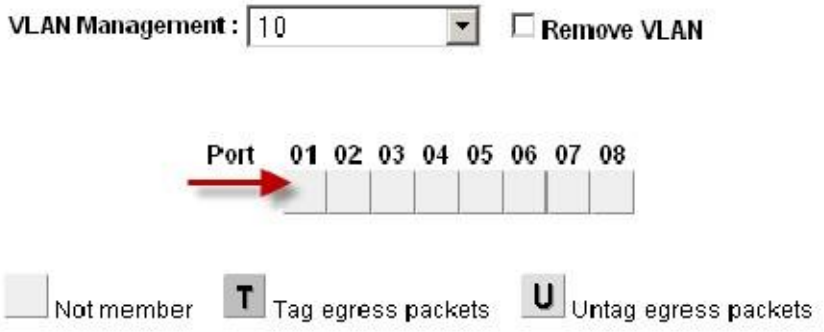
Cuando seleccione una VLAN del Gestión VLAN desplegable, que muestra cómo esa VLAN está configurado en cada puerto. Un cuadro en blanco significa que el puerto no es miembro de la VLAN seleccionada. La caja que contiene Tsignifica la VLAN se envía en ese puerto con la etiqueta 802.1Q. Uindica que el puerto es un miembro de esa VLAN y sale del puerto sin etiquetar. El puerto de línea externa tendrá que tener las dos VLANs añadido y etiquetados.

Nota

No cambie la configuración del puerto que está utilizando para acceder a la interfaz web del switch. Se podría encerrarse a cabo, con el único medio de recuperación en el GS108T está golpeando en el botón Restablecer valores de fábrica - que no tiene una consola serie. Para los interruptores que han consolas seriales, tienen un cable de módem nulo mano en caso de desconectarse de conectividad de red con el interruptor. Configuración de la VLAN de administración se describe más adelante en esta sección.

Haga clic en las casillas de debajo el número de puerto, como se muestra en la Figura 14.13, "pertenencia Toggle VLAN" para alternar entre las tres opciones de VLAN.

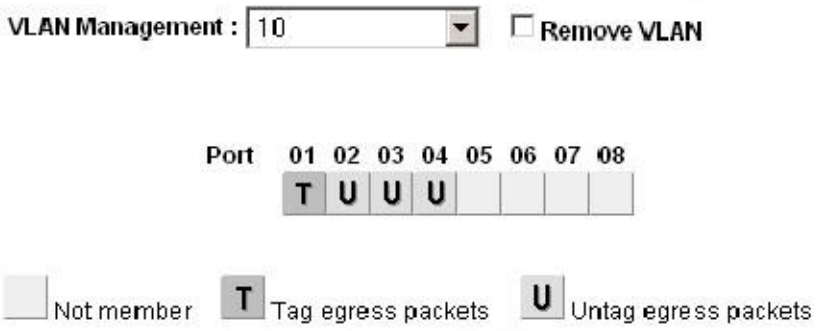
Figura 14.13. Membresía Toggle VLAN



Configure VLAN 10 miembros

Figura 14.14, "Configuración de VLAN 10 membresía" muestra VLAN 10 configurarse como se describe en Tabla 14.1, "Configuración de VLAN Netgear GS108T". Los puertos de acceso en esta VLAN se establecen en sin etiqueta, mientras que el puerto de línea externa está establecida en etiquetado.

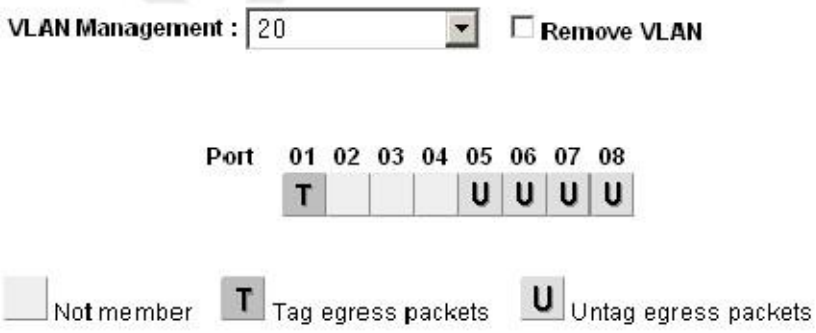
Figura 14.14. Configure VLAN 10 miembros



Configure VLAN 20 membresía

Seleccionar 20 de la Administración de VLAN desplegable para configurar la pertenencia de puertos para VLAN 20.

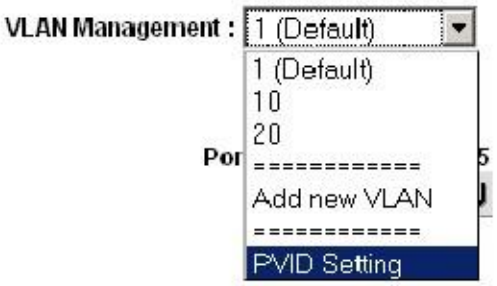
Figura 14.15. Configure VLAN 20 membresía



Cambiar PVID

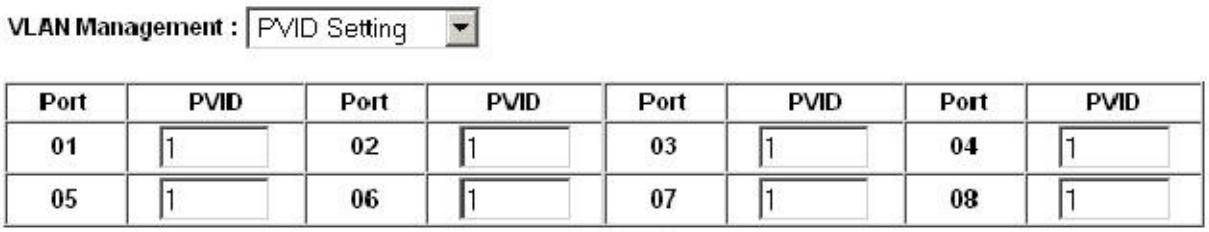
En switches Netgear, además de la configuración de marcado configuradas previamente, también debe configurar el PVID para especificar la VLAN utilizada para las tramas entrar en ese puerto. En la caída de Gestión VLAN abajo, haga clic en Configuración PVID como se muestra en la Figura 14.16, "PVID Setting".

Figura 14.16. Ajuste PVID



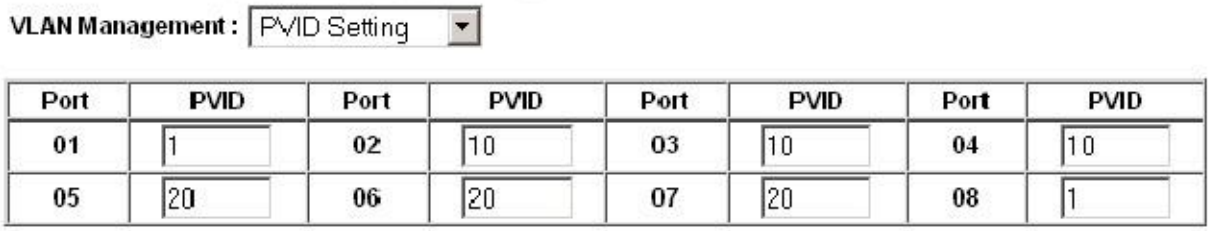
La configuración predeterminada es PVID de VLAN 1 para todos los puertos, como se muestra en la Figura 14.17, "Default PVID
Configuración ".

Figura 14.17. PVID Configuración por defecto



Cambie el PVID para cada puerto de acceso, pero dejar el puerto de línea externa y el puerto que está utilizando para el acceso
interfaz de administración del conmutador establece en 1. Figura 14.18, "Configuración de VLAN 10 y 20 PVID" muestra la configuración de PVID coincidir las asignaciones de los puertos que se muestran en la Tabla 14.1, "Netgear GS108T
Configuración de VLAN ", con el puerto 8 se utiliza para acceder a la interfaz de administración del conmutador. Aplicar sus cambios cuando haya terminado.

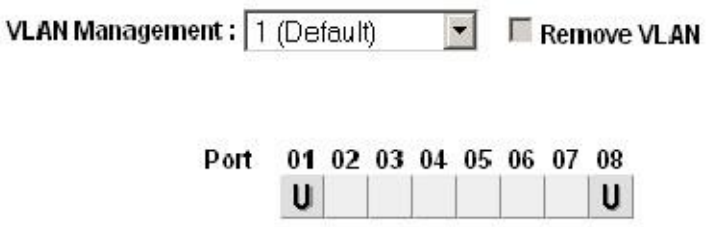
Figura 14.18. VLAN 10 y 20 de configuración de PVID



Eliminar VLAN configuración 1

De forma predeterminada, todos los puertos son miembros de la VLAN 1 con marcos de egreso sin etiquetar. Seleccionar 1 (predeterminado)
de la Administración de VLAN desplegable. Eliminar VLAN 1 de todos los puertos excepto el que usted está utilizando para gestionar el switch y el puerto de línea externa, por lo que no se desconecta. Estoy utilizando el puerto 8 para gestionar el
cambiar. Al terminar, la pantalla debe ser similar a la Figura 14.19, "Remove VLAN 1 miembro".

Figura 14.19. Eliminar VLAN 1 membresía



Aplique los cambios cuando haya terminado.

Verifique la funcionalidad VLAN

Configure las VLAN en pfSense, incluyendo el servidor DHCP en las interfaces de VLAN si va a estar mediante DHCP. Conecte los sistemas en los puertos de acceso configurados y probar la conectividad. Si todo funciona si lo desea, continúe con el siguiente paso. Si las cosas no funcionan como se pretende, revisar su etiquetado y PVID configuración en el switch, y la configuración de VLAN y asignaciones de interfaz en pfSense.

Dell PowerConnect switches gestionados

La interfaz de administración de conmutadores Dell varía ligeramente entre los modelos, pero el siguiente procedimiento tendrá en cuenta la mayoría de los modelos. La configuración es muy similar en estilo a Cisco IOS.

En primer lugar, crear las VLAN:

```
console # config
console (config) # vlan    base de datos
console (config-vlan) #  vlan 10 nombre dmz ethernet medios
console (config-vlan) #  vlan 20 nombre teléfonos ethernet medios
console (config-vlan) #  salida
```

A continuación, configurar un puerto troncal:

```
console (config) # interfaz ethernet 1/1
console (config-if) # switchport mode trunk
console (config-if) # switchport vlan permitido agregar 1-4094 etiquetados
console (config-if) # salida
```

Por último, añadir puertos a las VLAN:

```
console (config) # interfaz ethernet 1/15
console (config-if) # switchport permitido add vlan 10 sin etiquetar
console (config-if) # salida
```

Capítulo 15. Múltiple WAN Conexiones

Las múltiples WAN (multi-WAN) capacidades de pfSense le permiten utilizar múltiples Internet conexiones para lograr mayor tiempo de actividad y una mayor capacidad de rendimiento. Antes de proceder con un multi-
Configuración WAN, se necesita un interfaz de dos de trabajo de configuración (LAN y WAN). pfSense es capaz de manejar muchas interfaces WAN, con múltiples despliegues utilizando 10-12 WANs en producción. Se debe ampliar aún más alto que eso, aunque no seamos conscientes de las instalaciones que utilizan más de 12 WAN.

A partir de pfSense 2.0, todas las WAN son tratados de forma idéntica en la interfaz gráfica de usuario. Cualquier cosa que usted puede hacer con el principal
WAN también se puede hacer con interfaces OPT WAN, por lo que ya no hay ninguna diferencia significativa entre el primario WAN y WAN adicionales.

Este capítulo comienza cubriendo cosas que usted debe tener en cuenta al implementar cualquier multi-WAN solución, entonces cubre la configuración multi-WAN con pfSense.

La elección de su conectividad a Internet

La opción ideal de la conectividad a Internet dependerá en gran medida de las opciones disponibles en su ubicación, pero hay algunos factores adicionales a tener en cuenta.

Caminos de cables

Hablando desde la experiencia de los que han visto de primera mano los efectos de la búsqueda de cable múltiple retroexcavadoras, así como los ladrones de cobre nefastos, es muy importante asegurarse de que su conexión a opciones para un despliegue multi-WAN utilizan rutas de cableado dispares. En muchos lugares, todos T1 y Conexiones DSL, así como cualesquiera otros que utilizan pares de cobre se realizan en un solo cable sujeto a el mismo corte de cable.

Si usted tiene una conexión que viene adentro sobre par de cobre (T1, DSL, etc), selecciona una conexión secundaria la utilización de un tipo y la ruta diferente de cableado. Las conexiones de cable suelen ser los más ampliamente disponible
opción no sujetos a la misma interrupción como servicios de cobre. Otras opciones incluyen inalámbrica fija, y servicios de fibra que entra en un camino de cable diferente de sus servicios de cobre.

No se puede confiar en dos conexiones del mismo tipo para proporcionar redundancia en la mayoría de los casos. Un ISP corte de luz o el cable se corte comúnmente acabar con todas las conexiones del mismo tipo. Algunos pfSense usuarios hacen uso de múltiples líneas DSL o varios módems de cable, aunque la única redundancia que típicamente ofertas que se aíslan de módem u otro CPE (Customer Premise Equipment) fracaso. Usted debe considerar múltiples conexiones desde el mismo proveedor, ya que sólo una solución de ancho de banda adicional, como la redundancia tal despliegue ofrece es mínima.

Caminos hacia la Internet

Otra consideración a la hora de seleccionar la conexión a Internet es el camino de su conexión a Internet. Para fines de redundancia, múltiples conexiones a Internet del mismo proveedor, especialmente del mismo tipo no se debe confiar en ellas.

Con los proveedores más grandes, dos tipos diferentes de conexiones, tales como un módem DSL y línea T1 se suele atravesar significativamente diferentes redes hasta llegar a las partes centrales de la red. Estos núcleo componentes de la red son generalmente diseñados con alta redundancia y se abordan los problemas rápidamente, ya que tienen efectos generalizados. Por lo tanto este tipo de conectividad se aísla de la mayoría de los problemas de la ISP,
pero ya que comúnmente utilizan el mismo camino por cable, que todavía le deja vulnerable a interrupciones prolongadas a partir de cortes de cables.

Mejor redundancia, más ancho de banda, menos dinero

Durante muchos años, el servicio T1 ha sido la elección para cualquier entorno de alta disponibilidad requisitos. Generalmente los Acuerdos de Nivel de Servicio (SLA) ofrecidos en conexiones T1 son mejores que otros tipos de conectividad, y T1 son generalmente vistos como más fiable. Pero con pfSense de múltiples Capacidades WAN, usted puede tener más ancho de banda y una mejor redundancia por menos dinero en muchos casos.

La mayoría de las organizaciones que requieren conexiones a Internet de alta disponibilidad no quieren depender de DSL, cable u otras conexiones de Internet de banda ancha "menos de clase". Mientras que por lo general son mucho más rápido y más baratos, menor SLA es suficiente para que muchas empresas se quedan con la conectividad T1. En las zonas donde múltiples opciones de banda ancha de menor costo están disponibles, tales como DSL y cable, la combinación de pfSense y dos conexiones de Internet de bajo coste ofrece más ancho de banda y una mejor redundancia a un costo menor. La probabilidad de que dos conexiones de banda ancha diferentes bajando al mismo tiempo es significativamente menor que la probabilidad de un fallo T1 o interrupción de cualquier servicio individual.

Multi-WAN Terminología y conceptos

Esta sección abarca la terminología y los conceptos que usted necesita comprender para poder desplegar multi-WAN con pfSense.

Política de encaminamiento

Política de encaminamiento se refiere a un medio de enrutamiento de tráfico en más de la dirección IP de destino del tráfico,
como se hace con la tabla de enrutamiento en la mayoría de los sistemas operativos y routers. Esto se logra por el uso de una política de algún tipo, por lo general las normas de firewall o una lista de control de acceso. En pfSense, la puerta de enlace
campo disponible al editar o agregar reglas de firewall permite el uso de la política de enrutamiento. La puerta de enlace campo contiene todas las puertas de enlace definidos de Sistema Enrutamiento, además de los grupos de puerta de enlace que tienes
definido.

Política de encaminamiento proporciona un poderoso medio de dirigir el tráfico a la interfaz WAN adecuada o otra puerta de enlace, ya que permite nada que coincida con una regla de firewall puede igualar. Hosts específicos, subredes
protocolos y más se pueden utilizar para dirigir el tráfico.

> Nota
>
> Recuerde que todas las reglas de firewall que incluyen reglas de enrutamiento de la política se procesan de arriba hacia abajo
> orden, y el primer partido gana.

Portal de Grupos

Grupos Gateway son los que proporcionan la conmutación por error y la funcionalidad de balanceo de carga en pfSense. Ellos
se configuran en Sistema Enrutamiento, en la ficha Grupos. En pfSense 1.2.x estos fueron puerta de enlace piscinas manejados de una manera completamente diferente El nuevo mecanismo de agrupación es mucho más potente, lo que permite muchas de conmutación por error y equilibrio de carga de los escenarios más complejos. Cuando se combina con la nueva
Opciones de puerta de enlace (la sección "Configuración de puerta de enlace"), también es mucho más flexible y más fácil de
afinar.

Failover

Conmutación por error se refiere a la capacidad de utilizar una única interfaz WAN, pero una conmutación por error a otra WAN si el
preferido WAN falla.

Equilibrio de carga

El equilibrio de carga se refiere a la capacidad de distribuir la carga entre múltiples interfaces WAN. Tenga en cuenta que balanceo 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 es hacia abajo se retira del grupo de equilibrio de carga.

Monitorear IPs

En la configuración de conmutación por error o el balanceo de carga, cada puerta de enlace está asociada con una IP del monitor (la sección
llamado "IP Monitor"). En una configuración típica pfSense hará ping esta IP, y si deja de responder,
la interfaz se marca como abajo. Opciones en el grupo de la puerta de enlace le permitirá seleccionar diferente fracaso
desencadena además de la pérdida de paquetes. Los otros factores desencadenantes son de alta latencia, una combinación de cualquiera de pérdida de paquetes
o de alta latencia, o el 100% de pérdida de paquetes.

Así que lo que constituye el fracaso?

Como habrás adivinado, es un poco más complejo que "si hace ping a la IP del monitor fallan, la interfaz
se marca como abajo. "Los criterios actuales para un fracaso dependen de las opciones seleccionadas al crear el grupo de puerta de enlace y los ajustes individuales en una pasarela.

Los ajustes para cada puerta de enlace que controlan si se considera arriba y abajo están discutidos en el
sección llamada "Advanced". Los umbrales para la pérdida de paquetes, latencia, el tiempo de inactividad, e incluso la frecuencia
de la puerta de entrada de sondeo son todos configurables individualmente.

Killing Estado / conmutación forzada

Cuando una puerta de enlace ha fallado, por defecto pfSense limpiará todos los estados para las conexiones que utilizan dicha pasarela.
Ese mecanismo obligará a los clientes para volver a conectar, y al hacerlo, utilizará una puerta de entrada que está en línea
en lugar de una puerta de enlace que está abajo. Actualmente sólo funciona de un solo sentido, lo que significa que puede moverse
conexiones fuera de una puerta de entrada en su defecto, pero no puede obligarlos a volver si la puerta de entrada original, vuelva
en línea.
Este es un comportamiento opcional, activado por defecto. Para obtener información sobre cómo cambiar este ajuste, consulte la
sección llamada "Vigilancia Gateway".

Resumen de los requisitos multi-WAN

Antes de cubrir la mayor parte de los detalles de múltiples WAN, aquí está un breve resumen de los requisitos para hacer una configuración multi-WAN totalmente implementado:

• Crear un grupo de pasarela en Sistema Enrutamiento en la ficha Grupos.

• Asegúrese de que ha configurado al menos un servidor DNS para cada puerta de enlace WAN en Sistema General Configuración.

• Utilice el grupo puerta de enlace en las reglas del firewall de la
LAN.

Las secciones restantes de este capítulo cubrirán los puntos más finos de la aplicación de esos artículos a resultar en un sistema multi-WAN capaz.

Multi-WAN Advertencias y consideraciones

Esta sección contiene las advertencias y consideraciones específicas para multi-WAN en pfSense.

Múltiples WANs compartiendo una única puerta de enlace IP

Debido a la forma pf maneja el tráfico multi-WAN, sólo puede dirigirlo por la IP de puerta de enlace de la conexión. Esto está bien en la mayoría de escenarios. Si tiene varias conexiones en la misma red que utilizan la misma puerta de enlace IP, como es común si tiene varios módems de cable, debe utilizar un intermediario Dispositivo NAT de modo pfSense ve cada puerta de enlace WAN como una IP única.

Múltiple PPPoE o PPTP WANs

pfSense 2.0 soporta PPPoE y PPTP en un número ilimitado de redes WAN, las versiones anteriores sólo apoyado PPPoE y PPTP en la WAN primaria, y otras redes WAN OPT tuvieron que utilizar intermedio Dispositivos NAT. Si tiene varias líneas de PPPoE desde el mismo proveedor de Internet y el ISP soporta multi-Link PPPoE, usted puede ser capaz de unir sus líneas en un solo enlace agregado con el ancho de banda total de todas las líneas juntas en una sola WAN como se ve por pfSense. Configuración de escenario que se puede encontrar en la sección llamada "Multi-Link PPPoE (MLPPP)".

Servicios locales y multi-WAN

Hay algunas consideraciones con los servicios locales y multi-WAN, ya que todo el tráfico iniciado desde el cortafuegos en sí misma no se verá afectada por cualquier política de enrutamiento que ha configurado en la interfaz de reglas internas,
sino más bien la siguiente tabla de enrutamiento del sistema. De ahí que las rutas estáticas se requieren en algunas circunstancias
cuando el uso de interfaces OPT WAN, de lo contrario se utilizaría sólo la interfaz WAN. En pfSense 2.0 y más reciente puede utilizar reglas flotantes para aplicar la política de enrutamiento para el tráfico que sale desde el propio servidor de seguridad,
aunque eso también puede requerir alguna configuración NAT extra. Esto sólo se aplica al tráfico que se inicia por el firewall. En el caso del tráfico iniciado en Internet destinado a cualquier interfaz WAN, pfSense utiliza automáticamente PF `responder a` Directiva a todas las reglas de la WAN y OPT WAN, lo que garantiza la tráfico de respuesta se envía de vuelta a la interfaz correcta WAN.

DNS Forwarder

Los servidores DNS utilizados por el reenviador DNS deben tener puertas de enlace definido si utilizan una WAN OPT interfaz, tal como se describe más adelante en este capítulo. No hay otras advertencias al reenviador DNS en multi-Entornos WAN.

IPsec

IPsec es totalmente compatible con multi-WAN. Una ruta estática se agrega automáticamente para el túnel remoto punto final que apunta a la puerta de entrada de la WAN prescrito para garantizar el cortafuegos envía tráfico a cabo la correcta
interfaz cuando se está iniciando la conexión. Para las conexiones móviles, el cliente siempre inicia la conexión y el tráfico de respuesta se encamina correctamente la tabla de estado.

OpenVPN

OpenVPN capacidades multi-WAN se describen en la sección llamada "OpenVPN y Multi-WAN".

Servidor PPTP

El servidor PPTP no es compatible multi-WAN. Sólo se puede utilizar en la interfaz WAN con la puerta de enlace predeterminada del sistema.

CARP y multi-WAN

CARP es multi-WAN capaz, siempre y cuando todos los interfaces WAN utilizar direcciones IP estáticas y usted tiene por lo menos tres
IPs públicas por WAN. Esto se trata en la sección llamada "Multi-WAN con CARP".

IPv6 y Multi-WAN

IPv6 también es capaz de realizar en una capacidad multi-WAN, pero por lo general requieren Prefijo de Red Traducción (TNP) en una o más redes WAN. Esto se explica con más detalle más adelante en la sección titulada "Multi-WAN para IPv6".

Configuración de la interfaz y DNS

Primero tendrá que configurar sus interfaces WAN y servidores DNS.

Configuración de la interfaz

Las interfaces WAN primero se deben configurar. Configuración de la WAN primaria se ha descrito previamente en la sección llamada "Asistente de configuración". Luego de las interfaces OPT WAN, seleccione el tipo deseado de IP configuración, dependiendo de su tipo de conexión a Internet. Para conexiones IP estáticas, rellene el IP abordar y añadir o seleccionar una puerta de enlace.

Configuración del servidor DNS

Usted tendrá que configurar pfSense con los servidores DNS de cada conexión WAN para asegurar que es siempre capaz de resolver DNS. Esto es especialmente importante si su red interna utiliza de pfSense Reenviador DNS para la resolución DNS. Si sólo utiliza un servidor DNS de su ISP, una interrupción de ese WAN conexión dará lugar a una interrupción completa de Internet, independientemente de la configuración de la política de enrutamiento
desde DNS ya no funcionará.

Servidores DNS y rutas estáticas

pfSense utiliza su tabla de rutas para llegar a los servidores DNS configurados. Esto significa, sin estática rutas configuradas, sólo se utilizará la conexión WAN primaria para llegar a los servidores DNS. Gateways

se debe seleccionar para cada servidor DNS se define en el Sistema Configuración general, por lo que pfSense utiliza el
interfaz WAN correcta para llegar a ese servidor DNS. Los servidores DNS que vienen de pasarelas dinámicas son enrutada automáticamente el camino correcto. En esa página, para cada servidor DNS que aparece, seleccione la puerta de entrada correspondiente de la lista desplegable Usar puerta de enlace. Usted debe tener al menos una pasarela de
cada WAN cuando sea posible.

Esto es necesario por dos razones. Uno, más todos los ISP prohíben consultas recursivas desde hosts fuera de su red, por lo tanto usted debe utilizar la interfaz WAN correcta para acceder al servidor DNS de ese ISP. En segundo lugar, Si usted pierde su WAN principal y no tiene una puerta de acceso elegido para uno de sus otros servidores DNS, usted perderá toda la resolución de DNS de la propia capacidad de pfSense como todos los servidores DNS serán inalcanzables
cuando la puerta de enlace predeterminada del sistema es inalcanzable. Si está utilizando pfSense como su servidor DNS, este
se traducirá en un fracaso completo de DNS para su red.

La ampliación a un gran número de interfaces WAN

Hay numerosos usuarios pfSense despliegue 6-12 conexiones de Internet en una sola instalación. Uno usuario pfSense tiene 10 líneas DSL debido a que en su país es significativamente más barato conseguir diez 256 Kb conexiones de lo que es una conexión de 2,5 Mb. Utiliza pfSense para equilibrar la carga de un gran número de máquinas internas de cada 10 conexiones diferentes. Para obtener más información sobre esta escala de implementación, vea
la sección llamada "Multi-WAN on a Stick" sobre "Multi-WAN en un palo", más adelante en este capítulo.

Multi-WAN Casos Especiales

Algunas implementaciones multi-WAN requieren soluciones alternativas debido a las limitaciones en pfSense. Esta sección cubre
los casos y en la forma de acomodarlos.

Conexiones múltiples con el mismo IP Gateway

Debido a la forma pfSense distribuye el tráfico a través de múltiples conexiones de Internet, si usted tiene múltiples Conexiones a Internet que utilizan 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 viable. Nos gustaría dar cabida
esto en futuras versiones, pero es muy difícil debido a la forma en que el software subyacente dirige el tráfico cuando se hace la política de enrutamiento.

Multi-WAN y NAT

Las reglas de NAT por defecto generados por pfSense se traducirán cualquier tráfico que sale de la WAN o un OPT Interfaz WAN a la dirección IP de la interfaz. En una forma predeterminada dos interfaces LAN y WAN de configuración,
pfSense se NAT Todo el tráfico que sale de la interfaz WAN a la dirección IP de la WAN. La adición de OPT Interfaces WAN se extiende de este a Nat cualquier tráfico que sale de una interfaz OPT WAN IP de esa interfaz Dirección. Todo esto se realiza automáticamente a menos que se habilita Advanced Outbound NAT.

Las reglas de enrutamiento de políticas dirigen el tráfico a la interfaz WAN se utiliza, y la salida y 01:01 NAT reglas especifican cómo se traduce el tráfico.

Multi-WAN y Manual NAT Saliente

Si usted requiere NAT de salida manual con multi-WAN, es necesario asegurarse de configurar reglas NAT para todas sus interfaces WAN.

Multi-WAN y Port Forwarding

Cada avance de puerto se aplica a una sola interfaz WAN. Un puerto determinado puede abrirse en múltiples Interfaces WAN mediante el uso de múltiples entradas remitir el puerto, uno por cada interfaz WAN. La forma más fácil

lograr esto es agregar el puerto hacia delante en la primera conexión WAN, a continuación, haga clic en theTo la derecha de que la entrada para agregar otro puerto hacia adelante sobre la base de que uno. Cambie la interfaz a la WAN deseada, y haga clic en Guardar.

Gracias a PF de respuesta a la palabra clave utilizada en las reglas de la WAN, cuando el tráfico llega a través de una WAN específica
interfaz, el tráfico de retorno volverá a la forma en que entró Así que usted puede utilizar activamente puerto remite en todas las interfaces de WAN, al mismo tiempo, independientemente de cualquier configuración de conmutación por error que pueda estar presente.
Esto es especialmente útil para los servidores de correo, como se puede utilizar una dirección en una WAN secundario, como una copia de seguridad
MX, lo que le permite recibir correo incluso cuando la línea principal está suspendido. Este comportamiento es configurable
para obtener información sobre esta configuración, consulte la sección llamada "Disable Reply-To".

Multi-WAN y NAT 01:01

01:01 entradas NAT son específicos de una única interfaz WAN. Los sistemas internos pueden configurarse con un 1:01 Entrada NAT en cada interfaz WAN, o una entrada de 01:01 en una o más interfaces WAN y utilizar el valor por defecto NAT saliente en otros. Cuando se configuran las entradas de 01:01, que siempre tienen prioridad sobre cualquier otra de salida
Configuración de NAT para la interfaz específica en la que se configura la entrada de 01:01.

Equilibrio de carga y conmutación por error

El balanceo de carga funcionalidad en pfSense le permite distribuir el tráfico a través de múltiples WAN conexiones en turnos rotativos. Esto se hace en función de cada conexión.

Si una puerta de enlace que es parte de un grupo de equilibrio de carga falla, la interfaz se marca como hacia abajo y se retira
de todos los grupos hasta que se recupere. De conmutación por error se refiere a la capacidad de utilizar sólo una conexión WAN, pero
cambiar a otra WAN si la conexión preferida falla. Esto es útil para situaciones en las que desee
cierto tráfico, o la totalidad de su tráfico, para utilizar una conexión específica WAN a menos que no está disponible.

Configuración de un grupo de puerta de enlace para el equilibrio de carga o Failover

En el pfSense WebGUI, vaya a Sistema Routing. En la ficha Grupos, haga clic en. Esto traerá
a la pantalla de edición de puerta de enlace de grupos. Las siguientes secciones describen cada campo en esta página.

Nombre del grupo

En el campo Nombre del grupo, rellenar un nombre para el grupo de pasarela. El nombre debe tener menos de 32 caracteres
de longitud, y puede solo contener letras az, números 0-9, y un guión bajo. Este será el nombre que se utiliza para referirse a este grupo de pasarela en el campo Gateway en las reglas del cortafuegos. Este campo es obligatorio.

Puerta de enlace de prioridad

En la sección Prioridad de puerta de enlace se puede elegir la prioridad de las pasarelas dentro del grupo. Dentro grupos de puerta de enlace, gateways están dispuestos en las gradas. Tiers están numerados del 1 al 5, y los números más bajos
se utilizó por primera vez. Por ejemplo, las puertas de enlace en el Nivel 1 se utilizan antes de las puertas de enlace en el Nivel 2, y así sucesivamente.

Equilibrio de carga

Cualquier par de puertas de enlace en el mismo nivel se encuentran la carga equilibrada. Por ejemplo, si Puerta de enlace A, Gateway B,
y Puerta de enlace C son todos de nivel 1, las conexiones se equilibraría entre ellos. Gateways que son de carga equilibrada conmutará por error automáticamente entre sí. Cuando una puerta de enlace no se elimina de la grupo, por lo que en este caso si cualquiera de A, B, o C descendieron, el firewall podría equilibrar la carga entre las puertas de enlace en línea restantes.

Balancing ponderado

Si dos redes WAN deben equilibrarse de manera ponderada debido a las diferentes cantidades de ancho de banda entre ellos, que se pueden acomodar ajustando el parámetro Peso en la puerta de enlace como se describe en la sección llamada "Peso".

Failover

Se prefieren los Gateways en un nivel más bajo numerado, y si son hacia abajo y luego gateways de un mayor se utilizan niveles numerados. Por ejemplo, si Puerta de enlace A está en el Nivel 1, Puerta de enlace B está en el nivel 2, y
Puerta de enlace C está en el Nivel 3, entonces Puerta de enlace A se utilizó por primera vez. Si Puerta de enlace A se cae, entonces
Puerta de enlace B sería utilizado. Si tanto Puerta de enlace A y Puerta de enlace B han bajado, entonces Puerta de enlace C
se convirtió.

Escenarios complejo / combinado

Al ampliar los conceptos anteriores para el equilibrio de carga y conmutación por error, se puede llegar a muchos escenarios complicados que combinan tanto el balanceo de carga y conmutación por error. Por ejemplo, si usted tiene Puerta de enlace A en el Nivel 1, y luego tener Puerta de enlace B y Puerta de enlace C en el Nivel 2, a continuación, Puerta de enlace D
en el Nivel 3, se llega a la siguiente comportamiento: Puerta de enlace A se prefiere por su propia cuenta. Si Entrada Laestá abajo, entonces el tráfico se carga equilibrada entre Puerta de enlace B y Pasarela C. Si una de las Puerta de enlace B o Puerta de enlace C bajar, todavía se utilizaría el portal en línea que queda en ese nivel.
Si Puerta de enlace A, Gateway B, y Puerta de enlace C están todos abajo, el tráfico fallaría a Pasarela D.

Cualquier otra combinación de lo anterior se puede utilizar, siempre y cuando se puede disponer dentro del límite de los 5 niveles.

Nivel de disparo

Los controles de nivel de disparo desplegables cuando una puerta se retira de su uso en un grupo. Hay cuatro modos diferentes que se pueden utilizar.

Abajo Miembro

Cuando se utiliza de Down miembros, la puerta de entrada sólo se puede quitar de su uso cuando la puerta de entrada es abajo (100% packet loss). Esto sería coger el peor tipo de fallos, cuando la puerta de entrada es completamente no responde, pero puede pasar por alto las cuestiones más sutiles con el circuito que puede quedar inservible mucho antes la puerta de entrada llega a la pérdida del 100%.

La pérdida de paquetes

El disparador de la pérdida de paquetes podría considerar sólo una puerta de entrada hacia abajo si la pérdida del paquete supera el umbral
definido en el gateway (Vea la sección llamada "pérdida de paquetes umbrales"). Latencia no habría considerado.

Alta latencia

El disparador de alta latencia sería considerar sólo una puerta de entrada hacia abajo si la latencia supera el umbral definido en el gateway (Vea la sección llamada "Latencia Umbrales"). La pérdida de paquetes no sería considerado.

La pérdida de paquetes o de alta latencia

Si la pérdida de paquetes o de alta latencia de disparo está en uso, a continuación, una puerta de entrada sería removido de su uso si
o bien se superaron las de latencia o pérdida de umbrales. Esta es la opción más útil para la mayoría de la gente, y es la opción más común de usar. A menos que tenga una necesidad específica de lo contrario, utilice esta opción.

Descripción

Puede introducir una descripción aquí para su referencia. Este campo se muestra en la lista de puerta de enlace Grupos y pantalla de estado, y no afecta a la funcionalidad del grupo. Es opcional.

Problemas con el equilibrio de carga

Algunos sitios web de información de sesión store incluyendo su dirección IP, y si es una conexión posterior a ese sitio se encamina a una interfaz WAN diferente utilizando una IP pública diferente, la página web no lo hará funcione correctamente. Esto es bastante raro y sólo incluye algunos bancos en mi experiencia. La sugerido medio de trabajo en torno a esto es crear un grupo de conmutación por error y dirigir el tráfico destinado a estos sitios el grupo de conmutación por error en lugar de un grupo de equilibrio de carga.

La función de las conexiones pegajosa de pf se supone para resolver este problema, pero ha tenido problemas en el pasado.
Es seguro de usar, y debe aliviar este, pero hay también una desventaja de usar la opción pegajoso. ¿Cuándo utilizando conexiones adhesivas, una asociación se lleva a cabo entre la IP del cliente y una puerta de entrada dada, no es con sede fuera de la destinación. Así que si la opción de conexiones pegajoso está activado, cualquier cliente lo haría no equilibrar la carga de conexiones entre sus múltiples WAN, pero se asocia con el que sea pasarela pasó a utilizar para su primera conexión.

Funcionalidad Verificación

Una vez que su configuración multi-WAN se ha configurado, tendrá que verificar su funcionalidad. La Las secciones siguientes describen cómo va a probar cada parte de su configuración multi-WAN.

Pruebas de conmutación por error

Si ha configurado la conmutación por error, tendrá que poner a prueba después de completar la configuración para asegurarse de
funciona como usted desea. No cometa el error de esperar hasta que una de sus conexiones a Internet deja de probar primero su configuración de conmutación por error.

Vaya a Estado Gateways y asegúrese de que todas las puertas de enlace WAN son espectáculo como "en línea" en Estado,
así como en la ficha Puerta de enlace de grupos. Si no lo hacen, compruebe que está utilizando una dirección IP del monitor adecuado como
discutido en la sección llamada "IP Monitor".

Creación de un Fallo de WAN

Hay un número de maneras en que puede simular una falla de la WAN, que se diferencian en función del tipo de Conexión a Internet se utiliza. Para cualquier tipo, primero pruebe a desenchufar el objetivo de interfaz WAN Ethernet cable del firewall.

Para las conexiones de cable y DSL, usted también tendrá que tratar de apagar el módem, y justo desenchufar el cable coaxial o línea telefónica del módem. Para T1 y otros tipos de conexiones con un enrutador fuera de pfSense, intente desconectar la conexión a Internet desde el router, y también apagar el router en sí.

Todos los escenarios de prueba descritos probablemente va a terminar con el mismo resultado. Sin embargo, hay algunos circunstancias en las que probar todas estas cosas individualmente encontrará una culpa que no tendrían de otra manera notado hasta que un fallo real. Uno de los más comunes es el uso de un monitor de IP asignado a su ADSL o módem de cable (en algunas circunstancias puede que no sea consciente de donde reside su puerta de enlace IP). Por lo tanto cuando se desconecta la línea de cable coaxial o de teléfono, simulando una falla proveedor en lugar de una conexión Ethernet o error de módem, el ping monitor todavía tiene éxito, ya que se hacer ping al módem. De lo que le dijiste pfSense para supervisar, la conexión está todavía, por lo que no se producirá un error aun cuando la conexión es en realidad hacia abajo. Hay otros tipos de fallo que pueden sólo de manera similar detectarse mediante pruebas de todo el individuo posibilidades de fracaso. En caso de que tenga que cambiar a un IP monitor diferente, se puede editar en la entrada de puerta de enlace como cubierto en la sección llamada "IP Monitor".

Verificación de estado de la interfaz

Después de crear una falla de la WAN, actualice el Estatuto Pantalla Gateways para comprobar el estado actual.

Load Balancing Verificación Funcionalidad

En esta sección se describe cómo verificar la funcionalidad de la configuración de equilibrio de carga.

Verificación de Equilibrio de carga de 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 el mismo propósito. Búsqueda de "¿cuál es mi dirección IP" y encontrará numerosos sitios web que le mostrará lo que 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 dicen a su dirección IP.

Sitios HTTP 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

Sitio HTTPS para encontrar su dirección IP pública

- https://portal.pfsense.org/ip.php

Si se carga uno de estos sitios, y actualice su navegador varias veces, debería ver a su IP abordar el cambio si la carga de configuración de equilibrio es correcto. Tenga en cuenta si usted tiene cualquier otro tipo de tráfico en la red, es probable que no podrás ver su cambio de dirección IP en cada actualización de la página. Actualizar la página 20 o 30 veces y usted debe ver el cambio de IP, al menos, un par de veces. Si la IP no cambia nunca, probar varios sitios diferentes, y asegúrese de que su navegador realmente está solicitando la página de nuevo, y no devolver algo de su caché o usando una conexión persistente con el servidor. Eliminar manualmente el caché y tratar múltiples navegadores web son cosas buenas para intentar antes de solucionar el cargar configuración del equilibrador más. Uso rizo, como se describe en la sección llamada "carga de Verificación equilibrio "es una mejor alternativa, ya que garantiza la caché y las conexiones persistentes no tendrá ningún impacto en los resultados.

Equilibrio de carga de pruebas con traceroute

La traceroute utilidad (o tracert en Windows) le permite ver la ruta de la red llevado a un determinado destino. Vea la sección "Uso de traceroute" para obtener más información sobre el uso de traceroute.

Cómo utilizar Tráfico Gráficos

Los verdaderos gráficos de tráfico de tiempo, en Estado Tráfico Graph, son útiles para mostrar el tiempo real throughput en sus interfaces WAN. Sólo puede mostrar un gráfico a la vez por la ventana del navegador, pero usted puede abrir ventanas o pestañas adicionales en el navegador y mostrar todas sus interfaces WAN simultáneamente. La característica Dashboard en pfSense 2.0 y posteriores (también disponible como un paquete beta en 1.2) permite la visualización simultánea de múltiples gráficos de tráfico en una sola página.

Los gráficos de tráfico RRD En Estado RRD gráficos son útiles para más de largo plazo e histórico evaluación de su utilización individuo WAN.

Nota

Su ancho de banda puede no ser exactamente igual distribuida, ya que las conexiones son simplemente dirigido de forma round robin sin tener en cuenta el uso de ancho de banda.

Política de Enrutamiento, equilibrio de carga y conmutación por error Estrategias

Usted tendrá que determinar la configuración multi-WAN que mejor se adapte a las necesidades de su entorno. Esta sección proporciona una guía sobre los objetivos comunes, y cómo se logra con pfSense.

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 WAN circuitos, usted no puede conseguir 10 Mbps de rendimiento con una sola conexión del cliente. Cada conexión individual debe estar atado a una sola específica WAN. Esto es cierto para cualquier solución multi-WAN, no se pueden agregar el ancho de banda de dos conexiones a Internet en un solo "pipe" grande sin la participación de la ISP. Con el equilibrio de carga, ya que las conexiones individuales se equilibran en una forma de round robin, que puede alcanzar 10 Mbps de rendimiento utilizando dos circuitos de 5 Mbps, pero no con una única conexión. Las aplicaciones que utilizan múltiples conexiones, como muchos aceleradores de descarga, podrán alcanzar la capacidad de caudal combinado de los dos o más conexiones. La excepción a esto es Multi-Link PPPoE (MLPPP), que puede alcanzar ancho de banda agregado total de todos los circuitos en un paquete, pero requiere el apoyo especial de la ISP. Para más información sobre MLPPP, consulte la sección llamada "Multi-Link PPPoE (MLPPP) "

En redes con numerosas máquinas internas con el acceso a Internet, balanceo de carga le permitirá para alcanzar cerca del rendimiento agregado equilibrando las muchas conexiones internas a cabo todo el Interfaces WAN.

La segregación de los servicios prioritarios

En algunas situaciones, es posible que tenga una conexión a Internet fiable y de alta calidad que ofrece un bajo ancho de banda, o los altos costos de las transferencias excesivas, y otra conexión que es rápido pero de menor calidad (más alto latencia, jitter más o menos fiable). En estas situaciones, se puede segregar a los servicios entre los dos Conexiones a Internet por su prioridad. Servicios de alta prioridad pueden incluir VoIP, el tráfico destinado a un red específica, como un proveedor de aplicaciones externalizadas, algunos protocolos específicos utilizados por los críticos

aplicaciones, entre otras opciones. Tráfico de baja prioridad comúnmente incluye todo el tráfico permitido que no coincide con la lista de tráfico de alta prioridad. Usted puede configurar las reglas de enrutamiento de la política en una forma tal que
para dirigir el tráfico de alta prioridad a la conexión a Internet de alta calidad, y el tráfico de menor prioridad a cabo la conexión de menor calidad.

Otro ejemplo de un escenario similar es conseguir una conexión a Internet dedicado para calidad crítica servicios tales como VoIP, y sólo con esa conexión para esos servicios.

Sólo Failover

Hay algunos escenarios en los que es posible que desee utilizar sólo la conmutación por error. Algunos usuarios tienen una Pfsense
conexión secundaria de copia de seguridad de Internet con un límite de ancho de banda bajo, como un módem 3G, y sólo quería
utilizar esa conexión si su conexión principal falla, los grupos de Gateway configurados para la conmutación por error permiten
a lograr este objetivo.

Otro uso para la conmutación por error es cuando se quiere asegurar un determinado protocolo o destino utiliza siempre sólo una WAN a menos que se pone.

Desigual Equilibrio Costo de carga

En pfSense 2.0 se puede lograr el equilibrio de carga de costos desiguales estableciendo pesos apropiados en la puertas de enlace como se comenta en la sección denominada "Peso". Al establecer un peso en una puerta de enlace, que se utilizará
más a menudo en un grupo de puerta de enlace. Los pesos se pueden ajustar de 1 a 5, lo que permite

Tabla 15.1. Balanceo de carga coste desigual

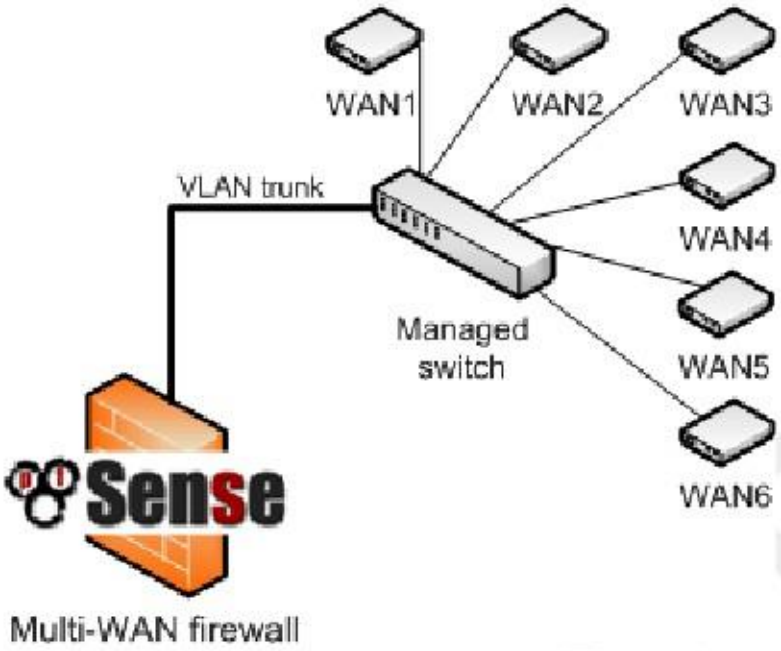
Peso WAN_GW	Peso WAN2_GW	Carga WAN	Carga WAN2
3	2	60%	40%
2	1	67%	33%
3	1	75%	25%
4	1	80%	20%
5	1	83%	17%

Tenga en cuenta que esta distribución está estrictamente equilibrar el número de conexiones, que no tiene interfaz throughput en cuenta. Esto significa que su uso de ancho de banda no será necesario ser distribuida por igual, aunque en la mayoría de entornos que funciona para ser distribuidos más o menos como se ha configurado en el tiempo. Esto también
significa que si una interfaz se carga a su capacidad con una sola conexión de alto rendimiento, adicional conexiones se redirige a la interfaz. Lo ideal sería que usted quiere a distribuir conexiones
basado en los pesos de interfaz y el rendimiento actual de la interfaz. Estamos investigando opciones
para este escenario ideal para las futuras versiones de pfSense, aunque los medios existentes de equilibrio de carga de obras
muy bien para la mayoría de todos los entornos.

Multi-WAN en un palo

En el mundo router, Cisco y otros se refieren a un router VLAN como un "router en un palo", ya que puede ser un enrutador que funciona con sólo una conexión de red física. Ampliando esto, podemos tener multi-WAN en un palo utilizando VLANs y un switch gestionable capaz de trunking 802.1Q. La mayor parte de los despliegues de ejecución de más de 5 WAN utilizan esta metodología para limitar el número de física interfaces necesarias en el firewall. En una implementación de este tipo, las WANs todos residen en una interfaz física en el servidor de seguridad, con la red interna (s) en las interfaces físicas adicionales. Figura 15.1, "Multi-WAN en un palo ", ilustra este tipo de despliegue.

Figura 15.1. Multi-WAN en un palo



Multi-WAN para servicios que se ejecutan en el Firewall

En pfSense 2.0 y superior, ahora es posible dirigir el tráfico desde el mismo servidor de seguridad en la puerta de enlace grupos usando reglas flotantes, que permiten los servicios locales se aprovechen de conmutación por error.

Multi-WAN para IPv6

Con pfSense 2.1 se puede hacer de múltiples WAN con IPv6 siempre que disponga de múltiples ISPs o túneles configuración y funcionamiento. Consulte la sección "Conexión con un Service Broker Túnel" si necesita ayudar a la creación de un túnel.

Portal de Grupos de Trabajo de la misma para IPv6 como lo hacen para IPv4, pero no se puede mezclar familias de direcciones
dentro de un grupo. Un grupo debe contener cualquiera de las puertas de enlace IPv4 únicas, o sólo puertas de enlace IPv6.
A lo largo de esta sección "Segundo WAN" se refiere a la segunda o adicional interfaz con IPv6 conectividad. Podría ser su interfaz real si tiene conectividad nativa, o un túnel si usted es uso de un corredor del túnel.

Advertencias

Tradicionalmente con IPv6 no hace NAT, ya que todo se encamina. Eso está muy bien para la conectividad y para las empresas o lugares que pueden permitirse Independientes del Proveedor (PI) de espacio de direcciones y un peering BGP.
No funciona tan bien en la práctica para los usuarios domésticos.

Prefijo de red Traducción (NPT) le permitirá utilizar una subred para la LAN y tienen plena conectividad con esa subred a través de la WAN que en realidad rutas que subred y también lo han traducido en las redes WAN adicionales por lo que parece que se origina allí. Si bien no es cierto para la conectividad LAN subred a través de ese camino, es mejor que no tener ninguna conexión en absoluto si su WAN principal es hacia abajo.

Esto puede no funcionar en absoluto para este tipo de IPv6 completamente dinámicos donde la subred no es estática. (DHCP-
PD, etc)

Requerimientos

Para la configuración de múltiples WAN para IPv6 que necesita:
Configuración de la conexión • Dos redes WAN y IPv6 en ellos.

• Gateways añadido a Sistema> Routing para ambos, y confirmó la conectividad en ambos.

• LAN utilizando una estática enrutado / 64 o similar.

Disposición

La configuración para IPv6 multi-WAN está muy cerca de la configuración de IPv4. La principal diferente es TNP lugar de NAT.

En primer lugar, en Sistema Enrutamiento en la ficha Puerta de enlace grupos, agregue Grupos puerta de enlace para las pasarelas V6,
con la configuración de capas como se desee. Esto funciona igual que IPv4.

A continuación, navegue a System General y asegurarse de que tiene un conjunto de servidores DNS IPv6 para cada IPv6 WAN.
Una vez más, al igual que IPv4

Ahora agregue una entrada NPT bajo Firewall NAT en la ficha del TNP, con la siguiente configuración:

• Interfaz: WAN Secondary (O túnel si el uso de un agente.)

• IPv6 Interna Prefijo: Su subred LAN IPv6.

• Destino IPv6 Prefijo: Su segunda WAN enrutado IPv6 subred. Tenga en cuenta que esto es no el / 64 de la interfaz WAN en sí - es el / 64 encaminada a usted en eso WAN por el río arriba.

Lo que esto hace es similar a NAT 01:01 para IPv4. Dado que el tráfico sale de la segunda WAN, si viene desde la subred LAN, será traducido al equivalente IP en la otra subred. Por ejemplo, si tiene
2001: xxx: yyy :: / 64 en su LAN, y 2001: aaa: bbb :: / 64 en su segunda WAN, a continuación,
2001: xxx: yyy :: 5 aparecería como 2001: aaa: bbb :: 5 si el tráfico se va por la segunda WAN.

Al igual que con IPv4 es necesario utilizar los Grupos de puerta de enlace en las reglas del firewall de la LAN. Edite sus normas de LAN
para el tráfico IPv6 y hacer que usan el grupo de pasarela, asegurándose de tener reglas para conectarse directamente subredes / VPNs sin una puerta de enlace establecido por lo que no son la política encaminada.

Tácticas Alternos

Algunos pueden preferir utilizar un "privado" de subred IPv6 en su LAN desde el FC00 :: / 7 el espacio, y la configuración del TNP
para ambas redes WAN.

Multi-Link PPPoE (MLPPP)

Multi-Link PPPoE (MLPPP) es una opción única WAN que pueden realmente unir togeher múltiple PPPoE líneas del mismo ISP. Esto significa que puede obtener el verdadero ancho de banda agregado de todos los circuitos en el bundle. Por ejemplo, si tiene tres 5 Mbit / s de líneas DSL en un paquete, usted podría recibir 15 Mbit / s de una única conexión en la línea.

Requerimientos

El mayor obstáculo para MLPPP es que el ISP debe soportar en sus circuitos. Pocos ISPs están dispuestos para apoyar MLPPP, así que si usted puede encontrar uno que lo haga, que valdría la pena tomar ventaja de ese hecho. Además, cada línea debe estar en una interfaz independiente conectado a pfSense.

Disposición

Configuración para MLPPP es en realidad bastante simple. Configuración de una WAN para una sola línea con sus credenciales. Una vez
es decir la configuración, navegue hasta Interfaces Asigne en la ficha PPP. A partir de ahí clickto editar la entrada para su PPPoE WAN, y simplemente Ctrl-clic para seleccionar las otras interfaces físicas que pertenecen a la mismo paquete MLPPP. Guardar, y aplicar. pfSense entonces intentará unir las líneas utilizando MLPPP.

Advertencias

Una desventaja de usar MLPPP es que ya no se puede obtener estadísticas o estado individuales para un solo line. Hay que leer a través del registro de PPP a fin de determinar si uno de los enlaces es hacia arriba o hacia abajo, como
aún no existe una forma de consultar las líneas de forma individual. En algunos casos es obvio si una línea está abajo, como
usted puede notar que el módem está fuera de sincronización o de que su ancho de banda máximo alcanzable se reduce, pero hace que la solución de problemas mucho más difícil.

Solución de problemas

En esta sección se describen algunos de los problemas más comunes con multi-WAN y cómo solucionar ellos.

Verifique su configuración de la regla

El error más común cuando se configura multi-WAN es la configuración de reglas de firewall inadecuado. Recuerde que los primeros triunfos de la regla coincidente - cualesquiera otras normas se ignoran. Si se agrega una política de enrutamiento
gobernar por debajo de la norma de LAN por defecto, no hay tráfico volverá a coincidir con esa regla porque va a coincidir con el valor por defecto
Descarta LAN primero.
Si su pedido y la configuración de la regla parece correcta, puede ser útil habilitar el registro en las reglas. Consulte la sección de solución de problemas en el capítulo de firewall para obtener más información. Velar por la adecuada
regla de política de enrutamiento es pasar el tráfico.

El balanceo de carga no funciona

En primer lugar, asegúrese de la regla de firewall está emparejado dirige el tráfico al grupo gateway equilibrio de carga. Si el
normas son correctas, y el tráfico se pongan en venta una regla con el grupo gateway equilibrador de carga especificado, compruebe que todas las conexiones como demostración en línea en Estado Gateways. Conexiones marcados como No será utilizada fuera de línea. Por último, esto puede ser un problema no con la configuración, pero con las pruebas metodología. En lugar de probar con un navegador web, pruebe las pruebas con rizarse como se describe en la sección denominado "Verificación de equilibrio de carga."

Conmutación por error no funciona

Si se producen problemas cuando falla una conexión a Internet, por lo general es porque la IP del monitor sigue siendo respondiendo a lo que el servidor de seguridad cree que la conexión está disponible. Comprobar estado Gateways de verificar.
Puede que esté utilizando la dirección IP del módem como un IP monitor, que por lo general sigue siendo accesible incluso si la conexión a Internet está caída.

Capítulo 16. Redes Privadas Virtuales

VPN proporcionan un medio de tráfico de túnel a través de una conexión cifrada, impidiendo que sea visto o modificados en tránsito. pfSense ofrece tres opciones de VPN con IPSec, OpenVPN y PPTP. 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 de VPN en detalle.

Proporcionamos información sobre PPTP sobre todo por razones de legado; PPTP no debe ser utilizado bajo cualquier circunstancias, porque ya no es segura. El protocolo ha sido completamente comprometida, por lo que es así que el tráfico PPTP se puede descifrar en cada caso. Más detalles sobre esto se puede encontrar en el capítulo 18, PPTP VPN.

Despliegues comunes

Hay cuatro usos comunes de las capacidades de VPN de pfSense, cada uno cubierto en esta sección.

Sitio para la conectividad de sitio

Sitio para la conectividad de sitio se utiliza principalmente para conectar redes en varias ubicaciones físicas, donde un dedicado, siempre-en la conexión entre los lugares se requiere. Este se utiliza con frecuencia para conectar sucursales a la oficina principal, conectar las redes de socios de negocios, o conectar su red a otra ubicación tal como un entorno de co-localización. Antes de la proliferación de la tecnología VPN, circuitos privados WAN eran la única solución para conectar múltiples ubicaciones. Estas tecnologías incluyen circuitos punto a punto dedicados, tecnologías de conmutación de paquetes, tales como frame relay y ATM, y más recientemente, MPLS (Multiprotocol Label Switching) y fibra y cobre basan metropolitana Los servicios de Ethernet. Si bien este tipo de conectividad WAN privada ofrecen, baja latencia confiable conexiones, sino que también son muy costosos con cargos mensuales recurrentes. La tecnología VPN ha crecido en popularidad, ya que proporciona el mismo sitio seguro para conectividad sitio usando las conexiones de Internet que son generalmente mucho menos costoso.

Limitaciones de la conectividad VPN

En algunas redes, sólo un circuito WAN privado puede cumplir los requisitos de ancho de banda o latencia. La latencia es generalmente el factor más importante. Un punto a otro circuito T1 ha de extremo a extremo de latencia de alrededor de 3 a 5 ms, mientras que la latencia para el primer salto en la red de su proveedor de Internet será generalmente al menos esa cantidad si no más alto. Servicios de Metro Ethernet tienen un extremo a otro de latencia de alrededor de 1-3 ms, por lo general menos de la latencia a la primer salto de la red de su proveedor de Internet. Eso hará variar algunas basadas en 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. VPNs generalmente ver latencia de alrededor de 30 a 60 ms dependiendo de las conexiones a Internet en el uso y la distribución geográfica distancia entre los lugares. Usted puede minimizar la latencia y maximizar el rendimiento de VPN mediante el mismo proveedor para todas sus ubicaciones VPN, pero esto no siempre es factible.

Ciertos protocolos funcionan muy mal con la latencia inherente a las conexiones a través de Internet. Compartir archivos Microsoft (SMB) es un ejemplo común. En sub-10 ms de latencia, se desempeña bien. Al 30 ms o superior, que es lento, y en más de 50 ms es dolorosamente lento, causando bloqueos frecuentes cuando navegar por las carpetas, guardar archivos, etc Conseguir un listado de directorio simple requiere numerosos de ida y vuelta conexiones entre el cliente y el servidor, lo que agrava significativamente el aumento de retardo del conexión. En Windows Vista y Server 2008, Microsoft introdujo SMB 2.0, que incluye nuevas capacidades para abordar la cuestión describen aquí. SMB 2.0 permite el envío de múltiples acciones en una única solicitud, así como la capacidad de las solicitudes de tuberías, es decir, el cliente puede enviar adicional pide sin esperar a la respuesta de las solicitudes anteriores. Si la red utiliza exclusivamente Vista y Server 2008 o más nuevos sistemas operativos esto no será un problema, pero dada la rareza de tales ambientes, lo cual suele ser una consideración.

Dos ejemplos más de los protocolos sensibles a la latencia son Microsoft Remote Desktop Protocol (RDP) y Citrix ICA. Hay una diferencia de rendimiento y capacidad de respuesta clara con estos protocolos

entre sub-20 ms tiempos de respuesta se encuentran típicamente en una WAN privada, y la respuesta de 50 a 60 ms + veces comunes a las conexiones VPN. Si los usuarios remotos trabajan en escritorios publicados mediante cliente ligero dispositivos, habrá una diferencia de rendimiento notable entre una WAN privada y VPN. Ya sea que diferencia de rendimiento es suficiente para justificar el gasto de una WAN privada significativa variará de un entorno a otro. He trabajado en entornos de cliente ligero que aceptaron el desempeño golpear, y en otros en los que se consideró inaceptable.

Es posible que haya otras aplicaciones de red en su entorno que son sensibles a la latencia, donde el disminución del rendimiento de una VPN es inaceptable. O usted puede tener todas sus ubicaciones en un plazo relativamente
pequeña área geográfica utilizando el mismo proveedor de Internet, donde el rendimiento de la VPN rivaliza con el de privado
Conexiones WAN. El rendimiento es una consideración importante en la planificación de una solución VPN.

El acceso remoto

VPN de acceso remoto permiten a los usuarios conectarse de forma segura a su red desde cualquier ubicación en la que una conexión a Internet disponible. Esto se utiliza con mayor frecuencia para los trabajadores móviles (a menudo denominado
como "Road Warriors") cuyo trabajo requiere viajes frecuentes y poco tiempo en la oficina, y para dar los empleados la posibilidad de trabajar desde casa. También puede permitir a los contratistas o proveedores de acceso temporal a
su red. Con la proliferación de los teléfonos inteligentes, también vemos un buen número de personas que desean una VPN
para acceder de forma segura los servicios internos de sus teléfonos utilizando una VPN de acceso remoto.

Protección para las redes inalámbricas

Una VPN puede proporcionar una capa adicional de protección para sus redes inalámbricas. Esta protección es de dos retirarse, ya que proporciona una capa adicional de cifrado para el tráfico que atraviesa su red inalámbrica, y se puede implementar de tal manera que requiere autenticación adicional antes de acceso a la red se permite recursos. Esto se desplegó casi lo mismo que las VPN de acceso remoto. Esto se trata en la sección llamada "protección adicional para su red inalámbrica".

Relé Secure

VPN de acceso remoto pueden ser configurados de tal manera que pasa todo el tráfico desde el sistema cliente a través de la
VPN. Esto es bueno haber al utilizar redes no confiables, tales como puntos de acceso inalámbricos, ya que le permite empujar
todo su tráfico de Internet a través de la VPN, y salir a Internet desde el servidor VPN. Esto lo protege de una serie de ataques que la gente podría estar tratando de redes no confiables, aunque tiene un impacto en el rendimiento, ya que añade el lúpulo y la latencia adicional a todas sus conexiones. Ese impacto suele ser mínima con conectividad de alta velocidad cuando se encuentre relativamente cerca geográficamente.

La elección de una solución de VPN para su medio ambiente

Cada solución VPN tiene sus pros y sus contras. Esta sección cubrirá las principales consideraciones en elegir una solución de VPN, proporcionando la información que necesita para tomar una decisión para su medio ambiente.

Interoperabilidad

Si usted necesita una solución para interoperar con un servidor de seguridad o enrutador producto de otro proveedor, IPSec
suele ser la mejor opción, ya que se incluye con cada dispositivo de VPN-capaz. También le impide estar encerrado en cualquier servidor de seguridad en particular o solución VPN. Para el sitio interoperable para la conectividad de sedes,
IPsec es generalmente la única opción. OpenVPN es interoperable con otros pocos envasados firewall / VPN soluciones, pero no muchos. Interoperabilidad en este sentido no es aplicable con PPTP ya que no se puede utilizar para el sitio de las conexiones del sitio.

Consideraciones sobre la autentificación

En pfSense 2.x, todos los tipos de VPN pueden admitir la autenticación de usuario. IPsec y OpenVPN también puede trabajar con claves o certificados compartidos. OpenVPN es un poco más flexible en este sentido, ya que puede trabajar sólo con certificados, claves sólo compartidos, sólo la autenticación de usuario, o una combinación de éstos. Usando OpenVPN con SSL, TLS habilitado, y autenticación de usuario es el método más seguro. Certificados OpenVPN también pueden ser protegido por contraseña, en cuyo caso un certificado comprometido solos no es adecuado para la conexión a la VPN si está configurado para utilizar certificados solamente. La falta de adicional autenticación puede ser un riesgo de seguridad en la que un sistema de pérdida, robo, o comprometida que contiene una clave
o certificado significa el que tiene acceso al dispositivo puede conectarse a la VPN hasta que la pérdida es descubierto y el certificado revocado.

Sin embargo, mientras que no es lo ideal, la falta de autenticación de nombre de usuario y contraseña en una VPN no es tan grande
un riesgo que pueda parecer. Un sistema comprometido puede fácilmente tener un capturador de teclado instalado para capturar la
nombre de usuario y contraseña y fácilmente derrotar a esa protección. En el caso de pérdida o robo
sistemas que contienen claves, si el disco duro no está cifrado, las llaves se pueden utilizar para conectarse. Sin embargo añadiendo autenticación de contraseña no es de gran ayuda allí tampoco, ya que suele ser el mismo nombre de usuario y contraseña se utilizará para iniciar sesión en el equipo, y la mayoría de las contraseñas son manipulable en cuestión de minutos utilizando
hardware moderno cuando se tiene acceso a una unidad no cifrada. La seguridad de contraseña es también con frecuencia comprometido por los usuarios con notas en su computadora portátil o en su maletín para portátil con escrito su contraseña
hacia abajo. Como con cualquier implementación de seguridad, las más capas tenga, mejor, pero siempre es una buena idea para mantener estas capas en perspectiva.

Facilidad de configuración

Ninguna de las opciones de VPN disponibles son extremadamente difíciles de configurar, pero hay diferencias entre las opciones. PPTP es muy sencillo de configurar y es el más rápido y más fácil para trabajar,
pero tiene considerables desventajas en otras áreas, especialmente la seguridad. IPsec tiene numerosos configuración opciones y puede ser difícil para los no iniciados. OpenVPN requiere el uso de certificados para el control remoto acceso en la mayoría de los entornos, que viene con su propia curva de aprendizaje y puede ser un poco difícil para gestionamos, pero hacemos todo lo posible para simplificar el proceso en nuestro GUI ahora que los certificados se gestionan
el firewall y los paquetes de exportación del cliente facilita el proceso de obtención de los clientes y en funcionamiento. IPsec
y OpenVPN son opciones preferibles en muchos escenarios para otras razones que se discuten en este capítulo. Cuando se trata de IPsec, facilidad de configuración no es uno de sus puntos fuertes. En versiones anteriores de pfSense OpenVPN era difícil de configurar, así, pero en pfSense 2.x OpenVPN es bastante sencillo de configurar
y utilizar.

Multi-WAN capaz

Si desea que los usuarios tienen la capacidad de conectarse a múltiples conexiones WAN, PPTP no es una opción debido a las funciones de forma de GRE en combinación con la forma en funciones multi-WAN de pfSense. Tanto IPsec y OpenVPN se pueden utilizar con múltiples WAN.

Disponibilidad del cliente

Para las VPN de acceso remoto, la disponibilidad de software de cliente es una consideración primordial. PPTP es el único
opción con soporte de cliente integrado en la mayoría de los sistemas operativos, pero las tres opciones son multiplataforma
compatibles. El software cliente es un programa que se encarga de la conexión a la VPN y gastos de cualquier otra tareas relacionadas como la autenticación, cifrado, enrutamiento, y así sucesivamente.

IPsec

Clientes IPsec están disponibles para Windows, Mac OS X, BSD y Linux aunque no se incluyen en
el sistema operativo a excepción de algunas distribuciones de Linux y BSD. Una buena opción gratuita para Windows es la musaraña
Cliente Soft [http://www.shrew.net/]. Mac OS X incluye soporte IPsec, pero amigable interfaz de usuario no para su uso. Hay opciones gratuitas y comerciales disponibles con una interfaz gráfica de usuario fácil de usar.

El cliente de Cisco IPsec incluido con los dispositivos iOS es totalmente compatible con pfSense IPsec usando xauth y configuración para el cliente se trata en la sección llamada "iOS móvil IPsec".

Muchos teléfonos Android también incluyen un cliente compatible con IPsec, que se discute en la sección llamada "Android Mobile IPsec".

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.

Dispositivos Android 4.x pueden utilizar un cliente OpenVPN de libre acceso que funciona bien y no necesita enraizamiento el dispositivo. Que el cliente está cubierto en la sección llamada "Android 4.x". Las versiones anteriores de Android también puede ser capaz de usar OpenVPN a través de un suplente cliente no root cubierto en la sección llamado "Android 2.1 a 3.2". Hay otras opciones disponibles si el dispositivo tiene sus raíces, pero que está más allá del alcance de este libro.

iOS no tiene actualmente un cliente de OpenVPN que funciona sin jailbreak del dispositivo. Para obtener más información, consulte la sección titulada "iOS".

PPTP

Clientes PPTP se incluyen en todas las versiones de Windows desde Windows 95 OSR 2, todos los Mac OS X liberar, dispositivos iOS de Apple, dispositivos Android, y los clientes están disponibles para todos los BSD y cada distribución importante de Linux. Sin embargo, como se explica al comienzo de este capítulo, el uso de PPTP debe hay que evitar a toda costa.

Amabilidad Firewall

Protocolos VPN pueden causar dificultades a muchos firewalls y dispositivos NAT. Esto es principalmente relevante de conectividad de acceso remoto, donde los usuarios van a estar detrás de un gran número de servidores de seguridad en su mayoría fuera de su control con diferentes configuraciones y capacidades.

IPsec

IPsec utiliza tanto el puerto UDP 500 y el protocolo ESP para funcionar. Algunos servidores de seguridad no manejan ESP tráfico y donde NAT está involucrado, ya que el protocolo no tiene los números de puerto TCP y como UDP que hacen que sea fácilmente rastreable por dispositivos NAT. Clientes IPsec detrás de NAT pueden requerir NAT-T a la función, que encapsula el tráfico a través del puerto UDP ESP 4500. pfSense es compatible con NAT-T en pfSense 2.0 y superiores.

OpenVPN

OpenVPN es el más firewalls de las opciones de VPN. Puesto que utiliza TCP o UDP y no es afectados por cualquiera de las funciones de NAT comunes, como la reescritura de los puertos de origen, es raro encontrar un servidor de seguridad que no funcionará con OpenVPN. La única dificultad es posible si el protocolo y el puerto en uso es bloqueado. Es posible que desee utilizar un puerto común, como UDP 53 (normalmente DNS) o TCP 80 (HTTP normalmente) o 443 (por lo general HTTPS) o para evadir más filtrado de salida.

PPTP

PPTP se basa en un canal de control que se ejecuta en el puerto TCP 1723 y utiliza el protocolo GRE para transmitir datos. GRE se bloquea o se rompe por los cortafuegos y dispositivos NAT con frecuencia. También es objeto de NAT limitaciones en muchos firewalls incluidos pfSense (descrito en la sección "Limitaciones" PPTP).
PPTP funciona en muchos ambientes, pero sus clientes seguramente se encontrará con lugares en los que no se hace trabajo. En algunos casos, esto puede ser un problema importante evitar el uso de PPTP. Como un ejemplo,

algunos proveedores de datos inalámbricos 3G asignan direcciones IP privadas a los clientes, y no hacéis correctamente NAT GRE
tráfico, por lo que el uso de PPTP a través de 3G imposible en algunas redes. Estos factores, combinados con los problemas de seguridad inherentes con PPTP, son aún más razones para evitar su uso.

Criptográficamente seguro

Una de las funciones críticas de una VPN es garantizar la confidencialidad de los datos transmitidos. PPTP tiene sufrido de múltiples problemas de seguridad en el pasado, y tiene algunos defectos de diseño que lo hacen un débil VPN solución. Ahora que ha sido completamente comprometida, no es de ninguna manera una forma segura para proteger el tráfico.
PPTP es aún ampliamente utilizado, aunque si debe ser es una cuestión de debate. Siempre que sea posible, que recomiendo no usar PPTP. Algunos implementarlo independientemente por el factor de conveniencia.

IPsec mediante claves previamente compartidas se puede romper si se usa una clave débil. Utilice una llave fuerte, al menos 10 caracteres
de longitud que contiene una combinación de letras, números y símbolos en mayúsculas y minúsculas.

Cifrado de OpenVPN se ve comprometida si el PKI o claves compartidas son revelados.

Resumen

Tabla 16.1, "Funciones y características de VPN Tipo" muestra una visión general de las consideraciones dispuesto en esta sección.

Tabla 16.1. Rasgos y características por Tipo VPN

Tipo de VPN	ClientWidely incluido en más OS	Multi-WAN interoperable	Crypto-Firewall graphically más secure	amigable	
IPsec	no	sí	sí	sí	No (sin NAT-T)
OpenVPN	no	no	sí	sí	sí
PPTP	sí	n / a	no	no	más

VPN y reglas de firewall

VPN y reglas de firewall se manejan algo incoherente en pfSense. En esta sección se describe cómo las reglas del firewall se manejan para cada una de las opciones de VPN individuales. Para las reglas añadidas de forma automática
discutido aquí, se puede desactivar la adición de esas normas mediante la comprobación, desactive cualquier auto-añadido VPN reglas bajo el Sistema Avanzado.

IPsec

Reglas para el tráfico IPsec que llegan a la interfaz WAN especificada se permite automáticamente como se describe en la sección llamada "IPsec". Tráfico cerrada dentro de una conexión IPsec activa se controla a través de

reglas definidas por el usuario en la pestaña IPsec bajo Firewall Reglas.

OpenVPN

OpenVPN no agrega automáticamente reglas para interfaces WAN, pero sí añadir automáticamente la normativa de que permite el tráfico de los clientes autenticados, opuesta del comportamiento de IPsec y PPTP. Tráfico encapsulado dentro de una conexión OpenVPN activo es controlado a través de las reglas definidas por el usuario en el

OpenVPNtab bajo Firewall Reglas.

PPTP

PPTP agrega automáticamente reglas que permitan TCP 1723 y el tráfico GRE a la IP WAN. El tráfico de clientes PPTP conectado se controla a través de las reglas definidas por el usuario en la ficha PPTP bajo Firewall Reglas, similar a la de IPsec.

VPNs y IPv6

Hay algunas consideraciones especiales para las VPN cuando se utiliza en combinación con IPv6. Los dos cosas principales son si o no un determinado tipo de VPN compatible con IPv6, y asegurándose de que las reglas de firewall no permitir el tráfico sin cifrar en que debe venir a través de una VPN.

Soporte IPv6 VPN

Soporte para IPv6 varía de un tipo a tipo, y en apoyo al cliente. Asegúrese de consultar con el proveedor de el otro dispositivo con el fin de asegurarse de que un firewall no pfSense o cliente admite IPv6 VPNs.

IPsec

pfSense 2.1 IPsec soporta IPv6 con una peculiaridad - si utiliza direcciones IPv6 pares, el túnel sólo puede llevar fase IPv6 2 redes, y lo mismo para IPv4. No se puede mezclar el tráfico procedente de familias de direcciones. Vea la sección llamada "IPsec y IPv6".

OpenVPN

OpenVPN es totalmente compatible con IPv6 para un sitio a otro y de clientes móviles y túneles puede llevar a IPv4 e El tráfico IPv6 al mismo tiempo. Vea la sección llamada "OpenVPN y IPv6".

PPTP

PPTP no soporta IPv6, y no hay planes para tratar de hacerlo en el futuro.

IPv6 VPN y reglas de firewall

Como se mencionó brevemente en la sección titulada "Preocupaciones de Firewall y VPN", algunos cuidados especiales deben ser tomado al enrutar el tráfico IPv6 a través de una VPN y utilizar subredes enrutables públicamente. El mismo consejo que también se aplican a IPv4, pero es mucho menos común que los clientes en ambos lados de una VPN IPv4 utilizando direcciones enrutables públicamente.

El principal problema es que debido a que es posible enrutar todo el camino de una LAN a la otra a través de LAN Internet, a continuación, el tráfico podría estar fluyendo sin cifrar entre las dos redes si la VPN es abajo (O no presentarse en absoluto!). Esto está lejos de ser la ideal, porque a pesar de que se tenga conexión, si cualquier tráfico fueron interceptados entre las dos redes y que el tráfico estaba usando un protocolo sin cifrar como HTTP, entonces se podría comprometer su red.

La mejor manera de evitar esto es no permitir que el tráfico de la LAN remota en IPv6 en la del lado opuesto WAN reglas. Sólo permite el tráfico desde la subred del lado remoto de las reglas de firewall para cualquier VPN tipo se utiliza para proteger el tráfico. Usted puede incluso querer agregar una regla de bloqueo explícita a la parte superior de la WAN reglas para asegurarse de que este tráfico no puede entrar directamente desde la WAN.

Capítulo 17. IPsec

IPsec proporciona una implementación VPN basada en estándares que es compatible con una amplia gama de clientes para la conectividad móvil, y otros firewalls y routers para el sitio de la conectividad del sitio. Es compatible con numerosos dispositivos de terceros y está siendo utilizado en la producción de dispositivos que van desde los consumidores
routers Linksys grado de todo el camino hasta los mainframes de IBM z / OS, y todo lo imaginable en el medio. En este capítulo se describen las opciones de configuración disponibles, y cómo configurar distintos común escenarios.

Para una discusión general de los diversos tipos de VPN disponibles en pfSense y sus pros y sus contras, ver Capítulo 16, Redes Privadas Virtuales.

La interfaz gráfica de usuario para IPsec fue completamente rediseñado entre pfSense 1.2.3 2.x. Ahora soporta múltiples fase 2 las definiciones de cada túnel, así como NAT transversal y un mayor número de cifrado y
hash de opciones, y muchas más opciones para los clientes móviles, incluyendo xauth.

IPsec Terminología

Antes de ahondar demasiado profundamente en la configuración, hay algunos términos que se utilizan en todo el capítulo que necesita algo de explicación previa. Otros términos se explican con más detalle sobre su uso en opciones de configuración.

Asociación de Seguridad

Una Asociación de Seguridad (SA) es un túnel de un solo sentido a través del cual el tráfico cifrado viajará. Cada túnel IPsec activa tendrá dos asociaciones de seguridad, uno para cada dirección. La Seguridad Las asociaciones son de configuración entre el público Direcciones IP para cada extremo. El conocimiento de estos activos
asociaciones de seguridad se mantienen en la base de datos de la Asociación de Seguridad (SAD).

Política de Seguridad

Una política de seguridad Manges las especificaciones completas del túnel IPsec. Al igual que con Seguridad Asociaciones, estos son de un solo sentido, por lo que para cada túnel habrá uno en cada dirección. Estas entradas se mantienen en la base de datos Política de Seguridad (SPD). El SPD se rellena con dos entradas para cada se añade conexión de túnel tan pronto como un túnel. Por el contrario, sólo existen entradas SAD al éxito negociación de la conexión.

Fase 1

Hay dos fases de la negociación para un túnel IPsec. Durante la fase 1, los dos puntos finales de un configuración del túnel de un canal seguro entre los puntos finales que utilizan Internet Security Association and Key Management Protocol (ISAKMP) negociar las entradas SA y las claves de cambio. Esto también incluye autenticación, comprobación de identificadores, y la comprobación de las claves pre-compartidas (PSK) o certificados. ¿Cuándo
fase 1 se ha completado los dos extremos pueden intercambiar información de forma segura, pero aún no han decidido qué
tráfico atravesará el túnel o cómo se va a cifrar.

Fase 2

En la fase 2, los dos extremos negocien cómo cifrar y enviar los datos de las máquinas privadas basados en Políticas de Seguridad. Esta es la parte que construye el túnel real que se utiliza para la transferencia de datos entre los puntos finales y clientes cuyo tráfico es manejado por los routers. Si la fase 2 ha sido exitosamente establecido, el túnel estará listo y preparado para su uso para el tráfico que coincide con la definición de la fase 2.

IPsec y IPv6

IPsec es capaz de conectarse a un túnel sobre IPv4 o IPv6 fase 1 se refiere a los compañeros, pero el túnel sólo puede contener el mismo tipo de tráfico dentro de la definición de la fase 2 del túnel que se utiliza para pasar el tráfico exterior. Esto significa que, si bien ya sea IPv4 o IPv6 pueden ser realizadas en el interior del túnel, si desea utilizar el tráfico IPv6 dentro del túnel, el túnel debe estar conectado entre IPv6 pares IPs, no IPv4. En otras palabras, la familia de direcciones interior y exterior debe coincidir, que no se pueden mezclar. Clientes Mobile IPsec todavía no soportan IPv6.

Elección de las opciones de configuración

IPsec ofrece numerosas opciones de configuración, lo que afecta el rendimiento y la seguridad de su IPsec conexiones. Siendo realistas, poco importa que las opciones que elija aquí el tiempo que usted no utiliza DES, y utilizar una clave pre-compartida fuerte, a menos que usted está protegiendo algo tan valioso que un adversario con muchos millones de dólares en poder de procesamiento está dispuesto a dedicar a la fractura de su IPsec. Incluso en ese caso, es posible que haya una manera más fácil y mucho más barato para entrar en la red y lograr el mismo resultado final (la ingeniería social, por ejemplo).

1 Configuración de fase

Estos ajustes controlan la parte de la negociación de fase 1 del túnel, como se describió anteriormente.

Activar / Desactivar el túnel

La casilla de verificación Disabled controla si o no este túnel (y su fase asociada 2 entradas) se activo y utilizado.

Protocolo de Internet

El selector de protocolo de Internet define el protocolo para la fuera del túnel. Es decir, el protocolo que se utilizará entre las direcciones de pares externos. Para la mayoría, esto será IPv4, pero si ambos extremos son capaz de IPv6, es posible que desee utilizar en su lugar. Sea cual sea el protocolo de que se elija aquí será usada para validar la puerta de enlace remota y los identificadores asociados.

Selección de la interfaz

En muchos casos, la opción de interfaz para un túnel IPsec será WAN, ya que los túneles se conectan a sitios remotos. Sin embargo, hay un montón de excepciones, la más común de las cuales se describen a continuación.

Entornos CARPA

En entornos CARP (capítulo 24, Firewall de redundancia / alta disponibilidad), cualquier CARP virtuales Las direcciones IP también están disponibles en el menú desplegable Interface. Usted debe elegir la adecuada Dirección CARP para su WAN o donde el túnel IPsec terminará en el sistema pfSense. Por utilizando la dirección IP CARP, asegura que el túnel IPsec será manejado por el miembro MAESTRO del cluster CARP, por lo que incluso si el firewall principal está abajo, el túnel se conectará a cualquier CARP miembro del clúster se ha hecho cargo.

IP Alias VIP

Si tiene varias direcciones IP en una interfaz usando IP Alias VIPs, también estarán disponibles en esta lista. Si desea utilizar una de las IPs de la VPN en su lugar, seleccione aquí.

Multi-WAN Entornos

Cuando se utiliza multi-WAN (Capítulo 15, Varias conexiones WAN), usted debe escoger la adecuada Opción de interfaz para la interfaz tipo WAN a la que el túnel se conectará. Si usted espera que el

conexión que debe introducir a través de la WAN, pick WAN. Si el túnel se debe utilizar una WAN diferente, elija el que sea
Se necesita un interfaz OPT WAN. Se agregará automáticamente una ruta estática para asegurarse de que el tráfico a las rutas remotos de puerta de enlace a través de la WAN adecuada.

Comenzando con pfSense 2.1 también se puede optar por un grupo de pasarela de esta lista. Un grupo puerta de entrada a ser
utilizada con IPsec sólo debe tener una pasarela por nivel. Cuando se utiliza un grupo de puerta de enlace, si la primera puerta de enlace
se cae, el túnel se moverá a la siguiente disposición WAN en el grupo. Cuando llega el primero WAN
una copia de seguridad, el túnel será reconstruido allí de nuevo.

Wireless Protección Interna

Si va a configurar IPsec para añadir encriptación para una red inalámbrica, tal como se describe en la sección llamada "Protección adicional con VPN", usted debe elegir la interfaz OPT que corresponde a su
tarjeta inalámbrica. Si está utilizando un punto de acceso inalámbrico externo, elija el pfSense interfaz puede utilizar para conectarse al punto de acceso inalámbrico.

Pasarela Remota

La puerta de enlace remoto es el mismo nivel de IPsec para esta fase 1. Este es el router en el otro lado del túnel a la que IPsec negociará esta fase 1.

Descripción

La descripción de la fase 1 es un texto que se utilizará para identificar esta fase 1. No se utiliza en el Configuración de IPsec, es sólo para referencia.

Método de autenticación

Una fase 1 IPsec se puede autenticar utilizando una clave pre-compartida (PSK) o certificados RSA, la Selector de Método de autenticación le permite elegir cuál de estos métodos se utilizará para la autenticación La distancia entre pares. Los campos apropiados para el método elegido se mostrará en la configuración de la fase 1 pantalla.

PSK Mutual

Al utilizar PSK Mutual, el par se valida mediante una cadena definida. El más largo es el mejor, pero ya que es una cadena sencilla, hay una posibilidad de que se puede adivinar. Por esta razón le recomendamos una clave larga / compleja cuando se utiliza el modo PSK.

RSA Mutual

En RSA Mutual modo, usted selecciona una CA y el certificado utilizado para verificar los pares. Durante la fase 1 intercambio, cada interlocutor envía su certificado a la otra por pares y después valida en contra de su CA compartida. Debe crear o importar el CA y el certificado para el túnel antes de intentar configurar la fase 1.

Mutual PSK + Xauth

Utilizado con el móvil IPsec, esta selección permite xauth nombre de usuario y verificación de la contraseña junto con una clave pre-compartida compartida (o "grupo").

Mutual RSA + Xauth

Utilizado con el móvil IPsec, esta selección permite xauth nombre de usuario y verificación de la contraseña junto con Autenticación de certificados RSA utilizando certificados tanto en el cliente y el servidor.

Híbrido RSA + Xauth

Utilizado con el móvil IPsec, esta selección permite xauth nombre de usuario y verificación de la contraseña junto con un certificado sólo en el lado del servidor. No es tan seguro como Mutual RSA + Xauth, pero es más fácil en los clientes.

Modo de Negociación

Tres opciones de modo de negociación son compatibles: principal, agresivo, y base.

Modo principal

Principal es el modo más seguro, aunque también requiere más paquetes entre los pares de lograr una negociación exitosa. También es mucho más estricta, el identificador debe ser la dirección IP del extremo remoto y no un identificador personalizado.

Modo Agresivo

Agresivo es generalmente el más compatible y es el modo más rápido. Es un poco más indulgente con tipos de identificadores, y tiende a tener más éxito en la negociación con los dispositivos de otros fabricantes de alguna casos. Es más rápido, ya que envía toda la información de identificación en un solo paquete, que también hace que sea menos seguro porque la comprobación de que los datos no es tan estricta como la que se encuentra en el modo principal.

El modo de base

Base modo se discute en un proyecto de IETF [http://tools.ietf.org/html/draft-ietf-ipsec-ike-base-mode-02] y está destinado a resolver problemas con ambos Principal y Agresivo modos; Permite personalizada identificadores, y sigue siendo seguro. Apoyo a la Base modo no es tan común como las otras opciones, sin embargo.

Mi identificador identificador / Peer

En Agresivo y Base modos, usted puede elegir el identificador utilizado para enviar al interlocutor remoto, y también para la verificación de la identidad del interlocutor remoto. Los siguientes tipos de identificadores pueden ser elegidos
para el Mi Identificador y selectores identificador del par. Si es necesario, aparecerá un cuadro de texto para que ingrese un valor que se utilizará para el identificador.

Mi dirección IP / IP Peer

Esta elección es una macro que utilizará automáticamente la dirección IP de la interfaz, o el seleccionado VIP, como el identificador. Para sus compañeros, esta es la dirección IP desde la que se recibieron los paquetes, que debe ser la puerta de enlace remoto.

Dirección IP

La opción Dirección IP le permite introducir una dirección IP diferente para ser utilizado como su identificador. Una potencial
utilizar para esto sería si el servidor de seguridad está detrás de un router NAT de realizar. Usted puede utilizar el externo Dirección IP en este campo.

Nombre distintivo

Un nombre distinguido es otro término para un nombre de dominio completo, como host.example.com. Introduzca un valor en ese formato en la caja.

Nombre de Usuario Distinguido

Un usuario Nombre distintivo es una dirección de correo electrónico, tales como vpn@example.com, en lugar de un FQDN.

ASN.1 nombre distinguido

Si utiliza la autenticación RSA Mutual, esto puede ser el sujeto del certificado que se utiliza, o similar cadena.

Tag KEYID

Una cadena de su elección que se utiliza como identificador.

DNS dinámico

Un nombre de host para resolver y utilizar como identificador. Esto es sobre todo útil si el servidor de seguridad está detrás de NAT
y no tiene conocimiento directo de su dirección IP externa, aparte de un nombre de host DNS dinámico. Este no es relevante o disponible para un identificador de punto ya sólo tiene que utilizar el nombre de host en el remoto Campo Puerta de enlace y el uso Dirección IP Peer para el identificador.

Pre-Shared Key (Si utiliza Mutual PSK)

Este campo se utiliza para entrar en el PSK para la fase 1 de autenticación. Como se mencionó anteriormente, esto debe ser
clave a largo / complejo. Si esto PSK ha sido facilitado por su pares, ingrese aquí. Si usted tiene que generar uno, recomendamos el uso de una herramienta de generación de contraseñas se establece en una longitud de al menos 15, pero puede ser mucho más largo.

Generación Política

Esta directiva controla cómo pfSense actuará como un respondedor de 2 políticas de eliminación, y no se utiliza en absoluto
cuando este servidor de seguridad inicia la conexión IPsec. Si no hay fase 2 las políticas existentes y esto es ajustado a On, entonces pfSense aceptará la primera política propuesta por el par remoto. La Exigir opción es equivalente a On. Único hará que pfSense Creación y seguimiento de políticas únicas para cada cliente. Apagado evitar que las políticas que se generen de forma automática, en lugar de confiar sólo en las políticas configuradas manualmente en la fase 2.

El valor por defecto de esto es Apagado para túneles normales, En para PSK-only móvil IPsec, y Único para otros tipos de IPsec móviles.

Comprobación Propuesta

Esta configuración controla cómo pfSense responderá a ciertos parámetros suministrados por el par remoto. Estos parámetros son: fase 1 curso de la vida, fase 2 de por vida, fase 2 longitud de la clave, y la fase 2 de PFS.

Si Obedecer que se elija, los valores suministrados por el par remoto se utilizarán cada vez. Esta opción es útil cuando se conecta a equipos de terceros, especialmente los equipos de Cisco, que pueden tener una tendencia a enviar valores inesperados para estos parámetros. La desventaja de Obedecer es que si el par remoto tiene valores menos seguros para estos parámetros, la integridad del túnel podrían verse comprometidas en comparación a la configuración que desea utilizar.

Estricto se asegurará de que sólo se utilizan los valores de longitud de la clave y la vida útil se suministra, a menos que el los valores de pares son más seguro, en cuyo caso los puede utilizarse en su lugar. Si PFS está habilitado en ambos lados, el valor PFS deben coincidir. Si no se requiere la SLP, no va a ser ejecutada.

Reclamación funciona de manera similar a Estricto excepto que se notificará a la par de una ajustada fase 2 por vida y el uso de su cuenta, si es su propio tiempo.

Exacto rechazará cualquier cosa excepto una coincidencia exacta de los valores.

Por defecto, pfSense utiliza un valor de Reclamación para túneles normales, y Obedecer para túneles IPsec móviles.

Los algoritmos de cifrado

Hay muchas opciones para los algoritmos de cifrado tanto en la fase 1 y la fase 2. DES (Data Encryption Estándar) se considera inseguro debido a su pequeño tamaño de 56 bits clave, y nunca debe ser usado a menos se ven obligados a conectar con un dispositivo remoto que sólo es compatible con DES. Las opciones restantes son todos considerados criptográficamente seguro. Cuál elegir depende de qué dispositivo se está conectando a, y el hardware disponible en su 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 el otro extremo apoya. En los sistemas sin un acelerador de hardware de criptografía, Blowfish y REPARTO son las opciones más rápidas. Cuando se utiliza con sistemas `glxsb` aceleradores, como ALIX, elija AES 128 para un mejor rendimiento. Para los sistemas con `hifn` aceleradores, eligieron 3DES o AES para el mejor rendimiento. Tanto AES y

Blowfish le permiten seleccionar la longitud de la clave de cifrado en los pasos entre 128 bits y 256 variables - poco. Los valores más bajos serán más rápidos, los valores más grandes son más criptográficamente seguro.

Los algoritmos hash

Los algoritmos hash se utilizan con IPsec para verificar la autenticidad de paquetes de datos. MD5, SHA1, SHA256, SHA384, SHA512 y son los algoritmos hash disponibles en la fase 1 y la fase 2. Todos se consideran criptográficamente seguro, aunque SHA1 (Secure Hash Algorithm, Revisión 1) y sus variantes son considerado el más fuerte que MD5. SHA1 requiere más ciclos de CPU que MD5, y el más grande valores de SHA a su vez requieren mayor potencia de la CPU. Estos algoritmos hash también puede ser denominado con HMAC (Hash Message Authentication Code) en el nombre, en algunos contextos, pero que el uso varía dependiendo del hardware o el software que se utilice.

Nota

La implementación de SHA256-512 es el RFC 4868 [http://tools.ietf.org/rfc/rfc4868.txt] compatible en FreeBSD 8.3 en la que pfSense 2.1 se basa, y que es la primera versión en pfSense donde existe apoyo para aquellas implementaciones SHA de mayor valor. RFC 4.868 cumplimiento rompe la compatibilidad con las pilas que implementaron el proyecto-ietf-ipsec-CIPH-sha-256-00 [http://tools.ietf.org/html/draft-ietf-ipsec-ciph-sha-256-00], incluyendo FreeBSD 8.1 y antes. Antes de utilizar SHA256, 384, o 512, verifique con el otro lado para Asegúrese de que también son RFC 4868 implementaciones compatibles o no van a trabajar. La relevante FreeBSD cometen mensaje [http://lists.freebsd.org/pipermail/svn-src-head/2011-February/025040.html] cuando esto sucedió, explica en un poco más de detalle.

Grupo clave DH

Todos los de la DH (Diffie-Hellman, el nombre de sus autores) las opciones de grupos clave consideradas criptográficamente seguro, aunque los números más altos son un poco más seguro a costa de una mayor Uso de la CPU.

Vidas

El tiempo de vida especifica la frecuencia debe ser rekeyed la conexión, especificado en segundos. 28.800 segundos en la fase 1 es una configuración bastante estándar y es apropiado para la mayoría de los escenarios.

Mi certificado (Si utiliza Mutual RSA)

Esta opción sólo aparece si se utiliza un modo de autenticación basada en RSA. La lista se completa con el certificados presentes en la configuración del cortafuegos. Los certificados se pueden importar y administrar en Sistema
 Administrador de Cert en la ficha Certificados. Seleccione el certificado que desea utilizar para esta fase IPsec 1 de la lista. La CA de este certificado debe coincidir con el elegido en la opción Mi Autoridad de certificados.

Mi entidad emisora de certificados (Si utiliza Mutual RSA)

Esta opción sólo aparece si se utiliza un modo de autenticación basada en RSA. La lista se rellena utilizando presente en las CA de configuración de servidor de seguridad. Una CA puede ser importado y gestionado bajo el Sistema
 Cert
Manager. Elija el CA desea utilizar para esta fase IPsec 1 de la lista.

NAT Traversal

NAT, también conocida como NAT-T, puede encapsular el tráfico ESP de IPsec en el interior de la UDP paquetes, para funcionar más fácilmente en presencia de NAT. Si su firewall o servidor de seguridad en el otro final del túnel, estará detrás de un dispositivo NAT, se debe establecer a un Habilitar. En los casos en que saben que los dos extremos del túnel se conectan directamente a una dirección IP enrutable públicamente, lo mejor es a Inhabilitar esto, ya que puede causar problemas de la renegociación de un túnel cuando no es necesario. En algunos casos,

clientes IPsec especialmente móviles, es posible que necesite Fuerza esta opción para asegurarse de que los clientes siempre
utilizar NAT-T.

Dead Peer Detection (DPD)

Dead Peer Detection (DPD) es una verificación periódica de que el host en el otro extremo del túnel IPsec sigue vivo. Si un cheque DPD falla, el túnel está derribada mediante la eliminación de sus entradas SAD asociados y la renegociación se intenta. El campo de segundo controla la frecuencia con que se intente un cheque DPD, y el campo reintentos controla cuántas de estas pruebas deberán fallar antes de un túnel se considera abajo. Los valores por defecto de 10 y segundo 5reintentos se traducirá en el túnel está considerado después de aproximadamente un minuto. Estos valores se pueden incrementar para enlaces mala calidad para evitar derribar un utilizable, pero con pérdida, en un túnel.

2 Ajustes de fase

La fase 2 ajustes para un túnel IPsec gobiernan el tráfico que entra en el túnel, así como la forma que el tráfico se cifra. Para los túneles normales, esto controla las subredes que entrarán en el firewall. Para clientes móviles controla esta principalmente el cifrado para la fase 2, pero también se pueden suministrar opcionalmente una lista
de las redes a los clientes para su uso en la división de túnel. Desde pfSense 2.0, de múltiples fases 2 definiciones se puede agregar para cada fase 1 para permitir el uso de múltiples subredes dentro de un único túnel.

Activar / Desactivar

Este ajuste controla si esta entrada en la fase 2 está activo.

Modo

Nuevo en pfSense 2.0, esta opción le permite utilizar el modo túnel tradicional de IPsec, o el transporte modo. El modo túnel era la única opción disponible en pfSense 1.x. En pfSense 2.1, el modo de túnel También se dividió para especificar IPv4 o IPv6.

Modo túnel IPv4/IPv6

Cuando se utiliza ya sea IPv4 túnel o IPv6 Túnel para esta fase 2, la categoría, el firewall del túnel IPv4 o IPv6 tráfico que coincide con la de la red local especificado y de red remota. Una fase 2 puede ser para cualquiera de los valores de red IPv4 o IPv6, y se validan en base a esa elección. Juego Traffic tanto en la red local y de red remota entrarán en el túnel y llegan a su destino hasta el otro lado.

Modo de Transporte

Transporte Modo cifrará el tráfico entre las direcciones IP utilizadas como fase 1 puntos finales. Este modo permite el cifrado del tráfico de IP externa del servidor de seguridad para IP externa del router otro lado. Cualquier tráfico
enviado entre los dos nodos serán encriptados, por lo que el uso de otros métodos de túneles que no emplean cifrado, por ejemplo, GIF o GRE túnel, se puede utilizar de manera segura. No se puede establecer una red local o Red remota para el modo de transporte, asume las direcciones basadas en los ajustes de fase 1.

Red Local (Si utiliza un modo de túnel)

Como su nombre lo indica, esta opción establece la Red Local, que se asocia con esta fase 2.
Esto es típicamente su LAN u otra subred interna para la VPN, pero también puede ser una única dirección IP si sólo un cliente tiene que utilizar el túnel. El selector de tipo se pre-cargado con opciones de subred para cada interfaz (por ejemplo, Subred LAN), así como Dirección y Red opciones que le permiten entrar en una dirección IP o subred de forma manual.

Dirección NAT para NAT + IPsec

Si necesita realizar NAT en sus IPs locales para hacerlos aparecer como una subred diferente, o uno de sus IPs públicas, puede hacerlo a través de los campos de NAT debajo de la red local. Si se especifica un

única dirección IP en la red local y una única dirección IP en el campo NAT, entonces una regla NAT 01:01 será añadido entre los dos. NAT 1:1 es también configurar si se utiliza una subred en ambos campos. Si utiliza una red local que es una subred, pero una dirección NAT que es una sola IP, entonces un 1: muchos NAT (PAT) regla se agrega que funciona como una regla de NAT saliente en WAN, todo el tráfico saliente será traducido desde la red local a la única dirección IP en el campo NAT. Si usted no tiene que hacer NAT en el IPsec tráfico, no, deje Ninguno.

Remote Network (Si utiliza un modo de túnel)

Esta opción (sólo presente en los túneles no móviles) especifica la IP Dirección o Red lo que existe en el otro lado (a distancia) de la VPN.

Protocolo

Con IPsec usted tiene la opción de elegir AH (Jurada Header) o ESP (Encapsulating Security Payload). En casi todos los casos, debe utilizar ESP, ya que es la única opción que cifra tráfico. AH sólo proporciona la garantía de que el tráfico proviene de la fuente de confianza y rara vez se utiliza.

Los algoritmos de cifrado

Las opciones de la fase 2 de encriptación permiten selecciones múltiples. El consejo en este capítulo, en el sección llamada "Los algoritmos de cifrado", sigue siendo válida. Sin embargo, puede seleccionar varias opciones para que
serán aceptadas o bien múltiples opciones cuando actúa como respondedor, o múltiples combinaciones serán intenta cuando se trabaja como un iniciador. Lo mejor es sólo para seleccionar el único sistema de cifrado que desea utilizar, pero en
algunos casos la selección múltiple permitirán un túnel a trabajar mejor, tanto en un respondedor y el papel de iniciador.

Los algoritmos hash

Al igual que con los algoritmos de cifrado, aquí se pueden seleccionar varios hashes. Todavía recomendamos solamente seleccionar el hash que necesita. Para más discusiones sobre la calidad de los diversos tipos de hash, consulte la sección llamada "Los algoritmos hash".

Grupo clave PFS

Perfect Forward Secrecy (PFS) ofrece material de claves con mayor entropía, por lo tanto, la mejora de la seguridad criptográfica de la conexión, a costa de un mayor uso de la CPU cuando se produce cambio de claves. La opciones tienen las mismas propiedades que la opción de grupo de claves DH en la fase 1 (Vea la sección llamada "DH grupo clave ").

Vida

El tiempo de vida especifica la frecuencia debe ser rekeyed la conexión, especificado en segundos. 3.600 segundos en la fase 2 es una configuración bastante estándar y es apropiado para la mayoría de los escenarios.

Automáticamente Ping Host (Keep Alive)

Para uso en túneles no móviles, esta opción hará que el servidor de seguridad para iniciar una mesa de ping periódicamente a la
IP especificada. Esta opción sólo funciona si el servidor de seguridad tiene una IP dentro de esta fase de la Red Local de 2
y el valor de la acogida de ping aquí debe estar dentro de la red remota.

IPsec y las reglas de firewall

Cuando se configura una conexión de túnel IPsec, pfSense agrega automáticamente reglas de firewall ocultos para permitir que los puertos UDP 500 y 4500, y el protocolo ESP de la puerta de enlace remota IP destinado a la IP Interface especifica en la configuración. Al permitir a los clientes móviles está habilitada, el mismo firewall

se añaden reglas, excepto con la fuente se establece en ninguno. Para anular la adición automática de estas reglas, verificación Deshabilitar todas las reglas VPN auto-añadido en virtud del Sistema Avanzado en el / pestaña NAT Firewall. Si
comprobar que esa caja, debe agregar manualmente las reglas de firewall para UDP 500, UDP 4500 y ESP para el interfaz WAN apropiado.

Tráfico iniciada desde el extremo remoto de una conexión IPsec se filtra con las reglas configuradas bajo Firewall Reglas, pestaña IPsec. Aquí se puede restringir qué recursos se puede acceder mediante IPsec remoto los usuarios. Para controlar el tráfico que se puede transmitir de redes locales para el IPsec VPN remoto conectado dispositivos o redes, las normas relativas a la interfaz local donde reside el host controlan el tráfico (por ejemplo, conectividad de hosts de LAN se controlan con las normas de LAN).

Sitio a sitio

Un sitio a otro túnel IPsec permite interconectar dos redes como si estuvieran conectados directamente por un router. Sistemas en el sitio A pueden llegar a los servidores u otros sistemas en el sitio B, y viceversa. Este tráfico También se puede regular a través de reglas de cortafuegos, al igual que con cualquier otra interfaz de red. Si más de uno cliente se conecta a otro sitio desde el mismo lugar controlado, un sitio para hacer un túnel sitio se probablemente será más eficiente, por no mencionar más conveniente y más fácil de soportar.

Con un sitio para hacer un túnel sitio, los sistemas de las dos redes no necesitan tener ningún conocimiento de que una VPN incluso
existe. No se necesita ningún software cliente, y todo el trabajo del túnel está a cargo de los routers en cada extremo de la conexión. Esto también es una buena solución para los dispositivos que cuentan con el apoyo de la red, pero no manejan
Conexiones VPN, como impresoras, cámaras, sistemas HVAC y otro hardware incorporado.

Sitio con el ejemplo de configuración del sitio

La clave para hacer un túnel IPsec de trabajo es asegurarse de que ambas partes han emparejan ajustes para la autenticación, cifrado, y así sucesivamente. Antes de comenzar, tome nota de lo local y remota WAN IP direcciones así mientras subredes internos locales remotas serás CONECTANDO. Una dirección IP de la subred remota al ping es opcional, pero se recomienda para mantener vivo el túnel. El sistema no comprobar si hay respuestas, ya que cualquier tráfico inició a una IP en la red remota desencadenará negociación IPsec, por lo que no importa si el host responde realmente o no, siempre y cuando se trata de una IP en el otro lado de la conexión. Aparte de la cosmética Descripción túnel y estas piezas de información, el otro configuración de la conexión serán idénticos.

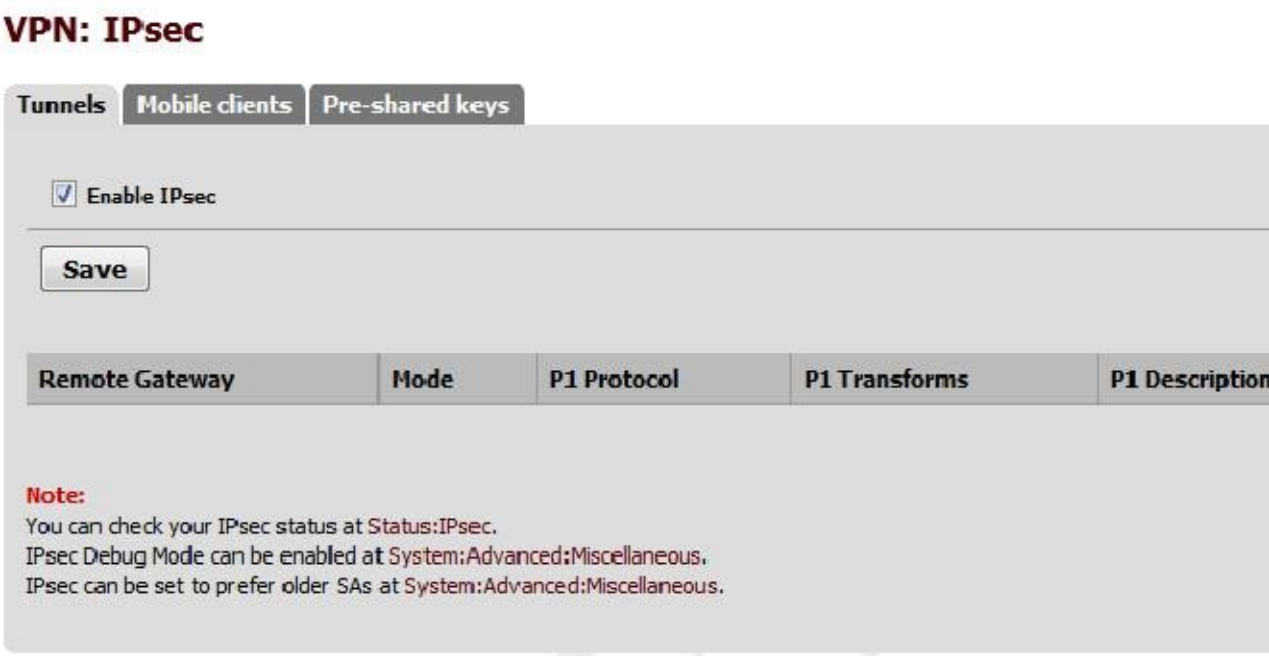
En este ejemplo, y algunos de los ejemplos siguientes de este capítulo, los siguientes ajustes serán asumido:

Tabla 17.1. IPsec Configuración de extremo

Del sitio		Sitio B	
Nombre	Oficina Louisville	Nombre	Oficina de Londres
WAN IP	172.23.1.3	WAN IP	172.16.1.3
LAN subred	192.168.1.0/24	LAN subred	10.0.10.0/24
LAN IP	192.168.1.1	LAN IP	10.0.10.1

Vamos a comenzar con el sitio A. En primer lugar, debemos permitir IPsec en el router. Vaya a VPN IPsec, Cheque Habilitar IPsec, haga clic en Guardar (Figura 17.1, "Habilitar IPsec").

Figura 17.1. Habilitar IPsec



Ahora, cree el túnel presionando botónpara. Ahora verá una página de gran tamaño que tiene la fase 1 configuración para el túnel. No se deje demasiado desanimado, ya que muchos de estos ajustes pueden dejarse en sus valores por defecto.

Para comenzar, complete la sección superior que tiene la información de fase 1 en general, que se muestra en la Figura 17.2,
"Sitio de una VPN Configuración de túnel". Se requieren elementos en negrita. Se requieren elementos en negrita. Asegurar que
Deshabilitar esta caja de túnel no está marcada. El Protocolo de Internet debe ser IPv4. La configuración de la interfaz probablemente debería ser WAN, pero vea la nota en la sección "Selección de la interfaz" en la selección de la interfaz adecuada si no está seguro. La puerta de enlace remota es la dirección WAN en el sitio B, 172.16.1.3.
Por último, introduzca una descripción para el túnel. Es una buena idea poner el nombre del sitio B de esta caja de texto, y
cierto detalle sobre el propósito del túnel también puede ayudar a la futura administración. Pondremos "ExampleCo Oficina de Londres " en la descripción de lo que tenemos alguna idea de dónde está el túnel termina.

La siguiente sección controla fase IPsec 1 o autenticación. Se muestra en la Figura 17.3, "sitio Fase 1 Configuración ". Los valores predeterminados son deseables para la mayoría de estos valores, y simplifica el proceso. El más
ajuste importante para hacerlo bien es la clave precompartida. Como se mencionó en el resumen de VPN, IPsec usando claves pre-compartidas se pueden romper si se usa una clave débil. Utilice una llave fuerte, al menos 10 caracteres de longitud
que contiene una combinación de letras, números y símbolos en mayúsculas y minúsculas. La misma clave necesitarán que se introducirán en la configuración del túnel para el sitio B más tarde, por lo que puede que lo escriba, o copiarlo y pegarlo en otro lugar. Copiar y pegar pueden venir muy bien, sobre todo con una clave compleja como abc123% XyZ9 $ 7qwErty99. Un ajuste de por vida también se puede especificar, de lo contrario el valor por defecto de 86400 se utilizará.

Configure NAT Traversal para Desactivar, ya que en este ejemplo no está detrás del firewall NAT. Compruebe Dead Peer Detección (DPD) e introduzca los valores razonables, como la 10 y segundo 5reintentos. Según
sus necesidades de un valor más alto puede ser mejor, más como 30 y segundo 6reintentos, pero una WAN problemática conexión a cada lado puede hacer que demasiado baja. Haga clic en Guardar para completar la configuración de la fase 1.

Después se ha añadido la fase 1, se tendrá que añadir una nueva definición de la fase 2 a la VPN. Para ello
ello, haga clic en el botón +, como se ve en la Figura 17.4, "del sitio de la Fase 2 lista (vacía)" para ampliar la fase 2 lista para esta VPN. Dado que no hay fase 2 entradas, haga clic en en el lado derecho de añadir una, como se ha visto En la Figura 17.5, "Adición de una entrada de la Fase 2 de sitio".

Figura 17.4. Sitio Fase 2 lista (vacía)

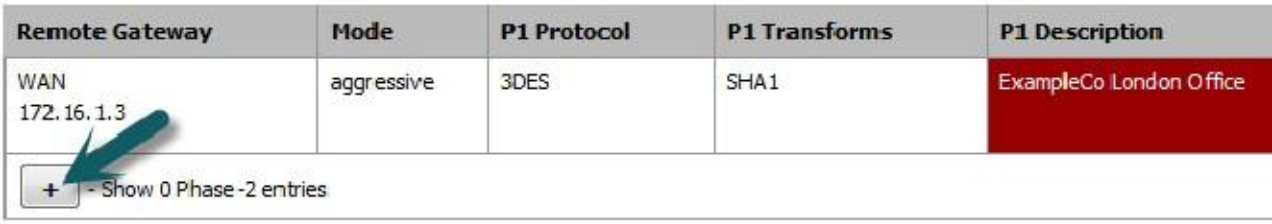
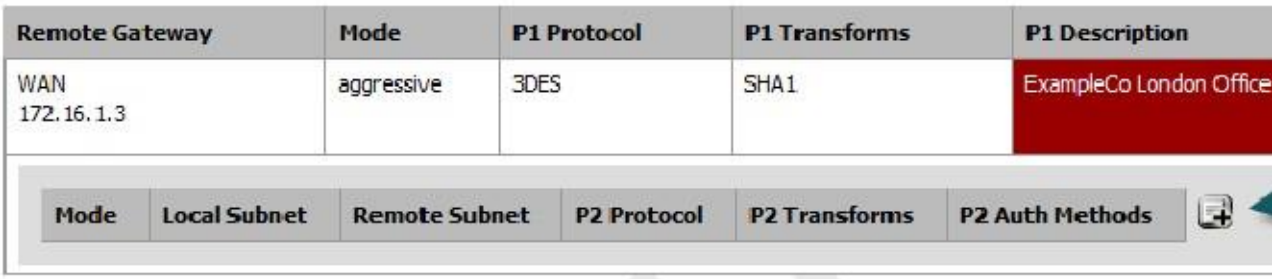
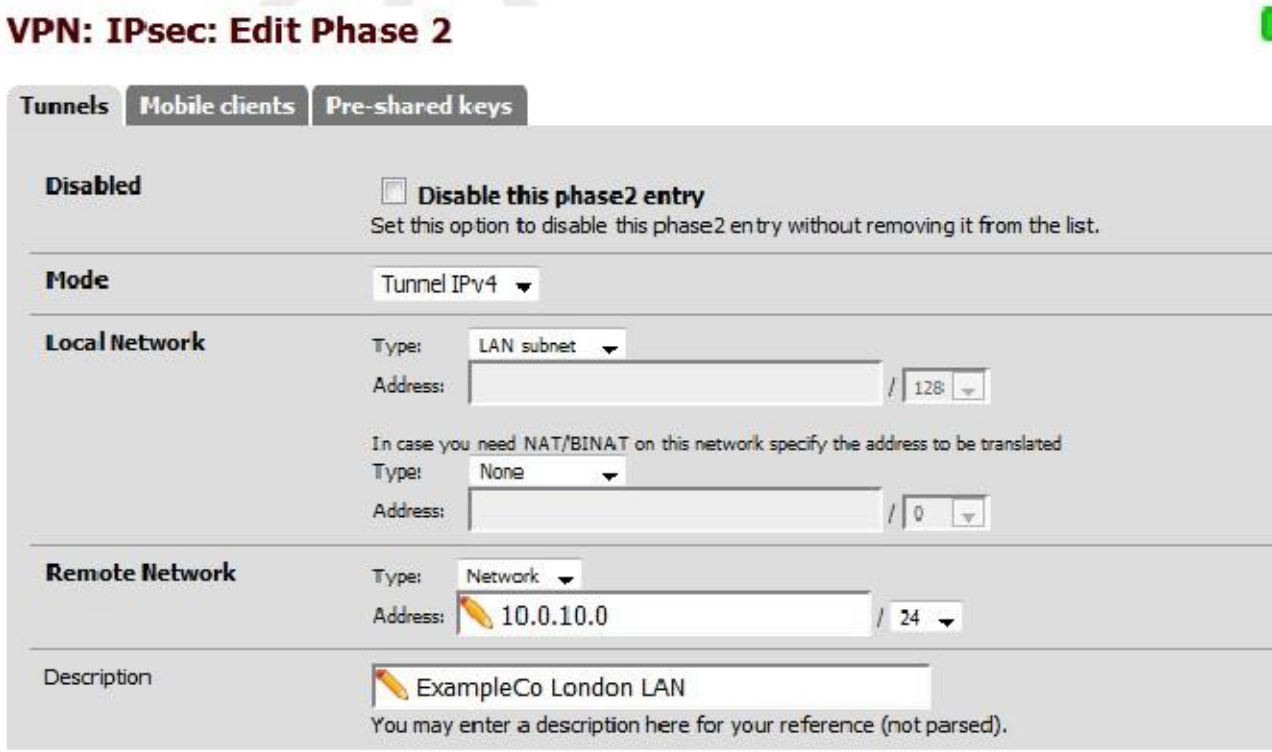


Figura 17.5. Adición de una entrada de la Fase 2 a sitio



Ahora puede agregar el establecimiento de la fase 2 de este VPN. La fase 2 (Figura 17.6, "del sitio de la Fase 2 Configuración general ") ajustes pueden tener un poco más de la variabilidad. En este caso, ya que queremos hacer un túnel
tráfico, seleccionamos IPv4 túnel para el modo. Para la subred local, es probablemente la mejor manera de salir de esta como LAN subred. También puede cambiar esto a Red y rellenar los valores adecuados, en este caso 192.168.1.0/24, pero dejando como LAN subred se asegurará de que si la red cada vez renumerado, este extremo del túnel seguirá. Tenga en cuenta el otro extremo se debe cambiar manualmente. La subred NAT debe ser Ninguno. La subred remota será la red en el sitio B, en este caso 10.0.10.0/24.

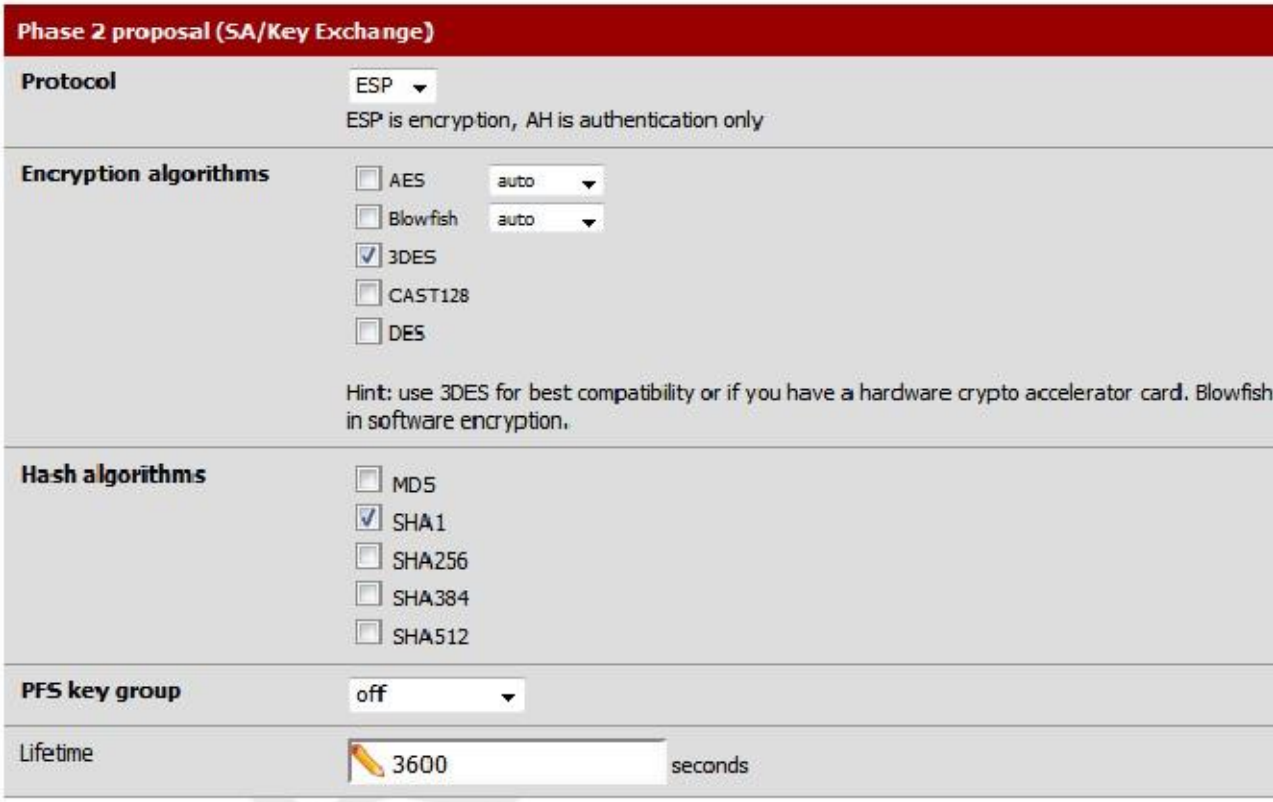
Figura 17.6. Sitio de una fase de configuración general 2



El resto de los ajustes de fase 2, se observan en la Figura 17.7, "del sitio de la Fase 2 Configuración", cubre la el cifrado del tráfico. La elección Protocolo debe ESP para el cifrado. Los algoritmos de cifrado

y los algoritmos de hash pueden ambas funciones fijas al permitir múltiples opciones, y ambas partes negociarán y estoy de acuerdo
de la configuración. En algunos casos, eso puede ser una buena cosa, pero por lo general es mejor restringir esto a las opciones que usted sabe que van a estar en uso. Para este ejemplo, el único algoritmo de cifrado seleccionado es 3DES, y el único algoritmo de hash SHA1 es seleccionado. PFS o Perfect Forward Secrecy, pueden ayudar a proteger contra ciertos ataques clave, pero es opcional. Un ajuste de por vida también se puede especificar, de lo contrario
el valor predeterminado de 3600 se utilizará.

Figura 17.7. Del sitio de la Fase 2 Configuración



Por último, se puede introducir una dirección IP para un sistema de la LAN remota que periódicamente se deben enviar una mesa de ping ICMP, como en la Figura 17.8, "sitio Keep Alive". El valor devuelto por el ping no está marcada, esto sólo se asegurará de que una parte del tráfico se envía en el túnel de manera que se quedará estableció. En esta configuración,
podemos utilizar la dirección IP de LAN del router pfSense en el sitio B, 10.0.10.1.

Figura 17.8. Sitio Keep Alive

Haga clic en el botón Guardar y, a continuación, tendrá que hacer clic en Aplicar cambios en la pantalla de IPsec Túneles, como
observa en la Figura 17.9, "Aplicar configuración de IPsec".

Figura 17.9. Aplicar configuración de IPsec

El túnel para el sitio está terminado, pero ahora se necesitan reglas de firewall para permitir el tráfico desde el sitio B de la red para entrar por el túnel IPsec. Estas reglas deben ser añadidos a la pestaña IPsec bajo Firewall □

Reglas. Véase el capítulo de reglas de firewall para obtener información específica sobre la adición de las reglas. Usted puede ser tan permisiva como
te gusta, (permitir cualquier protocolo desde cualquier parte), o restrictivas (permita TCP desde un host determinado en el sitio B hasta cierto anfitrión del sitio en un determinado puerto). En cada caso, asegúrese de que la dirección de origen (es) son
Direcciones del sitio B, tales como 10.0.10.0/24. Las direcciones de destino deben ser el sitio de la red, 192.168.1.0/24.
Ahora que del sitio se configura, es el momento de abordar el Sitio B. Repita el proceso en el router del sitio B a habilitar IPsec y añadir un túnel.

Sólo las tres partes de esta configuración se diferencian de Sitio A. Esos son los ajustes de fase 1, el túnel de la fase 2 redes y la configuración para mantener la vida, como se puede ver en la Figura 17.10, "Sitio B Fase 1 Configuración" y Figura 17.11, "Sitio B Fase 2 Configuración". En la fase 1, asegúrese de que la opción Deshabilitar esta caja de túnel es sin marcar. La configuración de la interfaz debe ser WAN. Rellene el Dead Peer Detection (DPD) de valor con el mismo ajuste que el sitio A. La puerta de enlace remota es la dirección WAN en el Sitio A, 172.23.1.3. La Descripción para el túnel sigue siendo una buena idea. Pondremos "ExampleCo Louisville Oficina " en este lado. Haga clic en Guardar y luego añadir una fase 2 de este lado. Para la fase B del Sitio 2, configuración de la Local
Subred, probablemente es mejor dejar esto como LAN subred. También puede cambiar esto a Red y rellenar 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.

Figura 17.10. Sitio B Fase 1 Ajustes

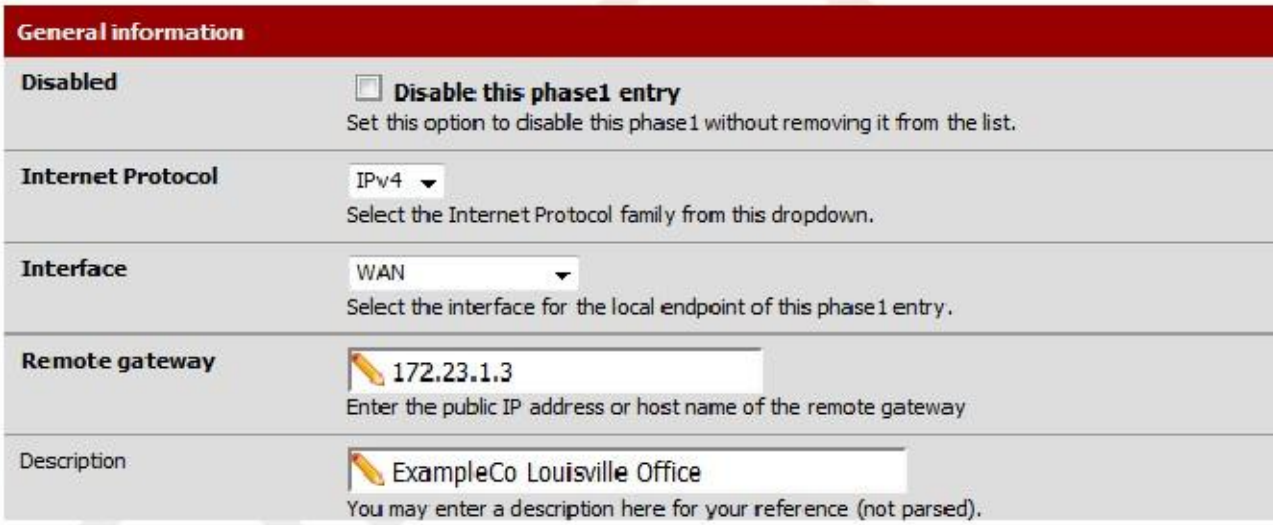
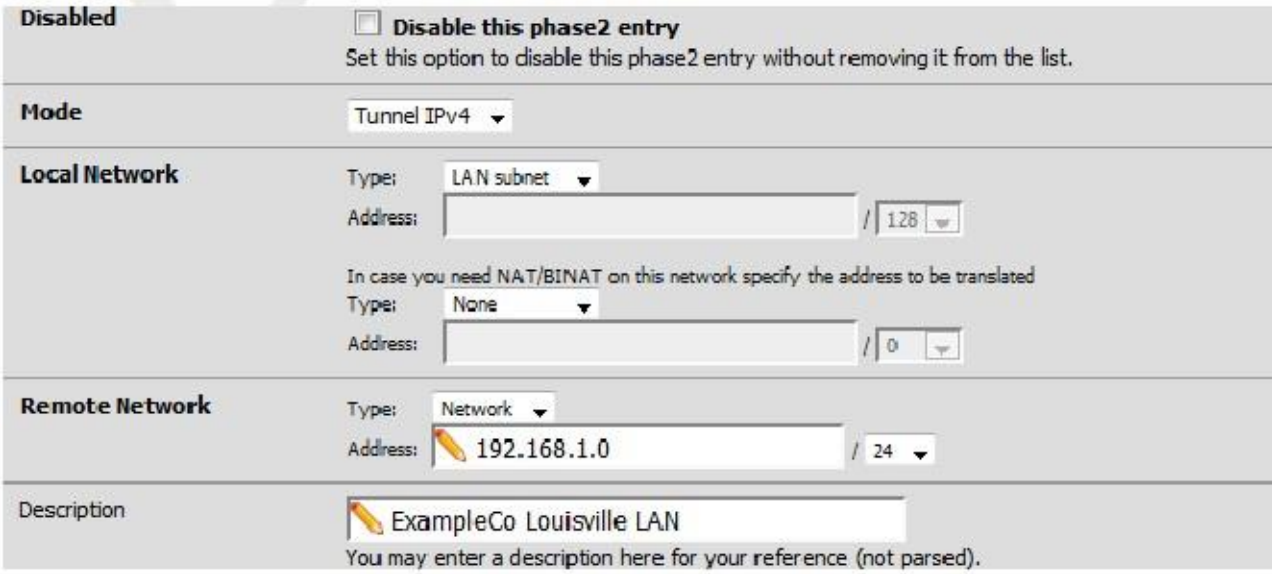


Figura 17.11. Sitio B Fase 2 Configuración



La configuración de la fase 1 y la fase 2 deben coincidir exactamente del sitio. Revise que la sección de este ejemplo para los detalles y figuras.

El último cambio es la configuración para mantener con vida (Figura 17.12, "Sitio B Keep Alive"). En esta configuración, se puede utilizar
la dirección IP de LAN del router pfSense en el Sitio A, 192.168.1.1.

Figura 17.12. Sitio B Keep Alive

Ahora haga clic en el botón Guardar y, a continuación, haga clic en Aplicar cambios en la pantalla de IPsec Túneles.

Al igual que con el Sitio A, también debe agregar reglas de firewall para permitir el tráfico en el túnel para cruzar desde el sitio A al Sitio B. Añadir estas reglas a la pestaña IPsec bajo Firewall Reglas. Para más detalles, consulte la sección llamada "IPsec y firewall reglas". Esta vez, el origen del tráfico sería del sitio, destino del sitio B.

Ambos túneles están configurados y deben estar activos. Compruebe el estado de IPsec visitando Estado IPsec. Usted debe ver una descripción del túnel junto con un icono indicador de su estado.

Si usted no ve un icono, puede haber un problema de establecer el túnel. Esto pronto, lo más probable es razón es que no hay tráfico ha intentado cruzar el túnel. Desde la red local incluye una dirección que el firewall tiene, verá un botón de conexión en esta pantalla que iniciará un ping a la distancia

la fase 2. Haga clic botónpara intente abrir el túnel, como se ve en la Figura 17.13, "sitio IPsec Status ". Si no aparece el botón de conexión, intente hacer ping a un sistema en la subred remota en el sitio B de un dispositivo dentro de la red local de la fase 2 en el sitio (o viceversa) y ver si el túnel se establece.
Mire la sección llamada "Prueba de IPsec Conectividad" otros medios de prueba de un túnel.

Figura 17.13. Sitio IPsec Estado

En su defecto, los registros de IPsec ofrecerán una explicación. Están ubicados en Estado Registros del sistema en la pestaña de IPsec VPN. Asegúrese de comprobar el estado y los registros en ambos sitios. Para más de solución de problemas
información, compruebe el la sección llamada sección "Solución de problemas de IPsec" más adelante en este capítulo.

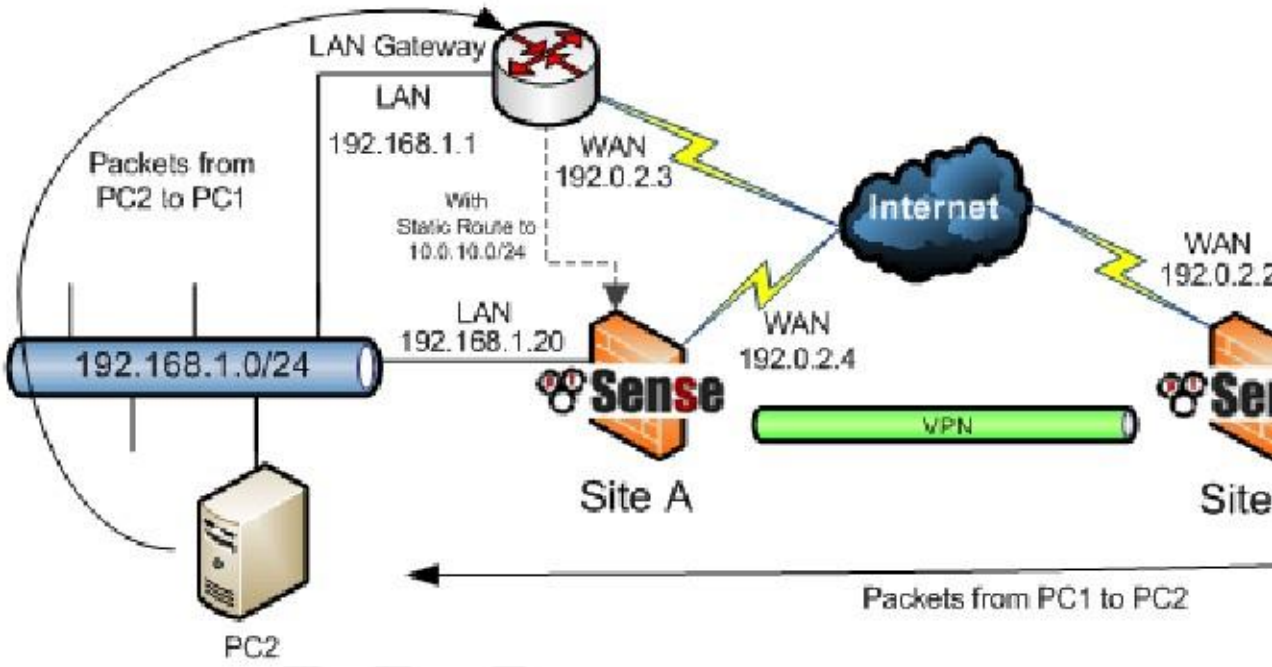
Consideraciones de enrutamiento y de puerta de enlace

Cuando el punto final de VPN, en este caso un router pfSense, es la puerta de enlace predeterminada para una red no debería haber problemas con el enrutamiento. Como un equipo cliente envía tráfico, pasará a la caja de pfSense, sobre el túnel, y por el otro extremo. Sin embargo, si el router es pfSense no la puerta de enlace predeterminada para un determinado
red, a continuación, tendrá que ser tomado otras medidas de encaminamiento.

Como ejemplo, imagine que el router pfSense es la puerta de enlace en el sitio B, pero no del sitio, como se ilustra En la Figura 17.14, "sitio para localizar IPsec Dónde pfSense no es la puerta de enlace". Un cliente, PC1 en el Sitio B envía
un ping a PC2 al sitio A. El paquete sale PC1, a continuación, a través del router de sitio B, al otro lado del túnel, la enrutador pfSense en sitio, y luego a la PC2. Pero lo que sucede en el camino de regreso? Puerta de entrada de PC2 es otro
un router por completo. La respuesta al ping será enviado a la puerta de enlace y muy probablemente se desechó, o peor aún, se puede enviar el enlace de Internet y se pierde de esa manera.
Hay varias maneras de evitar este problema, y cualquiera puede ser mejor en función de las circunstancias de un caso determinado. En primer lugar, una ruta estática se podía entrar en la puerta de enlace que redirigirá el tráfico destinado a la parte más alejada del túnel al enrutador pfSense. Incluso con esta ruta, adicional

complejidades se introducen porque este escenario da como resultado enrutamiento asimétrico como cubiertos en la sección llamada "Reglas de firewall bypass para el tráfico sobre la misma interfaz". Si eso no funciona, una estática ruta podría añadirse a los sistemas cliente de forma individual para que sepan que enviar tráfico directamente a la caja pfSense y no mediante la pasarela predeterminada. A menos que haya sólo un número muy pequeño de anfitriones que necesitan acceder a la VPN, este es un dolor de cabeza de gestión y deben evitarse. Por último, pero no menos importante, en algunas situaciones puede ser más fácil de hacer que el pfSense caja la puerta de entrada y se deja manejar
su conexión a Internet.

Figura 17.14. Sitio para localizar IPsec Dónde pfSense no es la puerta de enlace



Enrutamiento varias subredes a través de IPsec

Si usted necesita para enrutar múltiples subredes IP a través de IPsec, pfSense 2.0 permite la definición de múltiples subredes por conexión IPsec mediante la definición de una nueva entrada en la fase 2 para cada subred que desea ser capaz de
utilizar el servidor de seguridad. En las versiones anteriores 1.2.x aún puede hacerlo, pero no es lo más conveniente. Tienes
dos opciones - resumen CIDR y túneles IPsec paralelas.

> **Nota**
>
> El tráfico atravesará un túnel IPsec sólo si coincide con una entrada SAD existente. Las rutas estáticas voluntad no enrutar el tráfico a través de una conexión IPsec, nunca configurar rutas estáticas para cualquier IPsec
> tráfico excepto en el caso de tráfico iniciado desde sí pfSense (que se discutirá más adelante).

CIDR Summarization

Si las subredes son contiguas, se puede enrutar múltiples subredes en un túnel utilizando una subred más grande que incluye todas las subredes más pequeñas. Por ejemplo, si un sitio incluye las subredes 192.168.0.0/24 y 192.168.1.0/24, que se pueden resumir como 192.168.0.0/23. Vea la sección llamada "CIDR Recapitulación "para obtener más información.

Paralelos Túneles IPsec

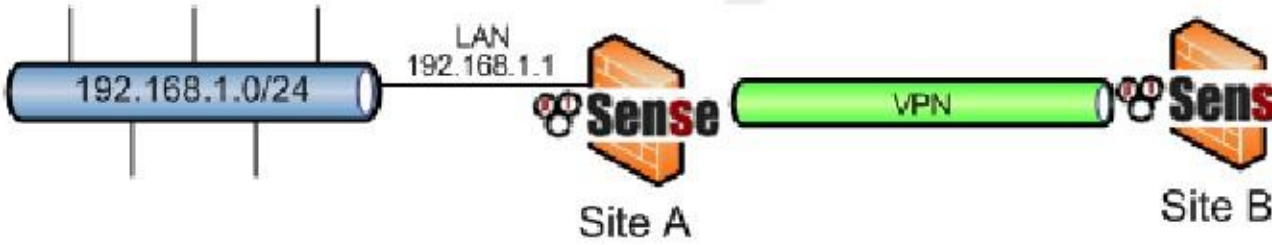
La única opción si las subredes no se resumen es crear túneles IPsec paralelos, uno para cada uno subred.

Haga clic the icon to la derecha de la primera conexión a añadir otra en función de ésta. Cambie 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.

iniciado por pfSense Tráfico e IPsec

Para tener acceso al extremo remoto de conexiones IPsec desde sí pfSense, tendrá que "falso" el sistema mediante la adición de una ruta estática que apunta la red remota a la IP LAN del sistema. Tenga en cuenta este ejemplo supone la VPN se conecta la interfaz LAN en ambos lados. Si la conexión IPsec se conecta una interfaz OPT, sustituir la interfaz y la dirección IP de la interfaz correspondiente. Porque de la forma en IPsec se ata en el kernel de FreeBSD, sin la ruta estática que el tráfico seguirá el tabla de enrutamiento del sistema, lo que probablemente envíe este tráfico a la interfaz WAN en lugar de sobre la Túnel IPsec. Tome la Figura 17.15, "sitio para localizar IPsec", por ejemplo.

Figura 17.15. Sitio para localizar IPsec



Usted necesita agregar una ruta estática en cada servidor de seguridad, que se realiza mediante la adición de una primera puerta de entrada de puntero a LAN IP del servidor de seguridad (Vea la sección llamada "Gateways") y, a continuación, añadir una ruta estática por medio de esta puerta de enlace (Ver la sección llamada "rutas estáticas"). Figura 17.16, "del sitio - ruta estática a distancia subred "y la Figura 17.17," Sitio B - ruta estática a la subred remota "mostrar la ruta que debe añadirse en cada lado.

Figura 17.16. Del sitio - ruta estática a la subred remota

Figura 17.17. Sitio B - ruta estática a la subred remota

IPsec móvil

Mobile IPsec le permitirá realizar una conexión llamada "Road Warrior" de estilo, el nombre del naturaleza variable de cualquier persona que no esté en la oficina que tiene que conectarse de nuevo a la red principal. Puede ser una persona de las ventas a través de Wi-Fi en un viaje de negocios, el jefe de su limusina por módem 3G, o una programador que trabaja desde su línea de banda ancha en casa. La mayoría de ellos se verán obligados a hacer frente a direcciones IP dinámicas, ya menudo ni siquiera saben la dirección IP que tienen. Sin un router o firewall apoyar IPsec, un túnel IPsec tradicional no funcionará. En escenarios de teletrabajo, es generalmente indeseable e innecesaria para conectar toda la red doméstica del usuario a la red, y presentará complicaciones de enrutamiento. Aquí es donde los clientes IPsec móviles vienen pulg

Sólo hay una definición para IPsec Mobile en pfSense, por lo que se estará preguntando cómo configurar varios clientes. En lugar de confiar en una dirección fija para el extremo remoto del túnel, IPsec autenticación a través xauth es posible permitir un inicio de sesión de usuario / contraseña para identificar a un usuario único. Este permite a los clientes a ser autenticados y distinguen entre sí.

Antes de empezar a configurar los clientes, usted tendrá que elegir un rango de direcciones IP que van a utilizar. Será necesario tener cuidado para que las direcciones IP no se solapan cualquier red existente; Las direcciones IP deben diferir de los que se utilizan en el lugar de alojamiento del túnel móvil, así como la LAN de la que el cliente se conecta. En este ejemplo, 10.50.99.0/24 se utilizará, pero puede ser en caso de suprimirse subred que desee.

Esto es diferente del estilo de IPsec móvil sugerido para 1.2.3, pero utilizando xauth es tanto más seguro y también permite conexiones desde los dispositivos móviles que funcionan con iOS y algunas versiones de Android. Además, pfSense 2.x admite empujando direcciones y otros ajustes a los clientes para la configuración automática.

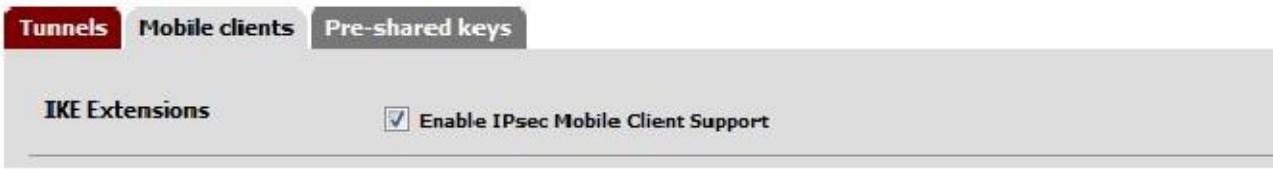
Ejemplo de configuración del servidor

Hay varios componentes en la configuración del servidor para clientes móviles: Ajuste del Cliente Móvil ajustes y la creación de la fase 1 y la fase 2 para la conexión del cliente, y la adición de reglas de firewall de IPsec. Después de eso, los usuarios deben ser añadidos con los permisos adecuados para utilizar la VPN.

Configuración del cliente móvil

En primer lugar, debemos permitir IPsec en el router si no lo ha hecho ya. Vaya a VPN IPsec, seleccione Habilitar IPsec, haga clic en Guardar. Con IPsec habilitada, el soporte de cliente móvil también debe estar encendido.
Desde VPN IPsec, haga clic en la pestaña de clientes móviles (Figura 17.18, "Habilitar clientes móviles IPsec"). Marque la casilla Soporte a Clientes Habilitar IPsec móvil y, a continuación, continúe con el siguiente conjunto de opciones.

Figura 17.18. Habilitar los clientes móviles de IPsec



Como queremos XAUTH y queremos utilizar el gestor de usuarios pfSense para la autenticación, podemos dejar las fuentes de autenticación establece en Sistema, como se ve en la Figura 17.19, "Autenticación clientes móviles".

Figura 17.19. Autenticación de clientes móviles

Nuevo en pfSense 2.x es la capacidad de enviar los ajustes al cliente para cosas como la IP del cliente y DNS. Estas opciones se muestran en la Figura 17.20, "clientes móviles empujado Settings".

La Dirección Virtual Pool define el pool de direcciones IP que será entregado a los clientes. Usaremos 10.50.99.0/24 en este ejemplo.

La opción Lista de Redes controla si el cliente intentará enviar todo su tráfico a través de la túnel o sólo el tráfico para redes específicas. Si esta opción está activada, las redes definidas en las opciones de red local para las 2 definiciones de fase móvil se envían al cliente. Si esta opción no esté marcada, los clientes intentarán enviar todo su tráfico, incluyendo el tráfico de Internet, a través de la túnel. No todos los clientes respetan esta opción. Sólo queremos que el cliente para llegar a la red en nuestra fase 2 para este ejemplo, por lo que se marque esta opción.

Si se comprueba Guardar Xauth contraseña, los clientes que apoyan este control permitirá al usuario guardar su credenciales. Esta es respetado principalmente por los clientes basados en Cisco como la hallada en iOS y Mac OSX. Para este ejemplo, queremos permitir que la conducta, por lo que el cuadro se comprobará.

Si marca DNS dominio predeterminado y especificar un valor, entonces este valor será empujado a los clientes como su sufijo de dominio predeterminado para las peticiones DNS. Por ejemplo, si se establece en example.com y un cliente peticiones el anfitrión, a continuación, la solicitud de DNS se intentará para host.example.com.

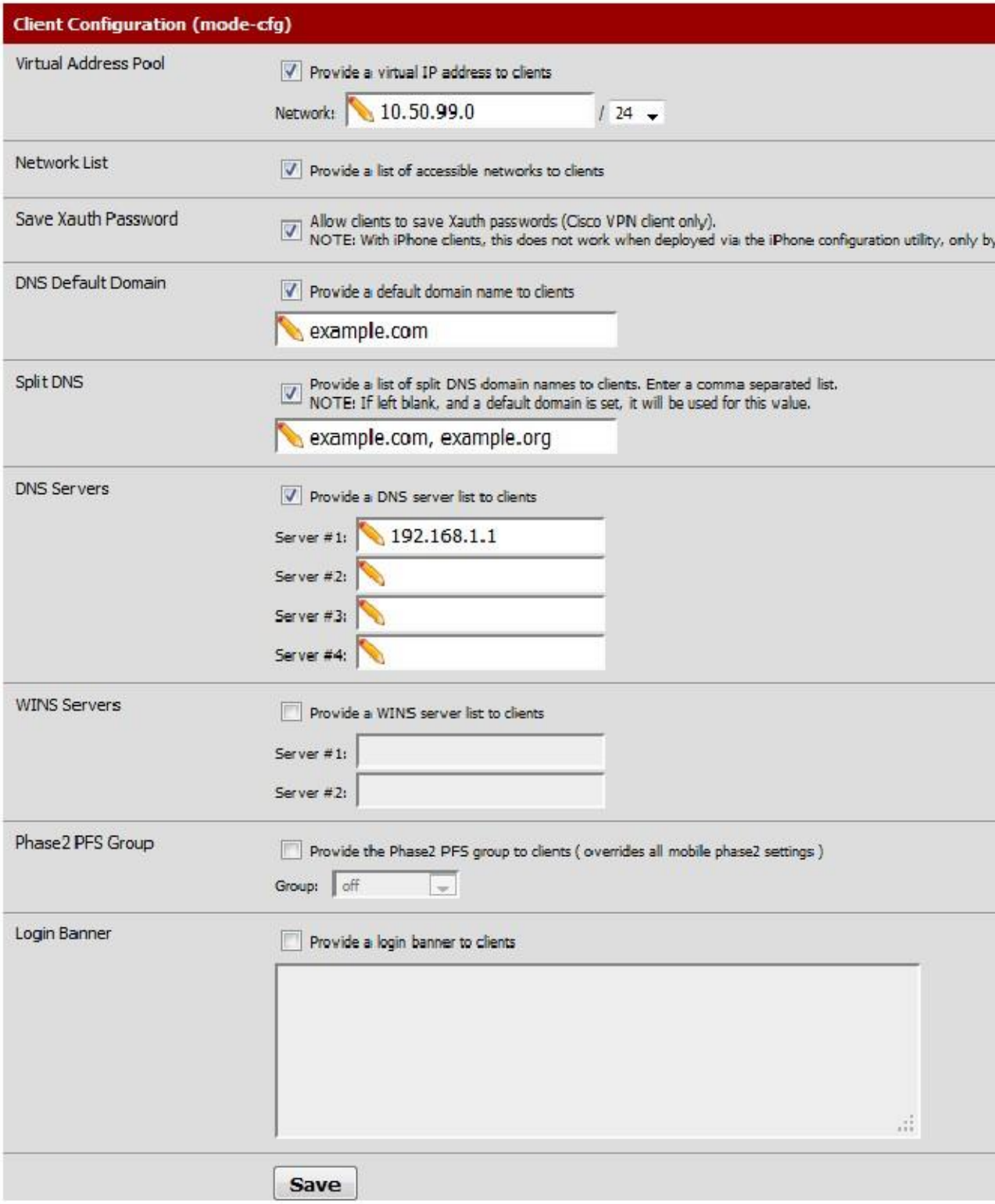
La opción Dividir DNS controla la forma en que el cliente envía peticiones DNS en el servidor DNS proporcionado (si los hay). Si esta opción no está seleccionada, el cliente deberá enviar todas sus peticiones DNS a un servidor DNS proporcionado.
Si la opción está marcada, pero deja en blanco, y un defecto DNS del dominio se configura, entonces sólo las peticiones de que
nombre de dominio irá al servidor DNS proporcionado. Si está marcada y se introduce un valor, entonces sólo solicitudes de dominio (s) introducida en el cuadro serán remitidos al Servidor DNS proporcionado. En nuestra ejemplo, tenemos tanto example.com y example.org y quiere peticiones DNS para los dos
dominio para ir a nuestros servidores, por lo que entrar en esos valores aquí separados por una coma.
Puede proporcionar los servidores DNS a los clientes mediante la comprobación Proporcione una lista de servidores DNS a los clientes, y entrando
Las direcciones IP de los servidores DNS locales, como 192.168.1.1.

Nota

Si tiene la intención de sus clientes móviles de la ruta a la Internet a través de la VPN, debe asegurarse los clientes obtienen un servidor DNS del cortafuegos utilizando esta opción, y que no tienen Habilitado DNS dividido. Si no se configura de esta manera, los clientes intentarán conseguir DNS de cualquier servidor al que fueron asignados por su ISP, pero enrutar la solicitud a través del túnel y es muy probable que falle.

También puede proporcionar servidores WINS, establezca el PFS Grupo Fase 2, e incluso mostrar una sesión en Banner clientes, pero para este ejemplo no vamos a utilizar esos, por lo que queda fuera.

Figura 17.20. Clientes móviles empujado Configuración



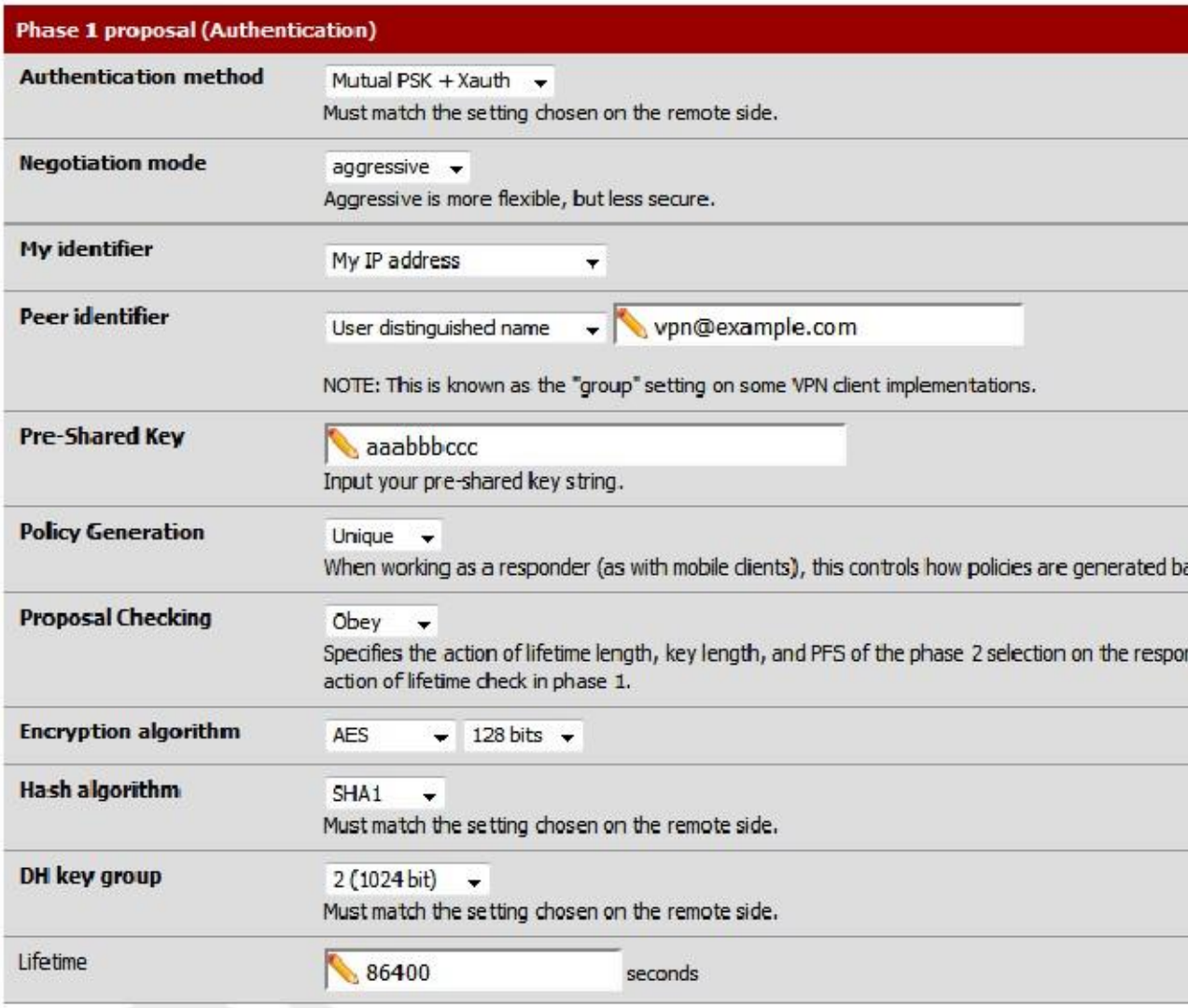
Después de guardar la configuración en la ficha Clientes móviles, pfSense le advertirá de que usted no se tiene un fase 1 definición para sus clientes móviles. Pulse el botón Crear Fase 1 para hacer uno y comenzar el siguiente paso (Figura 17.21, "los clientes móviles de la Fase 1 Creación del sistema").

Figura 17.21. Los clientes móviles de la Fase 1 Creación Prompt

Ahora vemos fase 1 ajustes para clientes móviles. Para empezar, el método de autenticación debe establecer en Mutual PSK + Xauth ya que tenemos la intención de usar esto de Android y iOS. Estos operativo sistemas tienen una peculiaridad especial ya que requieren valores muy específicos para el cifrado, hash, tiempos de vida, y así sucesivamente. Es importante que si usted desea utilizar IPsec móvil con Android o iOS que establecer los valores tal y como se muestra en la Figura 17.22, "los clientes móviles de la Fase 1" y la Figura 17.23, "Mobile
Clientes Fase 2 ".

En primer lugar, establecer agresivo para el modo de negociación. Los clientes se conectan desde azar / IPs dinámicas así que esto permitirá el uso de un tipo de identificador personalizado para el remoto lugar de la dirección IP.
Uso Mi dirección IP para la opción Mi identificador es el mejor. El identificador del par también se conoce como el nombre del grupo en ciertas configuraciones de cliente, que se ponga esto en un tipo de Usuario distinguido nombre, y luego entrar en nuestro identificador, vpn@example.com. Usted puede utilizar su propio identificador de encargo,
sólo tienes que seguir ese formato. El Pre-Shared Key, también citada por algunos clientes como la clave de grupo, en caso de
ser una cadena aleatoria razonablemente fuerte, sin duda, mucho más fuerte que nuestro ejemplo de aaabbbccc.
Con el fin de garantizar adecuadamente que el tráfico de vuelta a los clientes funciona correctamente, asegúrese de que la política de
Generación se establece en Unique. Con el fin de garantizar que la fase 1 de la negociación no tenga problemas, establecer
Propuesta Comprobando Obedecer.
El algoritmo de cifrado se debe establecer en AES con una longitud de clave de 128 bits. El Algoritmo de Hash debe establecerse en SHA1. El grupo de claves DH se debe establecer en 2 (1024 bits). El curso de la vida debe ser ajustado a 86400.

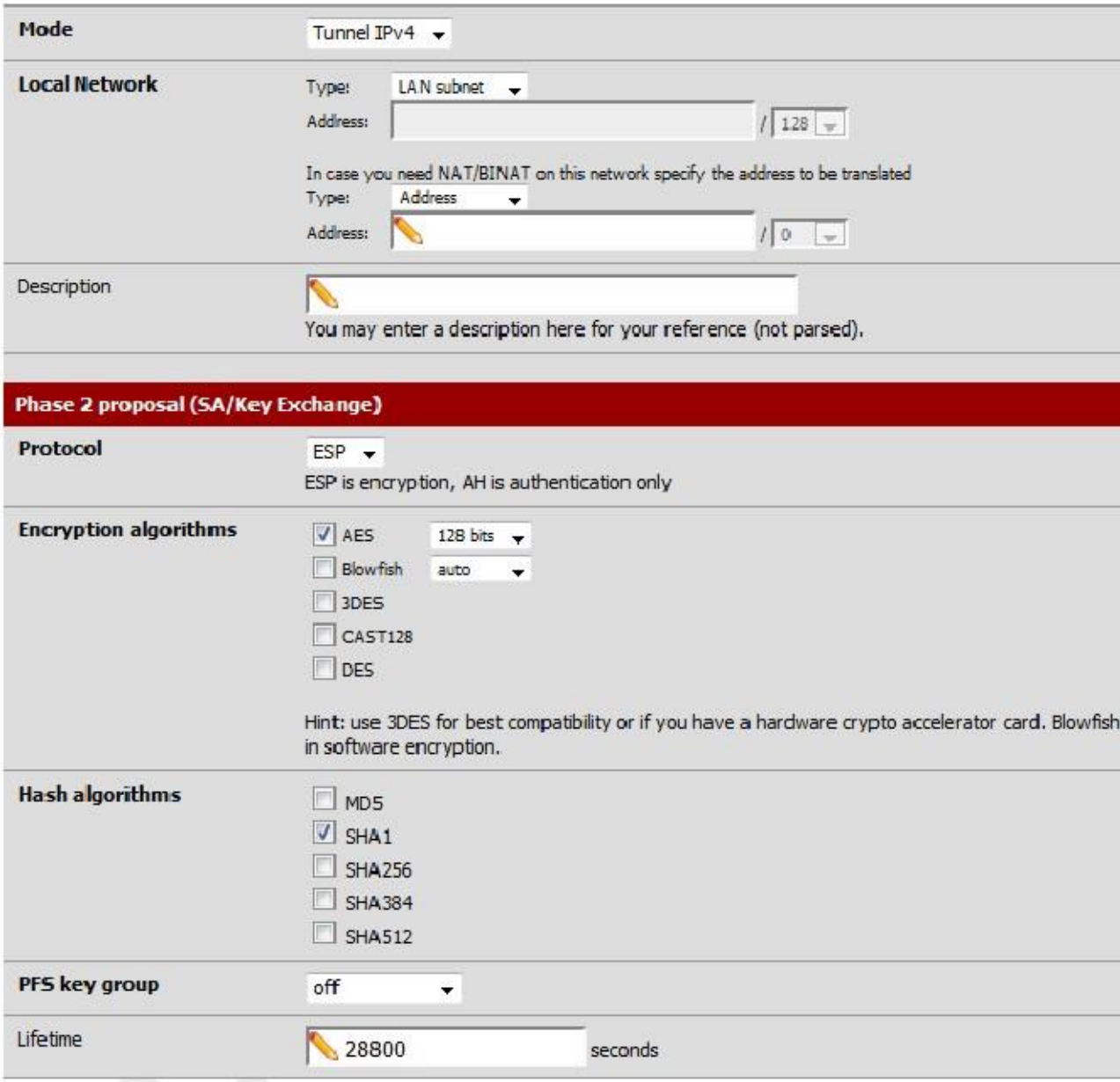
Figura 17.22. Los clientes móviles de la Fase 1



Ahora puede pulsar en Guardar para completar la configuración de la fase 1. A continuación, agregue una fase 2 y comenzar ese
parte de la configuración.

Figura 17.23, "los clientes móviles de la Fase 2" muestra la fase 2 opciones para este túnel móvil. El Modo se debe establecer en Túnel IPv4. La Red Local debe establecerse en Subred LAN o en otro local, red. La configuración de NAT se debe dejar en Ninguno. El Protocolo debe establecerse para ESP, que se cifrar un túnel de tráfico. Los algoritmos de cifrado para la fase 2 se deben establecer en AES de 128 bits, solamente. Para Los algoritmos hash, sólo se puede seleccionar SHA1. PFS deben estar off. El curso de la vida necesita ser 28800. Ahora haga clic en Guardar y continuar.

Figura 17.23. Los clientes móviles de la Fase 2



Después de hacer clic en Guardar, los ajustes deben aplicarse antes de que surtan efecto. Haga clic en Aplicar cambios (Figura 17.24, "Aplicar Mobile Configuración de túnel") y luego la configuración del túnel para los clientes móviles es completo.

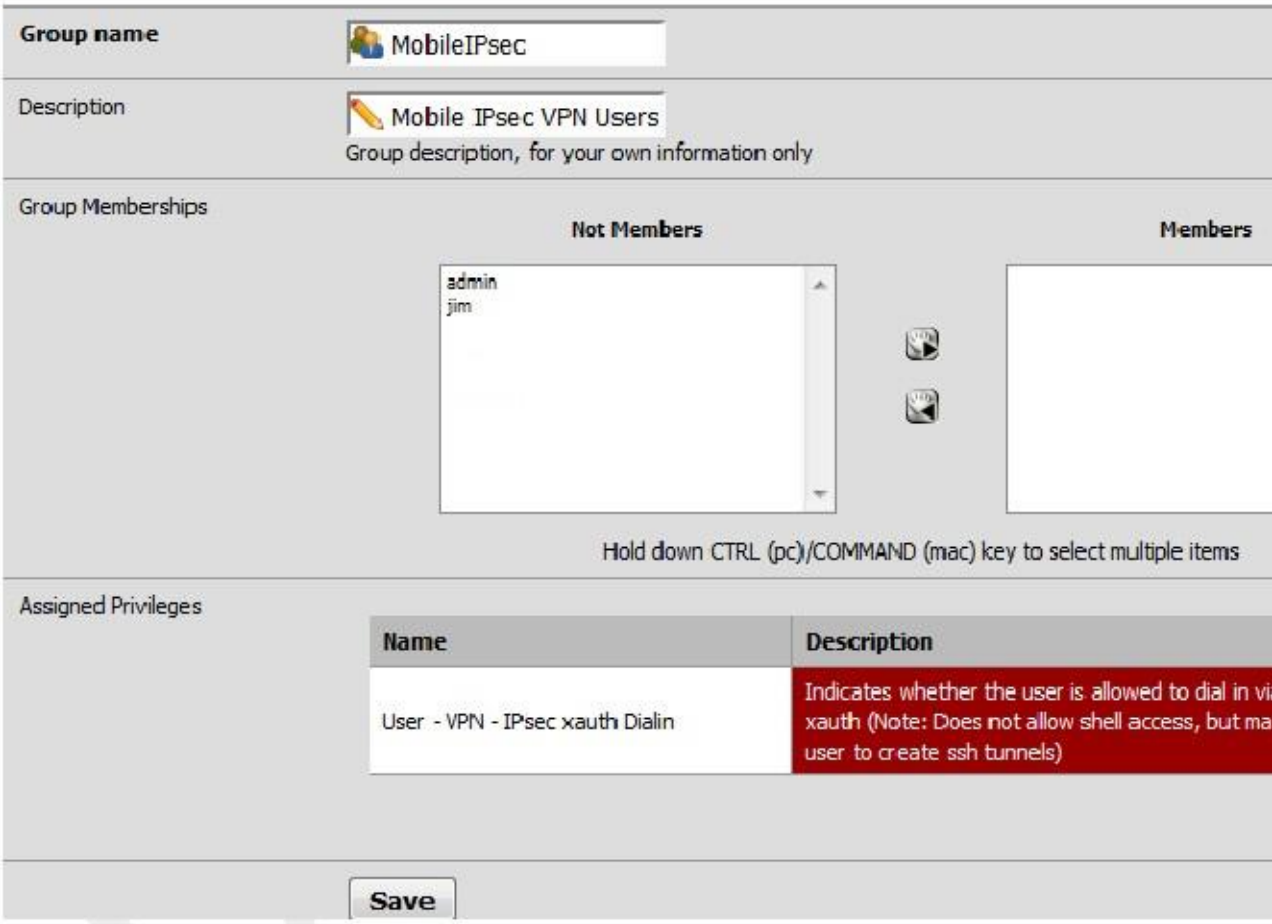
Figura 17.24. Aplicar Configuración de túnel Mobile

Mobile IPsec Creación del usuario

El siguiente paso para la configuración de IPsec móvil es agregar los usuarios que pueden autenticación a través xauth. Como nos
tendrá múltiples usuarios, tiene sentido contar con un grupo de IPsec que tener el permiso necesario
para conectar a la VPN.

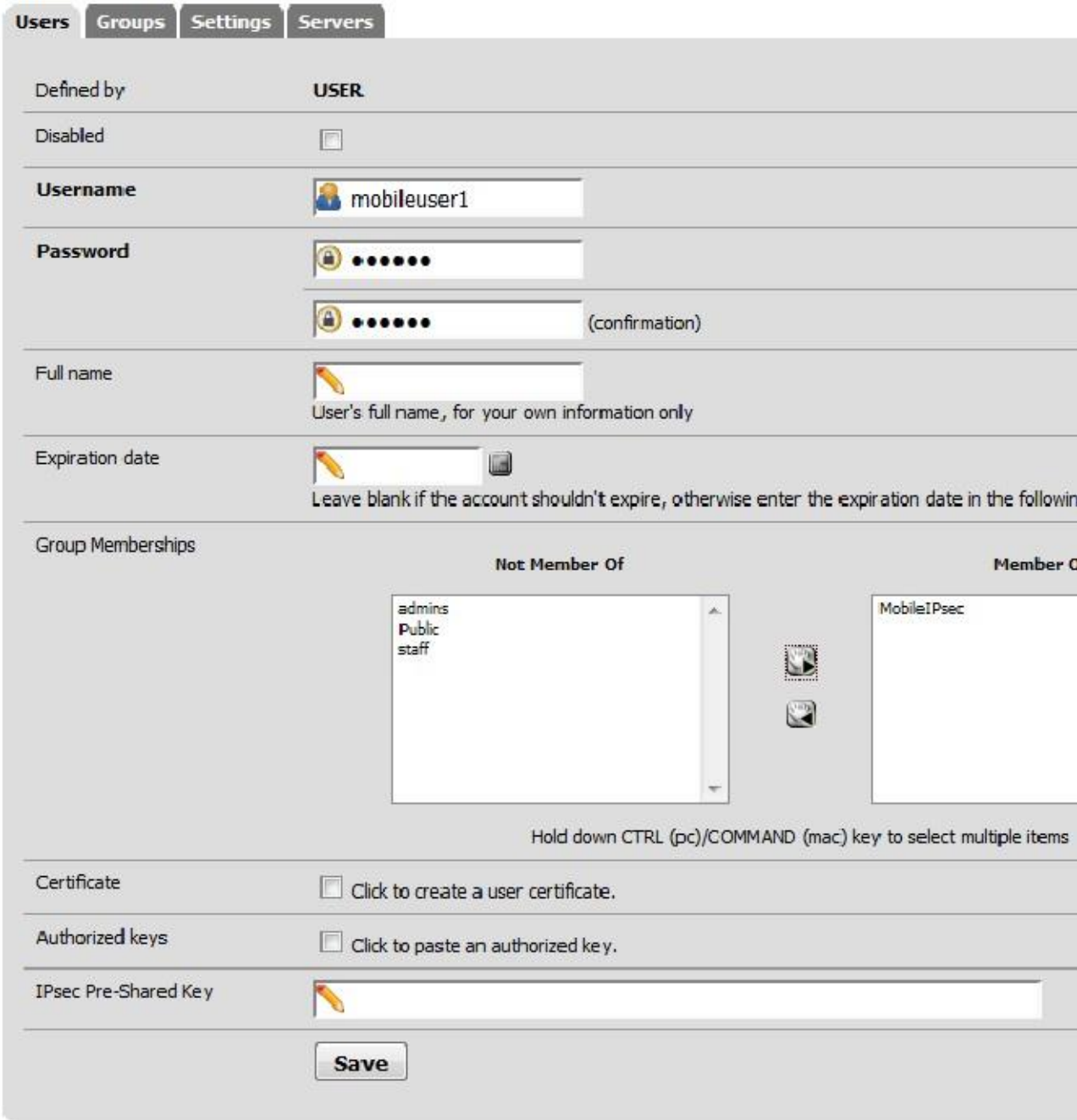
Para configurar el grupo, primero vaya a Sistema Administrador de usuarios en la ficha Grupos. Clickto crear una nueva
grupo, establezca el Nombre de grupo para MobileIPsec, y escriba una descripción como IPsec móvil
Los usuarios de VPN, a continuación, pulse Guardar para editar el grupo, así que podemos agregar sus permisos. Bajo Ahora haga clic en
Privilegios asignados, haga clic en, y de la lista, haga clic una vez en Usuario - VPN - IPSec xauth
Dialin, a continuación, haga clic en Guardar. Ahora tenemos un grupo para nuestros usuarios. El resultado final del grupo debe mirar
como en la Figura 17.25, "Mobile IPsec grupo de usuarios".

Figura 17.25. Mobile IPsec grupo de usuarios



Ahora tenemos que crear los usuarios para la VPN. En System Administrador de usuarios en la ficha Usuarios, haga clic en
para agregar un nuevo usuario. Introduzca un nombre de usuario, por ejemplo, mobileuser1. Introduzca una contraseña y vuelva a introducirla para
confirmarla. En la lista de miembros en el grupo, haga clic en MobileIPsec, y luego haga clic en el botón para mover al Miembro de lado. Luego haga clic en Guardar. Repita tantas veces como sea necesario para los usuarios de VPN. La usuario completa se muestra en la Figura 17.26, "El usuario móvil IPsec".

Figura 17.26. Mobile IPsec usuario



Reglas de cortafuegos

Al igual que con los túneles estáticos de sitio a sitio, túneles móviles también necesitarán reglas de firewall agregadas al IPsec
pestaña bajo Firewall Reglas. En este caso, el origen del tráfico sería la subred que ha elegido para los clientes móviles (o las direcciones de sus redes remotas), y el destino será su LAN red. Para más detalles, la sección llamada "IPsec y las reglas del cortafuegos".

Ejemplo de configuración de cliente

Cada equipo cliente móvil tendrá que ejecutar algún tipo de software de cliente de IPsec. Hay muchos diferentes clientes IPsec disponibles para su uso, algunos gratuitos y algunas aplicaciones comerciales. Típicamente IPsec es un protocolo bastante interoperable cuando se trata de túneles de enrutador a enrutador, pero los programas cliente
han demostrado ser más voluble, o en ocasiones incorporar extensiones propietarias que no son compatibles con

implementaciones de IPsec basadas en estándares. Como se mencionó antes, el cliente de Cisco IPsec incluye con la iPhone y iPod Touch no es compatible con pfSense IPsec, y el cliente proporciona para la conexión para cajas de fuegos de Watchguard ha visto resultados mixtos también.

Android Mobile IPsec

Soporte Android para IPsec para conectar con pfSense 2.x varía de una versión a otra. Muchos Motorola teléfonos como el Droid X y Droid RAZR línea han tenido IPsec para varias versiones, en el caso del Droid X, ya Gingerbread (Android 2.3.x) fue puesto en libertad. Más dispositivos consiguieron apoyo en 4.x. Android Esta sección cubre las dos formas más comunes para configurar una conexión IPsec para la ejemplo del servidor, dependiendo de la implementación de IPsec de su dispositivo. Ninguno de estos brindarle apoyo la lista de redes conectadas desde el servidor, y por lo tanto se debe definir la lista de redes para IPsec en la configuración del dispositivo.

Siga el conjunto de direcciones que mejor coincida con su dispositivo.

Nota

Debido a que Android considera usar una VPN una acción que debe ser seguro, el sistema operativo le obligará que usted utilice algún tipo de bloqueo para el dispositivo con el fin de proteger la configuración de VPN. Lo no importa qué tipo de bloqueo que usted elija (bloqueo de PIN, Patrón de bloqueo, contraseña, etc) pero no te deja configurar una VPN hasta que se ha añadido un cierre de seguridad. En los dispositivos Android 4.x con la cerradura de la cara, que no está disponible como un tipo de bloqueo de seguridad.

Motorola Estilo móvil Android IPsec

Desde la pantalla principal, pulse el botón Menú y luego Configuración, Red & Wireless, VPN (figura 17.27, "Motorola Android IPsec - Menú Red"), y por último avanzada IPsec VPNs (Figura 17.28, "Motorola Android IPsec - VPN del menú").

Figura 17.27. Menú Red - Motorola Android IPsec

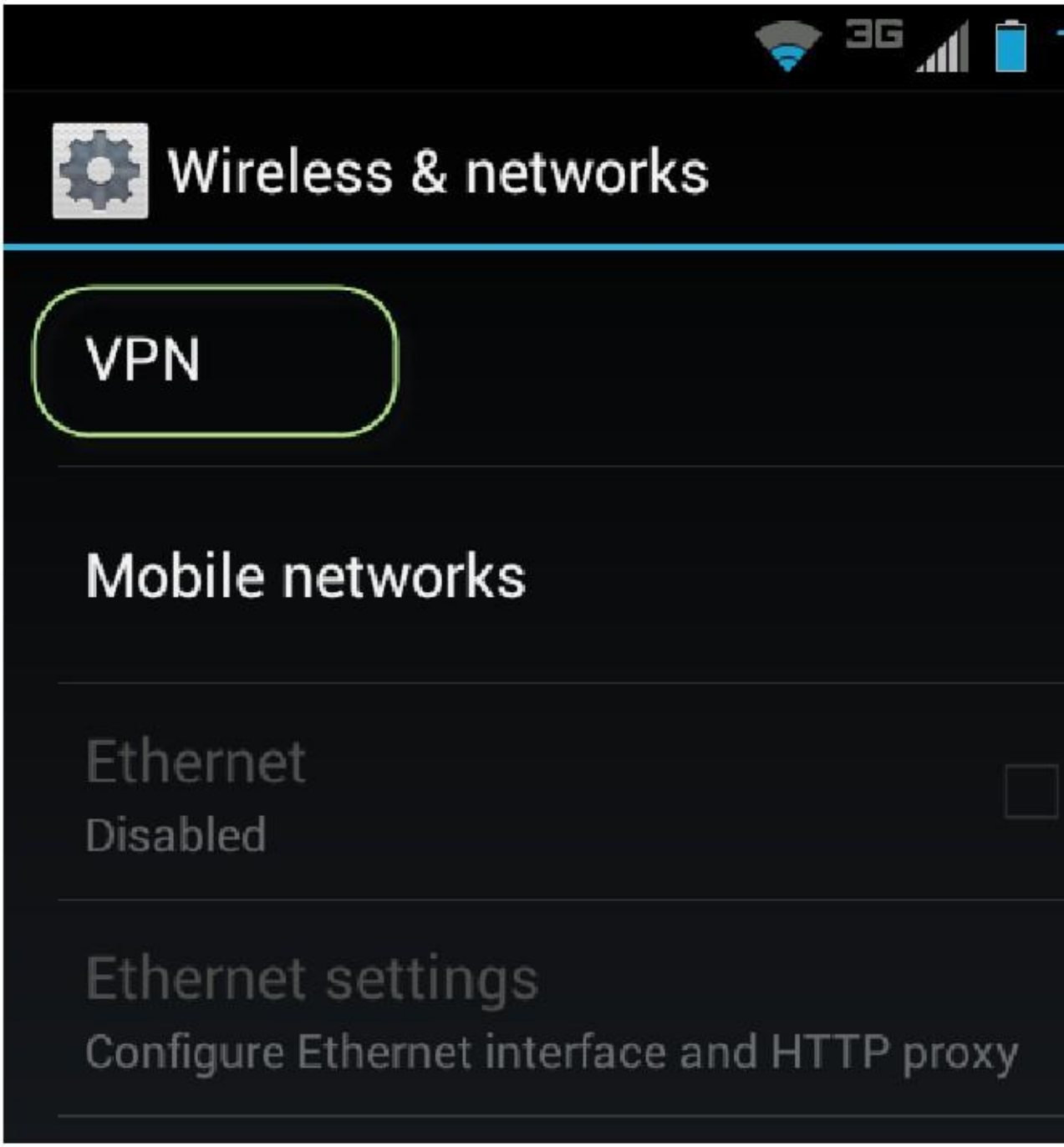
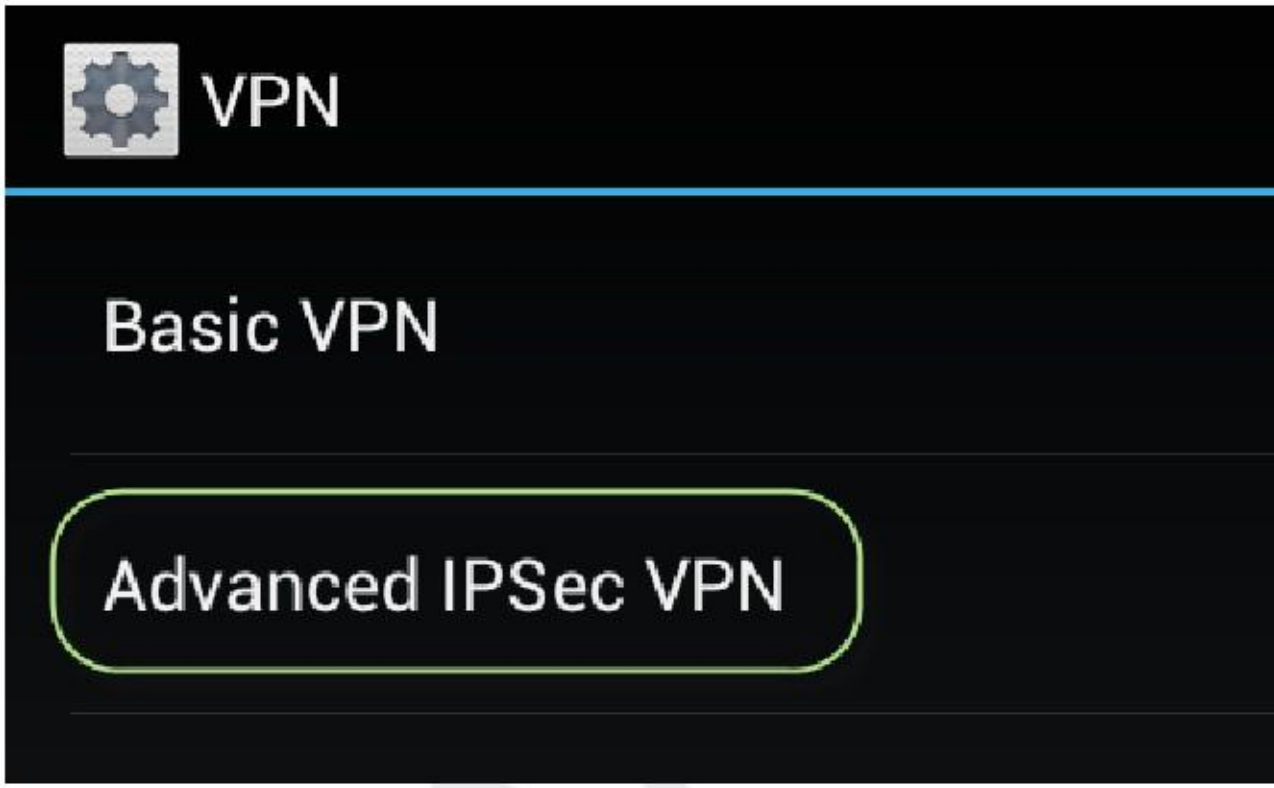


Figura 17.28. Motorola Android IPsec - Menú VPN



Pulse en Añadir VPN IPsec. Si esta opción no aparece, pulse el botón Menú y luego pulse en Añadir.

Se presenta una lista de tipos de IPsec VPN, como se muestra en la Figura 17.29, "Motorola Android IPsec - IPsec Lista de Tipo ", de esta lista, elija v1 PSK (AES, xauth, agresivo).


Certificate based, IKE V1 AES encryption
Certificate v1 (AES, xauth)
Certificate based, IKE V1 AES encryption, xauth
Certificate v2 (AES)
Certificate based, IKE V2 AES encryption
L2TP Certificate v1 (AES)
Certificate based, IKE V1 AES encryption L2TP/ IPSec
L2TP PSK v1 (AES)
Pre-shared key based, IKE V1 AES encryption L2TP/IPSec
PSK v1 (AES, aggressive)
Pre-shared key based, IKE V1 AES encryption, aggressive mode
PSK v1 (AES, xauth, aggressive)
Pre-shared key based, IKE V1 AES encryption, xauth, aggresive mode

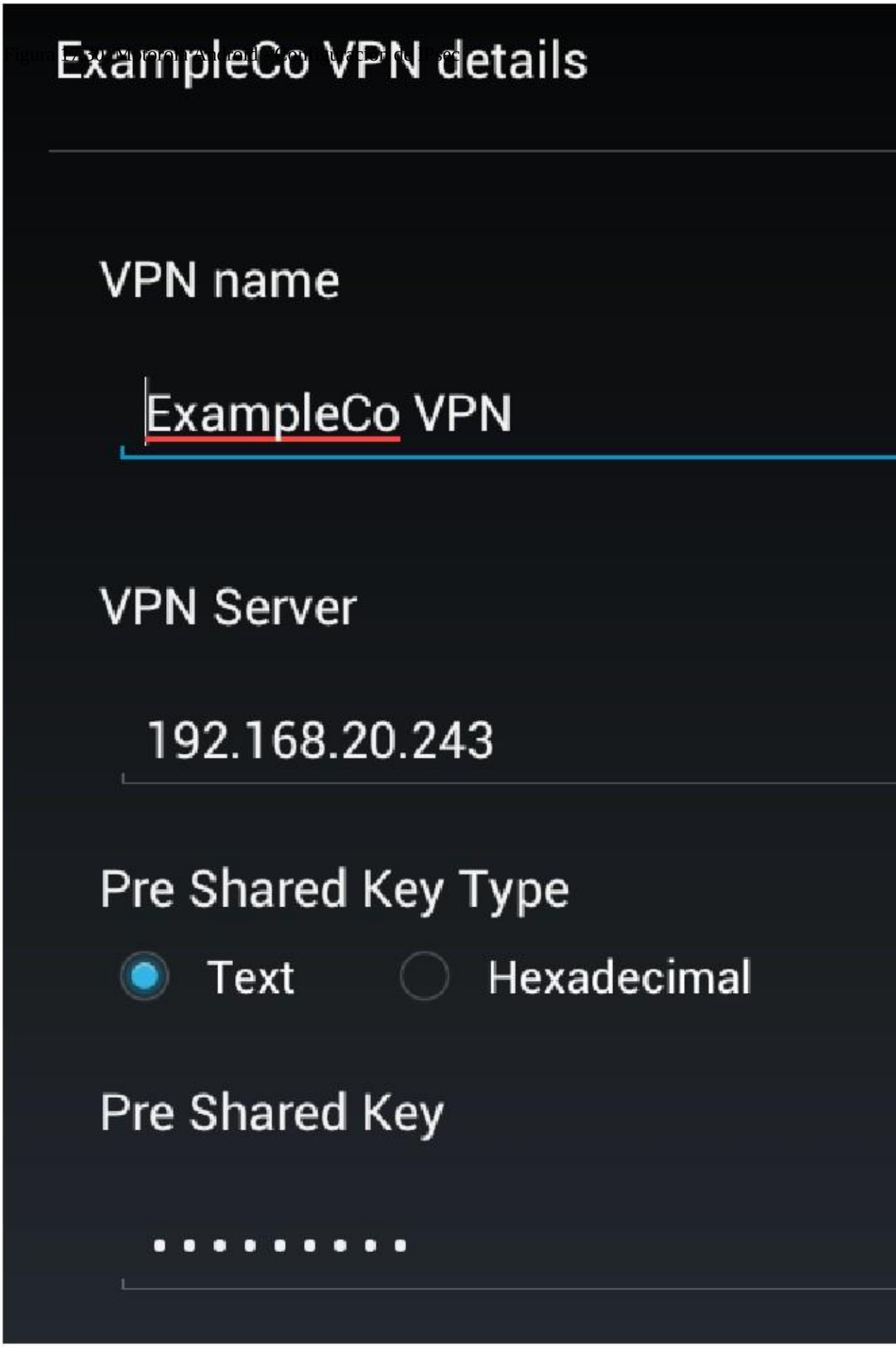
Para el Nombre de VPN, escriba una descripción de este VPN, como ExampleCo VPN.

El valor de servidor VPN debe ser la dirección IP del servidor, como 192.168.20.243.

Para Pre Shared Key Type, seleccione Texto, a continuación, introduzca la clave previamente compartida, que en este ejemplo es
aaabbbccc.

Estos valores se muestran en la Figura 17.30, "Motorola Android IPsec - Configuración".

Figura 7.30: Motorola Android - Configuración de IPsec



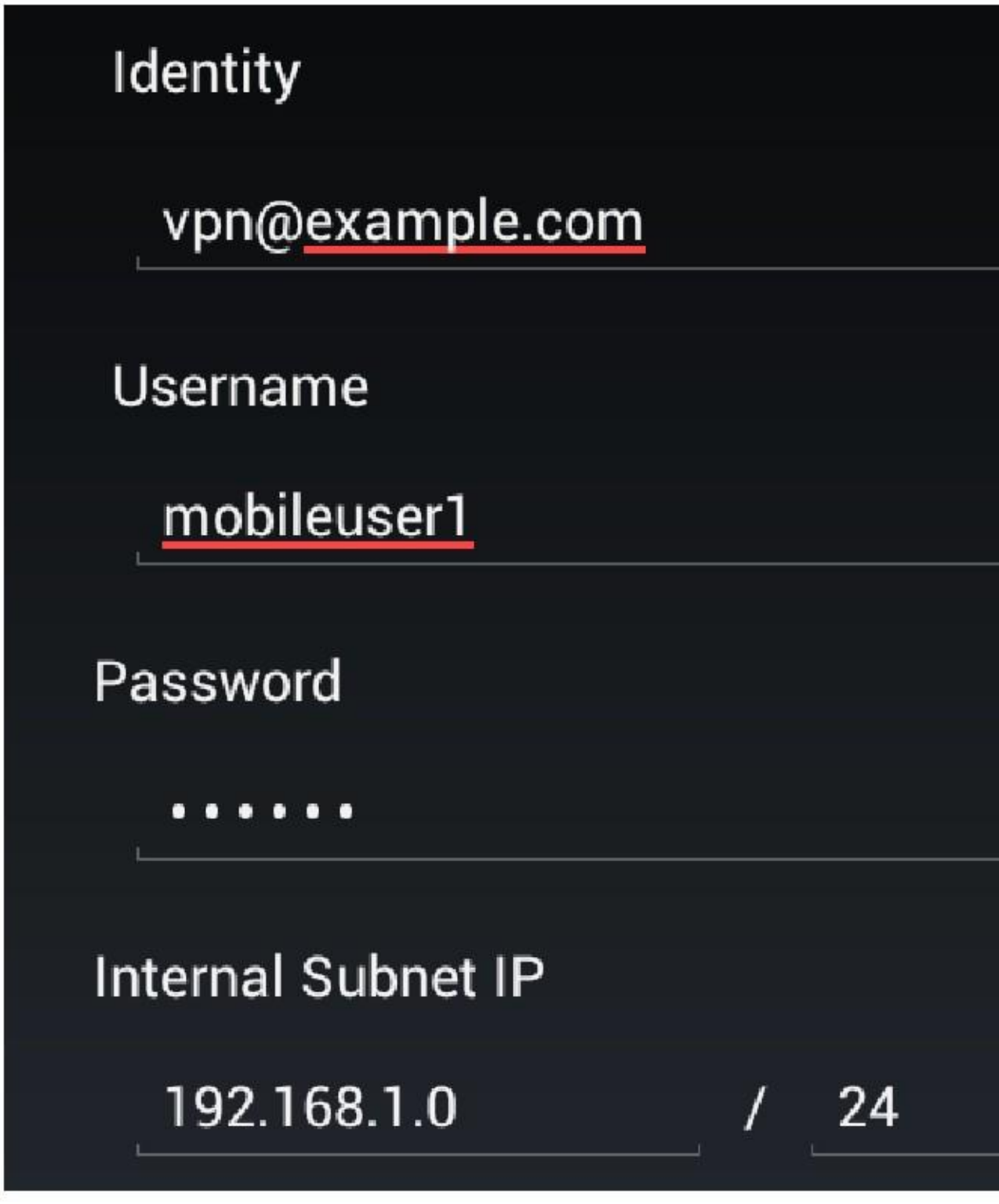
El tipo de identidad debería ser Usuario FQDN, y luego introduzca el identificador del par de los ajustes de fase 1. En este ejemplo, es vpn@example.com.

Introduzca el nombre de usuario y contraseña para la VPN si usted los quiere ser salvado.

Introduzca la subred IP interna, que es la subred que se alcance sobre el VPN. En este ejemplo, 192.168.1.1. Usted puede introducir hasta cuatro subredes.

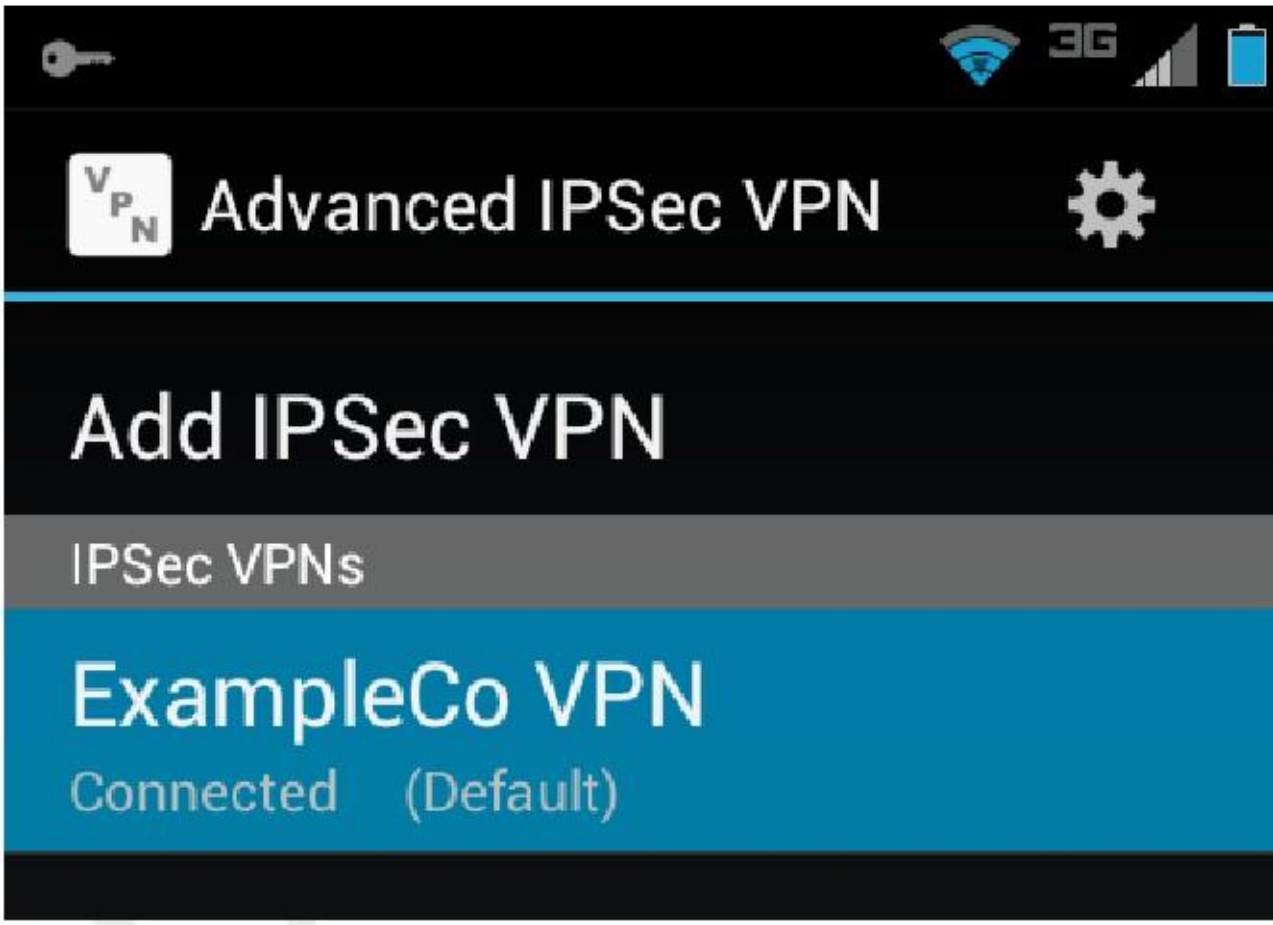
Estos valores se muestran en la Figura 17.31, "Motorola Android IPsec - Configuración (continuación)".

Figura 17.31. Motorola Android IPsec - Configuración (continuación)



Pulse Guardar y volverá a la lista de VPN. Si toca el nombre de VPN en la lista, lo hará
intentar una conexión VPN. Si tiene éxito, que se verá como en la Figura 17.32, "Motorola Android IPsec
- Conectado ". Un icono de la llave aparece en la barra de estado para mostrar que la VPN está conectado. Usted puede
desconectar pulsando sobre el nombre de VPN en la lista, o deslizando hacia abajo la barra de notificaciones y luego
pulsando en la entrada VPN en la lista de notificación para ver la ventana de estado, que también contiene una
desconexión
botón. Para editar o eliminar la VPN, pulsación larga sobre el nombre en la lista y elegir la acción deseada
en el menú.

Figura 17.32. Motorola Android IPsec - Conectado



Android 4.x general Estilo móvil IPsec

En Android 4.x, un método de configuración diferente puede estar disponible si el estilo anterior no estaba allí.

Para empezar, introduzca los ajustes del sistema. Esto varía entre los teléfonos y tabletas, pero podría ser o bien a través de la
Botón Menú si usted tiene uno, o tocando / arrastrando el área de notificación y luego presionando la configuración
icono allí. Por ejemplo, en un Asus Transformer Prime corriendo Jelly Bean (4.1.x Android), toca
el reloj, y luego el icono de engranaje.

En Inalámbrico y redes, pulse Más. ... y luego Añadir perfil VPN.

Para el nombre, escriba una descripción de este VPN, como ExampleCo VPN.

En la lista Tipo, elija IPsec Xauth PSK, como se muestra en la Figura 17.33, "4.x androide IPsec -
Tipos de VPN ".

Figura 17.33. Tipos de VPN - Android 4.x IPsec

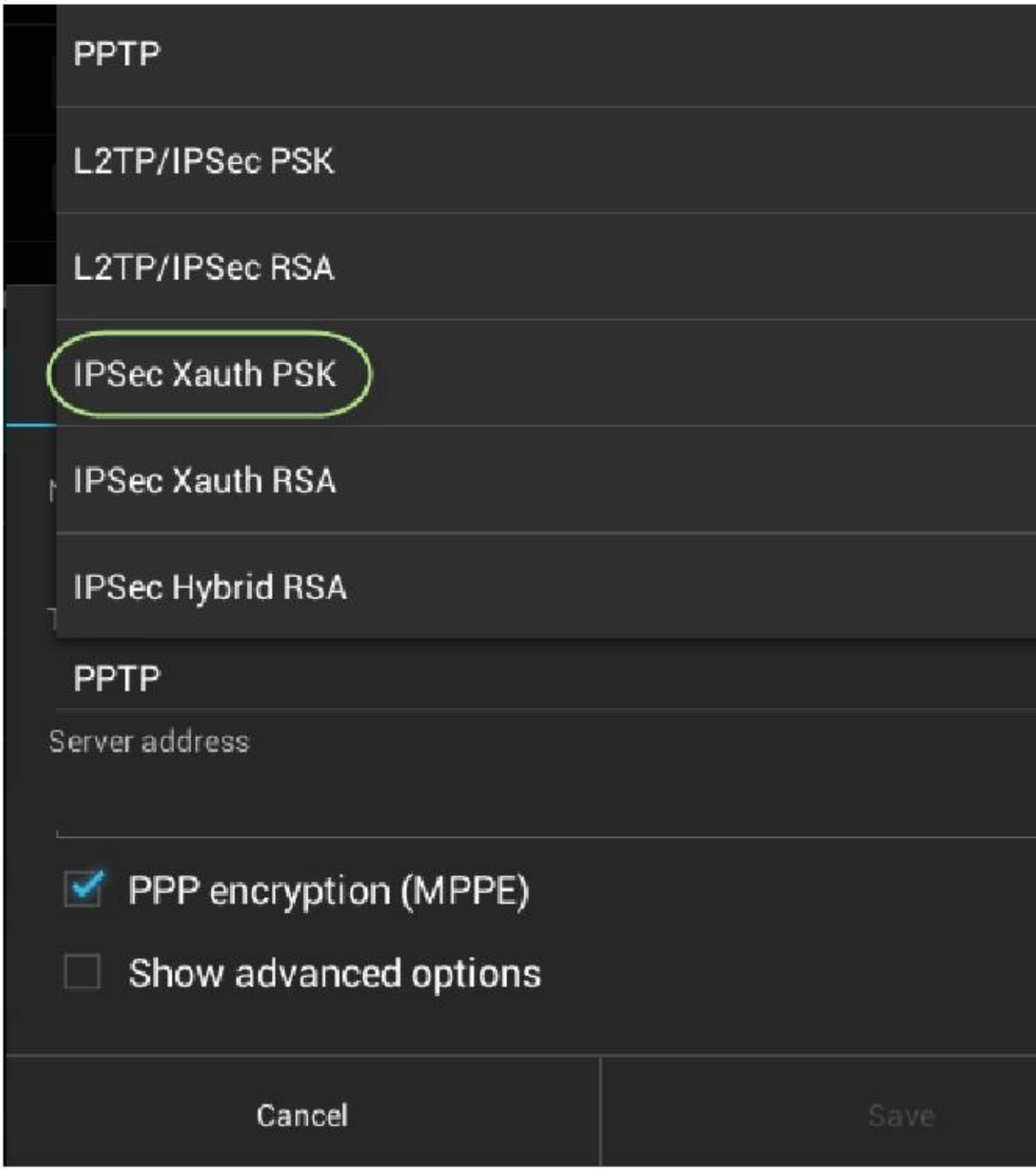
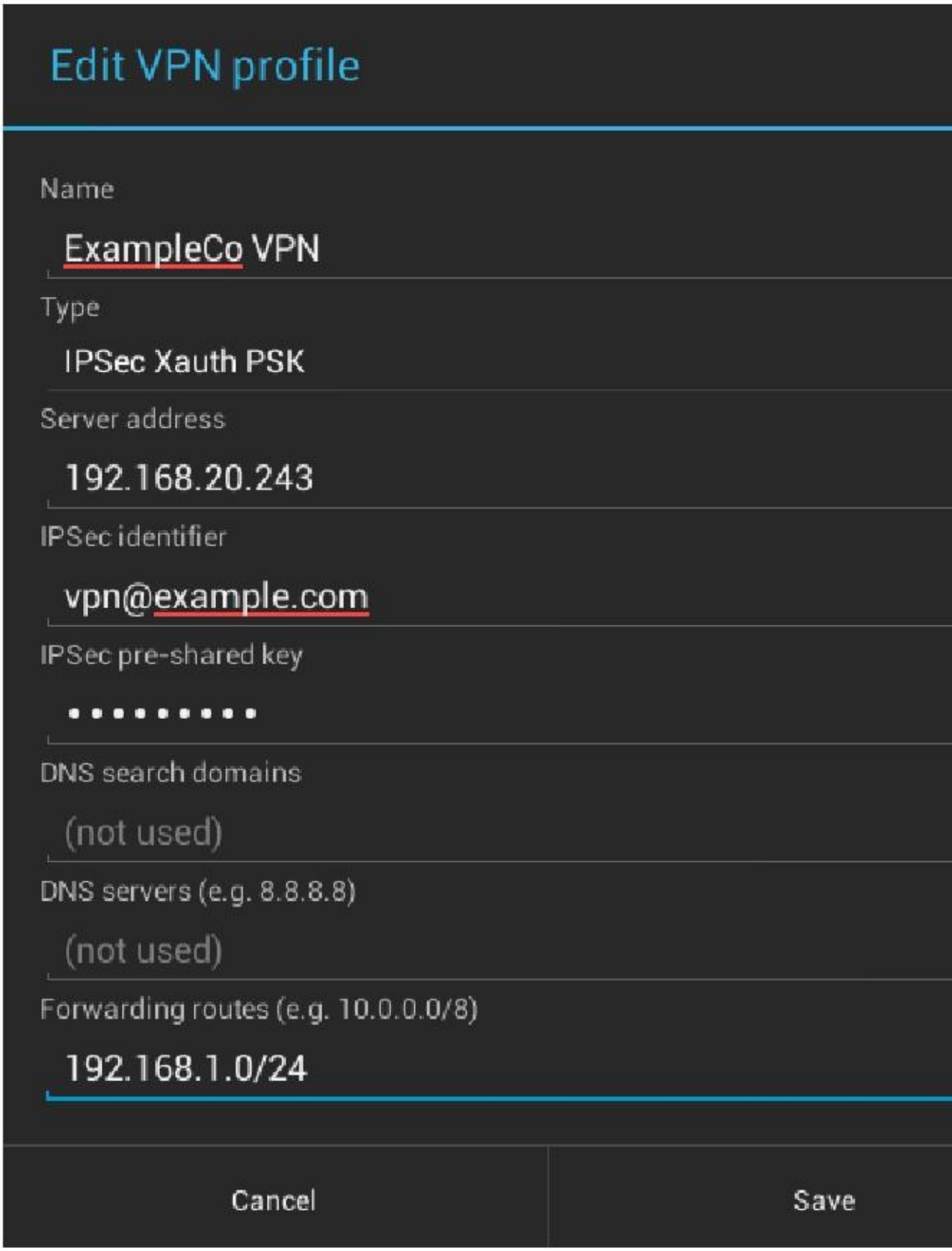


Figura 17.34. Android 4.x IPsec - Configuración IPsec



A continuación, introduzca el resto de la configuración de la VPN, como se ve en la Figura 17.34, "Android 4.x IPsec - IPsec
Configuración ". Para el identificador de IPsec, el identificador del par de la fase 1 ajustes. En este ejemplo, es vpn@example.com.

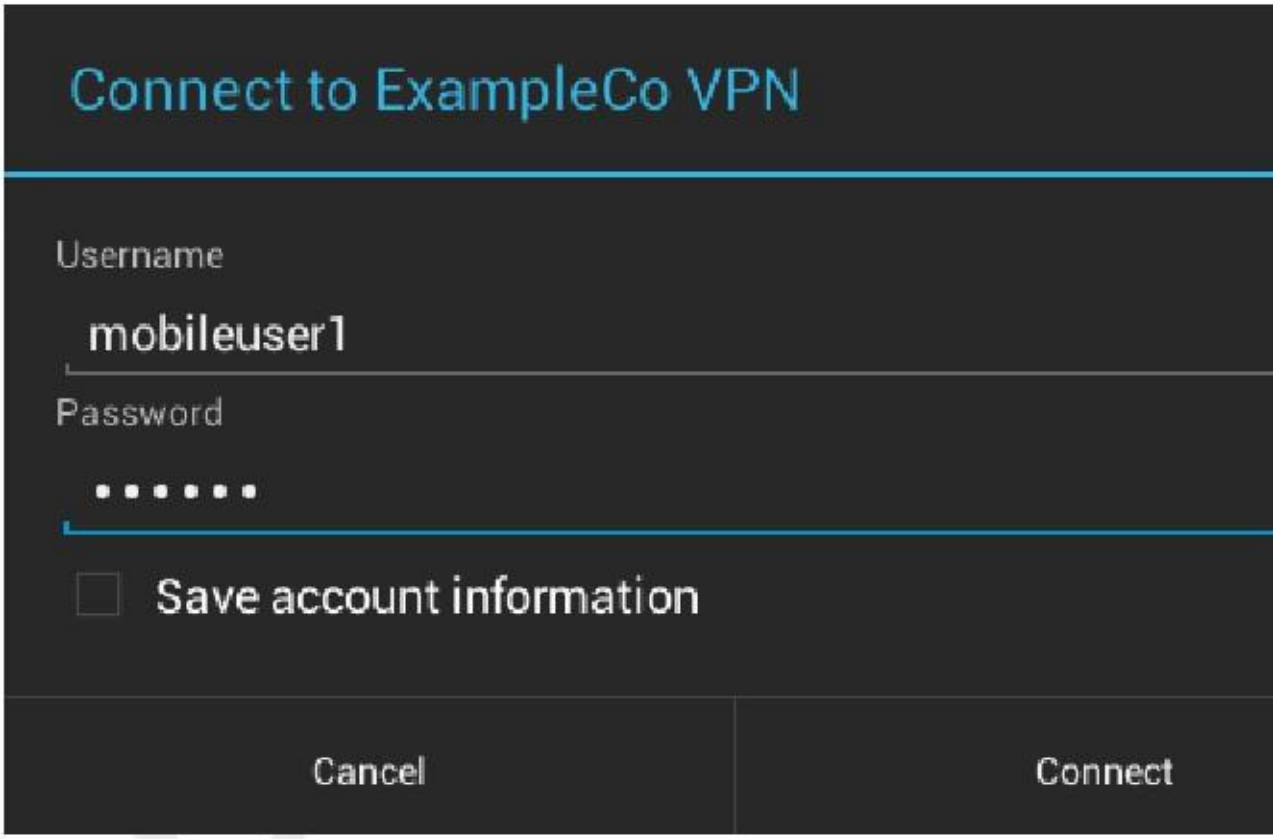
A continuación, introduzca la clave pre-compartida IPsec, que en este ejemplo es aaabbbccc.

Puede dejar los dominios de búsqueda DNS y los servidores DNS vacía.

Bajo Vías de tránsito para entrar en la subred que se alcance sobre el VPN. En este ejemplo, 192.168.1.1.

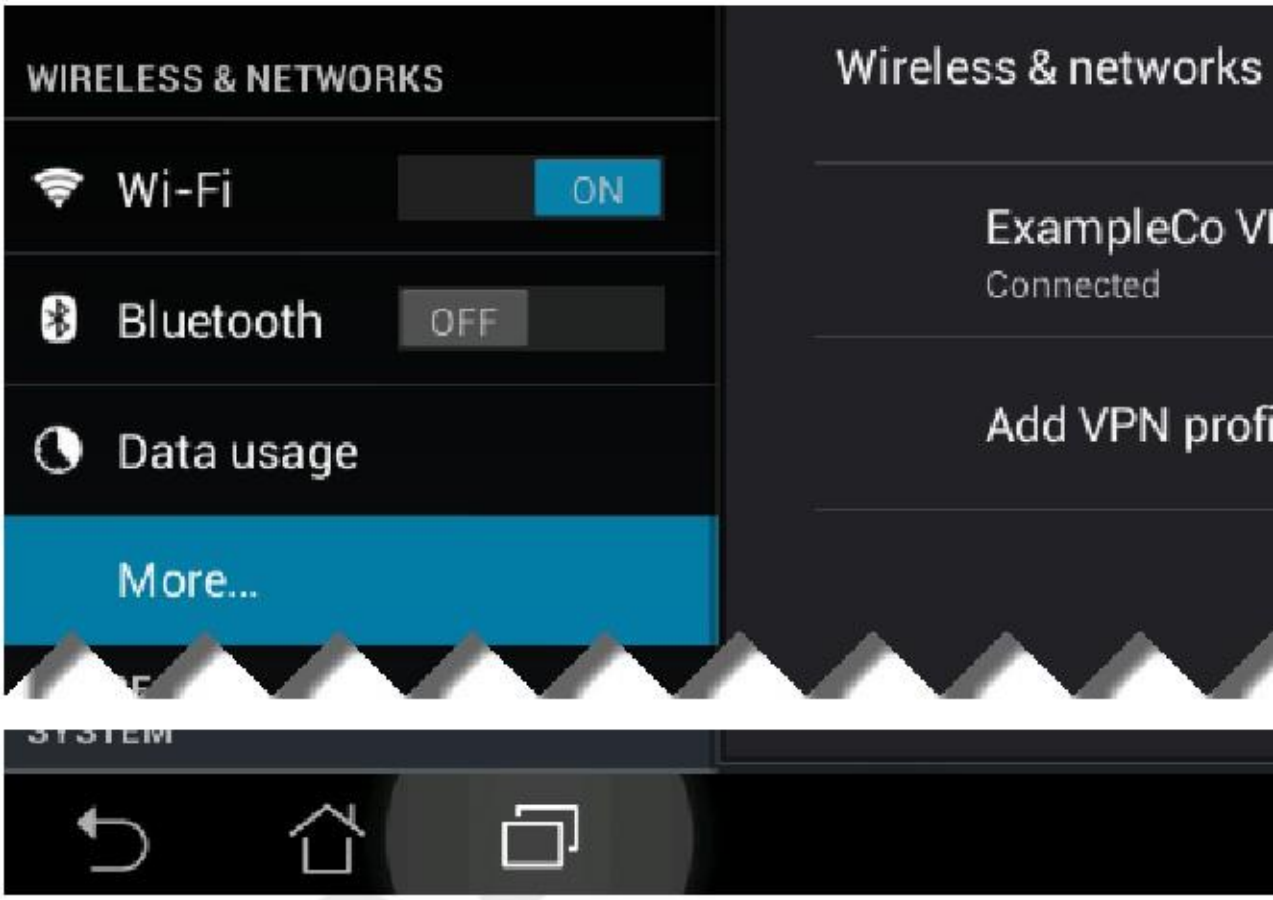
Pulse Guardar y volverá a la lista de VPN. Si toca el nombre de VPN en la lista, se intentará una Conexión VPN. Debido a que las credenciales no fueron introducidos durante el proceso de instalación, se le pedirá para ellos ahora, como se ve en la Figura 17.35, "Android 4.x IPsec - IPsec Autenticación del sistema". Entrar el nombre de usuario y contraseña. Si desea que las credenciales sean salvos, pulse en Guardar información de cuenta.

Figura 17.35. Android 4.x IPsec - IPsec Autenticación Prompt



Si tiene éxito, que se verá como en la Figura 17.36, "Android 4.x IPsec - Estado Conectado". Un icono de la llave aparece en el área de notificación para mostrar que la VPN está conectado. Se puede desconectar pulsando el Nombre de VPN en la lista, o deslizando hacia abajo la barra de notificaciones y después en la entrada VPN en el lista de notificación para ver la ventana de estado, que también contiene un botón de desconexión. Para editar o eliminar la VPN, pulsación larga sobre el nombre en la lista y elegir la acción deseada en el menú.

Figura 17.36. Estado Conectado - Android 4.x IPsec



iOS móvil IPsec

En la pantalla principal, puntee en Configuración y, a continuación VPN. En las versiones anteriores de iOS es posible que tenga que ir de
Configuración, al general, entonces VPN. Y algunos también requieren Ajustes, General, Red y luego VPN. Desde allí, pulse Añadir configuración VPN ....

En la parte superior de la pantalla, seleccione IPsec. Introduzca una descripción, como ExampleVPN.

Para el servidor, escriba la dirección IP o nombre de dominio completo del servidor. En nuestro ejemplo, es 192.168.20.243.

Cuenta es el nombre de usuario xauth de este usuario, ya sea mobileuser1. Si desea que el cliente para guardar el contraseña, escríbala en el cuadro Contraseña.

En Nombre de grupo, escriba el identificador de interlocutor de los ajustes de fase 1. En este ejemplo, vpn@example.com.

El campo secreto es la clave precompartida de los ajustes de fase 1. En este ejemplo, aaabbbccc.

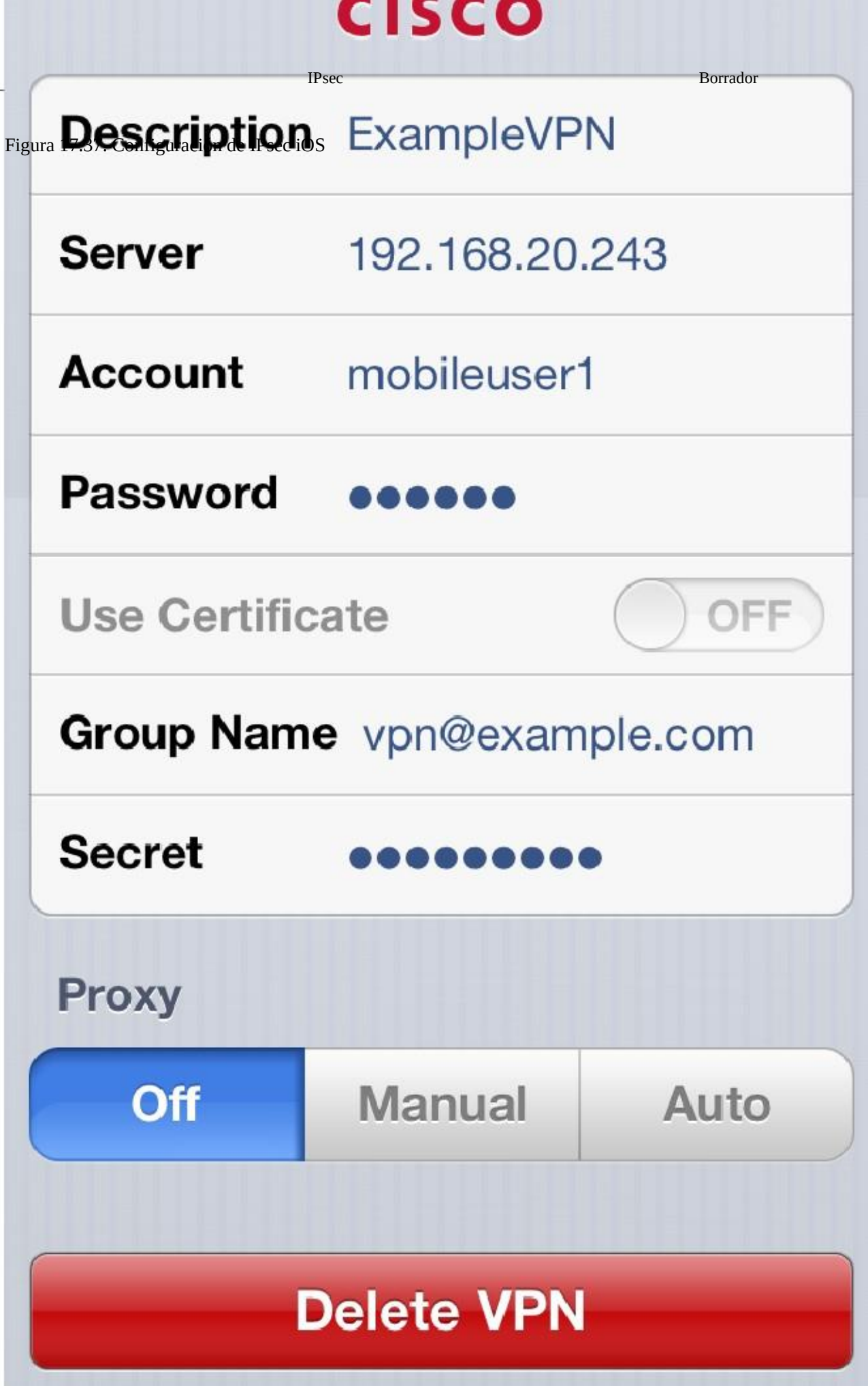
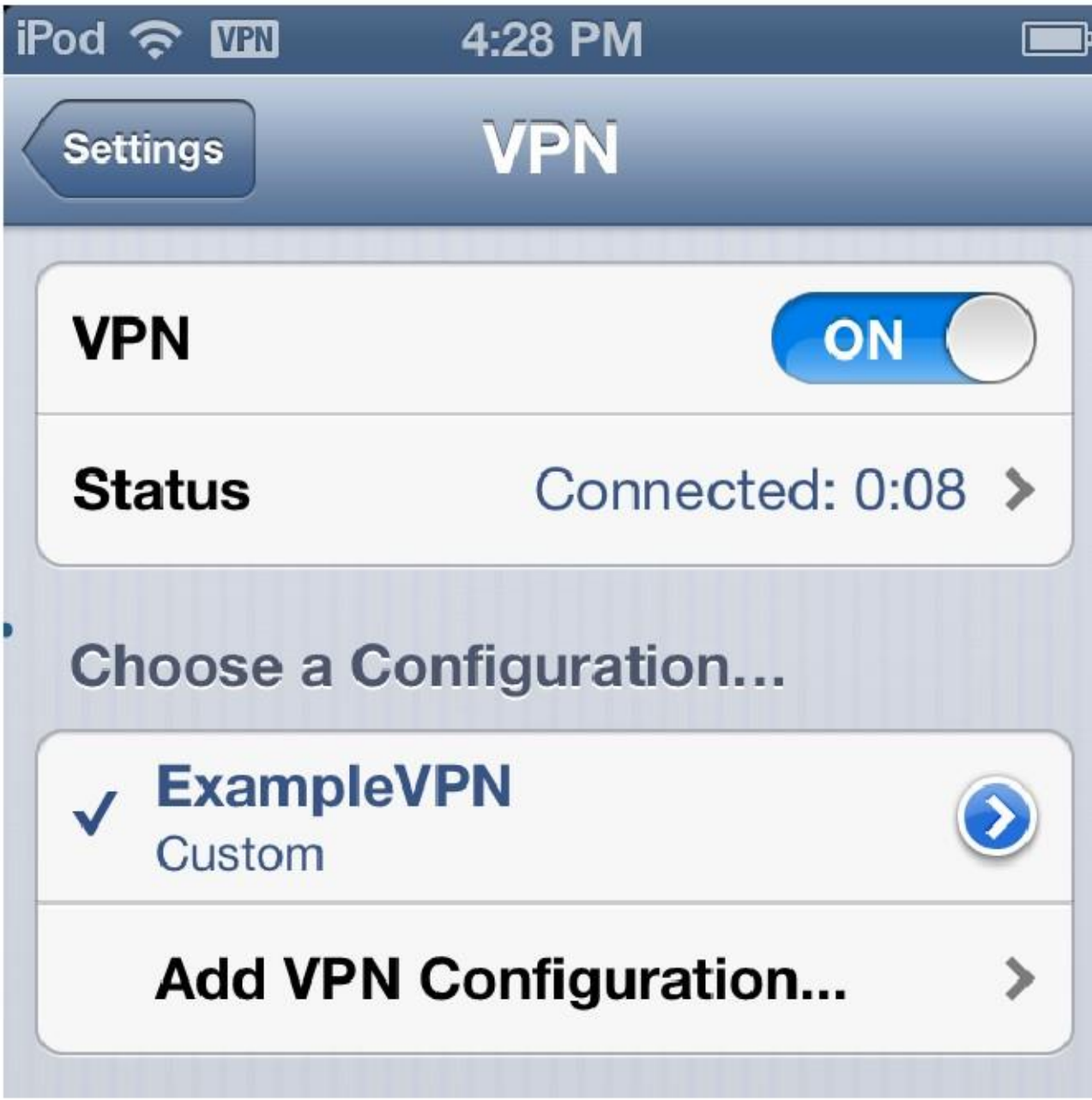


Figura 17.37: Configuración de IPsec iOS

La configuración VPN completa debe verse como la Figura 17.37, "Configuración IPsec iOS". Pulse Guardar y, a continuación,
toque el nombre de VPN para seleccionarla si tiene más de uno. Deslice la palanca de VPN On y el VPN debe conectar y el estado resultante debería parecerse a la Figura 17.38, "iOS IPsec - VPN Conectado". Hay un indicador de VPN se muestra en la barra de estado IOS para mostrar que la VPN está activo.

Figura 17.38. iOS IPsec - VPN conectado

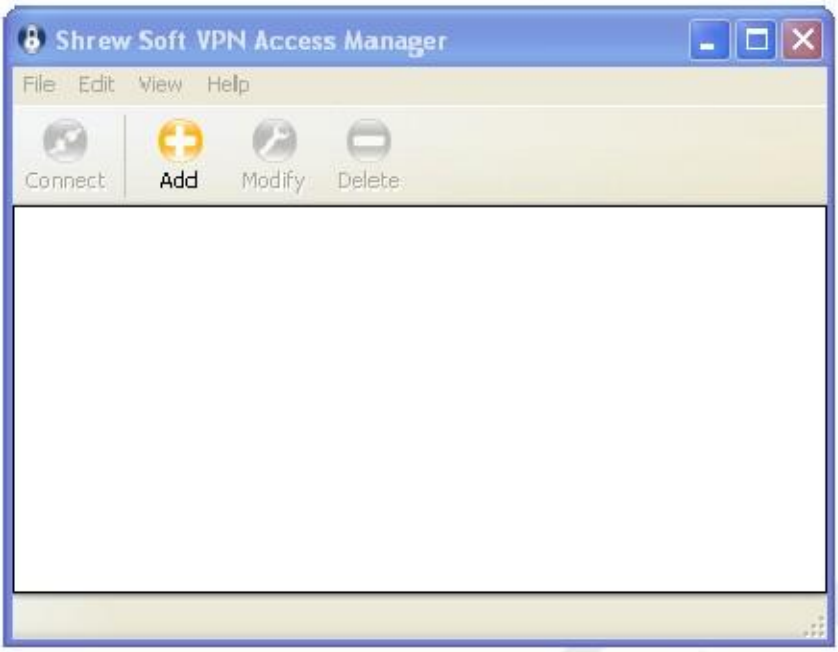


Shrew Soft Client para Windows

El Cliente Shrew Soft VPN es una sólida opción para el uso de IPsec en Windows. No sólo es fácil de usar y fiable, pero también está disponible completamente gratis. Visita http://www.shrew.net y descargar el última versión del cliente domada Soft para su plataforma. Ejecute el programa de instalación y haga clic en Siguiente o Continuar
a través de todas las indicaciones.

Inicie el Cliente domada Soft haciendo clic en el icono de Access Manager. Debe aparecer la pantalla principal, y verse como la Figura 17.39, "domada Soft VPN Access Manager - No hay conexiones todavía". A continuación, haga clic en el
Añadir botón para comenzar a configurar una nueva conexión.

Figura 17.39. Shrew Soft VPN Access Manager - No hay conexiones todavía

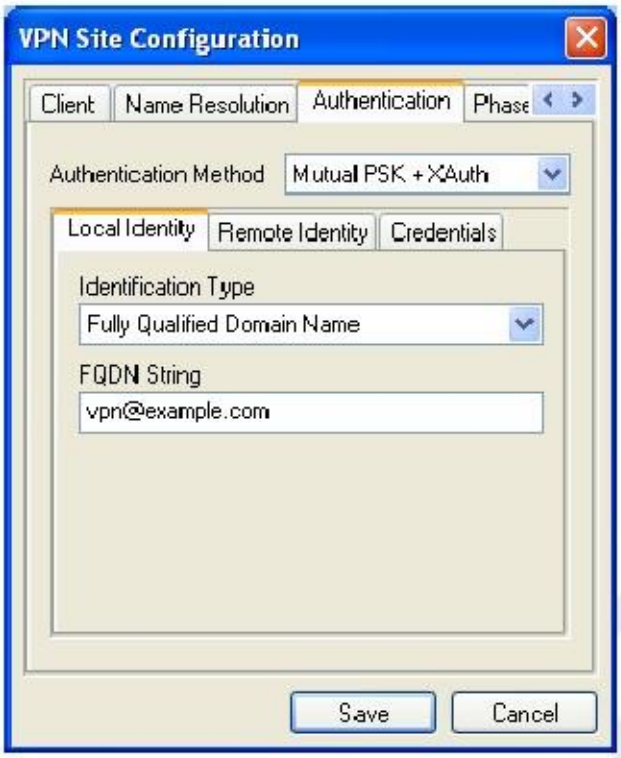


La ventana de configuración del sitio VPN debe abrir, con varias pestañas como en la Figura 17.40, "Client Setup: Pestaña General ". Se debe comenzar en la ficha General. Aquí, entre el Host como la Caja de pfSense WAN IP o la dirección IP de la interfaz de pfSense elegidos previamente para el uso de IPsec. En nuestro ejemplo, 192.168.20.243. El puerto debe ser 500. Auto configuración debe establecerse en ike config
tirar de manera que los ajustes se obtienen de pfSense. Para el método de dirección, cambio que a Uso adaptador virtual y la dirección asignada y luego verifique obtener automáticamente.

En la ficha del cliente, asegúrese de que NAT Traversal se establece en force-rfc, y el NAT Traversal Puerto debería ser 4500. Asegurar que todos los tres casillas de verificación en la parte inferior de la pantalla se comprueban. Compare el
ajustes en la pantalla con la figura 17.41, "Configuración de clientes: Tab Client" para asegurarse de que coinciden con la configuración adecuada.

En la ficha de resolución de nombres, cada cuadro debe ser revisado y obtener automáticamente también debe ser comprobado de manera que se obedecían las configuraciones del firewall. Consulte la Figura 17.42, "Configuración de clientes: Nombre
Resolución Tab "para ver ejemplos.

Figura 17.43. Configuración de clientes: autenticación, la identidad local

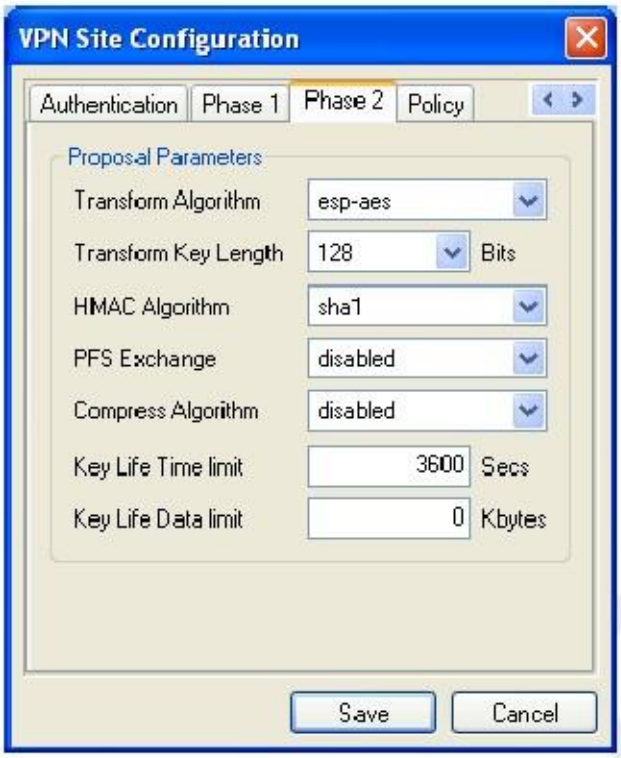


La ficha Autenticación tiene tres sub-pestañas que necesitan configuración también. En primer lugar, establecer el método de autenticación
a Mutual PSK + XAuth en la parte superior, y luego continuar a la ficha Identidad Local debajo, se muestra
En la Figura 17.43, "Configuración de clientes: autenticación, identidad local". Ajuste el tipo de identificación a Completamente
Qaulified de nombres de dominio, y la cadena de nombre de dominio completo para el identificador de interlocutor de la fase del servidor
Haga clic en la ficha Remoto de identidad (Figura 17.44, "Configuración de clientes: autenticación, la Identidad remoto"). Conjunto
el tipo de identificación a Any.

En la ficha Credenciales, que se muestra en la Figura 17.45, "Configuración de clientes: autenticación, credenciales", rellene el
Pre-Shared Key campo con la llave de los ajustes de fase 1, en nuestro ejemplo, aaabbbccc.

Ahora vuelve a la pestaña de la Fase 1, se observa en la Figura 17.46, "Configuración de clientes: Fase 1". Estos ajustes se corresponden con los establecidos en la sección del túnel de servidor de la Fase 1. Establezca el Tipo de Cambio de agresivo, la Bolsa de DH para Grupo 2, Algoritmo de cifrado para AES, Cipher Key Largo a 128
Bits, Hash Algorithm para SHA1, y la clave de la vida del tiempo límite 86400.

Figura 17.47. Configuración de clientes: Fase 2



Las opciones de la ficha de la Fase 2 también serán los mismos que los establecidos en los clientes móviles de la Fase 2 sección, como se puede ver en la Figura 17.47, "Configuración de clientes: Fase 2". Ajuste el algoritmo de transformación de esp-
aes, Transformar Longitud de la clave para 128 Bits, HMAC del algoritmo es SHA1, PFS es discapacitados, Comprimir Algoritmo es discapacitados, y el límite de tiempo de la vida es clave 3600.

Finalmente, está la ficha Directiva, que se muestra en la Figura 17.48, "Configuración de clientes: Política". Esto controla qué tráfico
Se enviará en el túnel. Desactive la opción Obtener automáticamente la topología, a continuación, haga clic en el botón Agregar.
En la pantalla de entrada de topología, se observa en la Figura 17.49, "Configuración de clientes: Política, Añadir Topología", Cheque
Obtener Topología Automáticamente o Túnel Todos. Esto hará que el cliente tire de la lista de redes de el servidor, o túnel todo el tráfico si el servidor no especifica ninguna. Alternativamente, puede dejar esa opción sin control y especificar qué subred será en el otro extremo del túnel. Para ello, haga clic en Agregar y, a continuación establecer el tipo de Incluir. Para la Dirección, ingrese la red detrás pfSense en el otro lado, y la Máscara de red que va junto con él. Para nuestro ejemplo que será 192.168.1.0 y 255.255.255.0 respectivamente. Haga clic en Aceptar.

Al hacer clic en Guardar, se le llevará de vuelta a la pantalla principal del cliente Shrew Soft, y usted tener la oportunidad de cambiar el nombre de la conexión, como en la Figura 17.50, "Configuración de clientes: Nuevo Nombre de conexión ".

Es una buena idea nombrar la conexión después de la ubicación en la que se conecta. En este caso, puse el nombre de que después de la oficina donde el túnel conduce como Figura 17.51, "listo para usar la conexión" shows.

Para conectar a la VPN, haga clic en él para seleccionarlo y luego haga clic en Conectar. El cuadro de diálogo de conexión VPN
aparecerá. Ahora, introduzca el nombre de usuario y contraseña y, a continuación, haga clic en el botón Conectar de allí. Si el túnel se establece con éxito, se indicará en la ventana. Figura 17.52 ", Túnel
Solicitar autenticación "se muestra la salida de una conexión exitosa.

Figura 17.52. Túnel de autenticación Prompt

Figura 17.53. Túnel Conectado

Ahora debería ser capaz de ponerse en contacto con los sistemas en el otro extremo del túnel. Si no ha salido bien o pasar el tráfico, vuelva a comprobar todos los ajustes en ambos lados, ya que se enumeran aquí. De lo contrario, continúe a la sección de solución de problemas.

TheGreenBow IPSec

TheGreenBow IPSec es un cliente comercial VPN para Windows que es compatible con pfSense. Las instrucciones para configurar este cliente con pfSense se pueden encontrar en el soporte de pasarela VPN Sección [http://www.thegreenbow.com/vpn_gateway.html] de su sitio web. Para obtener más información acerca de la compra y la configuración del cliente, visite su sitio web [http://www.thegreenbow.com]. Ellos ofrecer una prueba gratuita de 30 días del cliente para aquellos que buscan para evaluarla como una posible solución.

NCP Secure Entry Client

La entrada Secure Client por NCP [http://www.ncp-e.com/en/downloads/software.html] es otro cliente IPsec comercial para Windows, Windows Mobile y Symbian. Como es compatible con los estándares, sino que también puede conectarse a sistemas de pfSense.

SSH Sentinel

SSH Sentinel es otro cliente IPsec compatible con los estándares para Windows. Aunque SSH Sentinel hace trabajar con pfSense, su configuración es bastante complejo y el cliente libre disponible es de diez años, de haber sido puesto en libertad en 2002. Debido a estos factores, no se recomienda su uso, y la musaraña Soft cliente debe ser utilizado en su lugar.

IPSecuritas

IPSecuritas por Lobotomo Software [http://www.lobotomo.com/products/IPSecuritas/] es un programa gratuito Mac OS X cliente para IPsec que algunos usuarios han reportado a trabajar con pfSense.

Clientes Linux

Hay algunos clientes Linux libre acceso, pero varían entre distribuciones. Algunos son de primera termina a otros servicios públicos como ipsec-tools, pero deben trabajar siempre y cuando las configuraciones de cliente son
similar a la que se ha demostrado anteriormente.

Cisco VPN Client

El cliente de Cisco VPN no funciona actualmente con pfSense debido a la forma en que maneja un túnel tráfico. Esto debería funcionar ahora que xauth es posible, pero hasta ahora no hemos visto ningún informe de largo éxito a largo plazo.

Prueba de conectividad IPsec

La prueba más fácil para un túnel IPsec es un ping desde una estación cliente detrás del router a otro en el lado opuesto. Si esto funciona, el túnel está activo y trabajando adecuadamente.

Como se mencionó en la sección llamada "Traffic iniciado por pfSense y IPsec", el tráfico iniciado de pfSense normalmente no atravesar el túnel sin algún routing extra, pero hay una forma rápida de probar la conexión desde la consola del router mediante el ping- comando especificando una dirección de origen con la `-S` parámetro. Sin utilizar `-S` o una ruta estática, los paquetes generados por ping- no intentará para atravesar el túnel. Esta sería la sintaxis para usar con una prueba adecuada:

#ping-S <Local LAN IP> <Remoto LAN IP>

Cuando el `IP LAN local` es una dirección IP en una interfaz interna dentro de la subred local definición para el túnel, y el `Remoto LAN IP` es una IP en el router remoto dentro de la distancia subred lista para el túnel. En la mayoría de los casos esto no es más que la dirección IP de la LAN de la respectiva pfSense
routers. En nuestro ejemplo de sitio a sitio más arriba, esto es lo que tendría que escribir para poner a prueba desde la consola
del sitio del router:
#ping-S 192.168.1.1 10.0.10.1

Usted debe recibir respuestas de ping de la dirección LAN del sitio B si el túnel está activo y trabajando adecuadamente. Si usted no recibe ninguna respuesta, pasar a la sección de solución de problemas (la sección llamada "IPsec Solución de problemas ").

Solución de problemas de IPsec

Debido a la naturaleza meticuloso de IPsec, no es raro que surja problemas. Afortunadamente, hay algunos básicos (y algunos no tan básicos) pasos de solución de problemas que se pueden emplear para localizar problemas potenciales.

Túnel no establece

La causa más común de conexiones de túnel IPsec es una falta de coincidencia de configuración. A menudo es algo pequeño, tal como un grupo DH puesto a 1 en el lado A y 2 en el lado B, o tal vez una subred máscara de / 24 en un lado y / 32 en el otro. Algunos routers (Linksys, por ejemplo) también les gusta esconderse cierta Opciones detrás botones "avanzada" o hacer suposiciones. Una gran cantidad de ensayo y error puede estar involucrado, y un montón de lectura de registro, pero asegurándose de que ambas partes coinciden, precisamente, ayudarán a la mayoría.

Dependiendo de las conexiones a Internet en cualquiera de los extremos del túnel, también es posible (especialmente con clientes móviles) que un router que participan en un lado o el otro no maneja adecuadamente el tráfico IPsec, principalmente cuando NAT está involucrado. Los problemas son por lo general con el protocolo ESP. NAT Traversal (NAT-T) encapsula ESP en UDP el tráfico del puerto 4500 para conseguir alrededor de estos temas, pero no está en disponible en pfSense.

En el caso de un tiempo de espera en un cliente móvil, comprobar primero el estado del servicio en el Estado Servicios. Si el servicio se detiene, vuelva a comprobar que Permitir a los clientes móviles se comprueba en VPN IPsec, clientes móviles tab. Si el servicio se está ejecutando, compruebe los registros del cortafuegos (Estado Registros del sistema, pestaña Firewall) para ver si la conexión está siendo bloqueada, y si es así, agregue una regla para permitir el tráfico bloqueado.

Túnel establece pero no pasa tráfico

El principal sospechoso en caso de un túnel se acerca pero no pasará el tráfico serían las reglas de firewall de IPsec. Si usted es en el sitio y no se puede alcanzar el sitio B, verifique que el router B Sitio. Por el contrario, si usted está en el sitio B y no puede contactar sitio, revise el sitio A. Antes de examinar las normas, asegúrese de comprobar los registros del cortafuegos, que utilizadas en el Estado Registros del sistema, en la ficha Firewall. Si usted ve las entradas bloqueadas involucran las subredes son en el túnel IPsec, a continuación, pasar a la comprobación de las reglas. Si no hay entradas de registro que indican bloqueado paquetes, revisar la sección sobre consideraciones de enrutamiento de IPsec en la sección denominada "Enrutamiento y gateway consideraciones".

Paquetes bloqueados en el IPsec o `ENC0` la interfaz indica que el propio túnel ha establecido pero el tráfico está siendo bloqueado por las reglas de la interfaz IPsec. Paquetes bloqueados en la LAN u otra interfaz interna puede indicar que una regla adicional puede ser necesaria en el conjunto de reglas de esa interfaz para permitir el tráfico de la subred interna hacia el extremo remoto del túnel IPsec. Paquetes bloqueados en WAN o OPT WAN interfaces de impedirían un túnel desde el establecimiento. Normalmente, esto sólo ocurre cuando el automático Reglas VPN están deshabilitadas. Adición de una regla para permitir el protocolo ESP y el puerto UDP 500 a partir de ese remoto Dirección IP debe permitir que el túnel de establecer. En el caso de túneles móviles, tendrá que permitir el tráfico procedente de cualquier fuente para conectarse a los puertos.

Reglas para la interfaz IPsec se pueden encontrar en Firewall Reglas, en la pestaña IPsec. Errores comunes incluir el establecimiento de una norma única para permitir el tráfico TCP, lo que significa cosas como ICMP ping y DNS haría no trabajar a través del túnel. Consulte el Capítulo 10, Firewall para más información sobre cómo crear correctamente y solucionar problemas de reglas de firewall.

En algunos casos, también puede ser posible que una falta de coincidencia ajuste también podría causar un error en el tráfico que pasa el túnel. En una ocasión, vi a una subred definida en un router que no pfSense como 192.168.1.1/24, y en el lado pfSense era 192.168.1.0/24. El túnel establecido, pero el tráfico no pasaría hasta que el subred se corrigió.

También podría haber un problema con la forma en que se están enrutando los paquetes. La ejecución de una traceroute (Tracert en Windows) para una dirección IP en el lado opuesto del túnel puede ser esclarecedor. Repita la prueba de ambos lados del túnel. Compruebe el la sección llamada sección "Consideraciones de enrutamiento y de puerta de enlace" en este capítulo para obtener más información. Al utilizar traceroute, usted verá que el tráfico que no entran y dejar el túnel IPsec parecerá que faltan algunos saltos intermedios. Esto es normal y parte de cómo funciona IPsec. El tráfico que no entra correctamente un túnel IPsec aparecerá a salir de la WAN interfaz y ruta de salida a través de Internet, lo que apuntaría a una edición de enrutamiento tales como pfSense no ser la puerta de entrada (como en la sección titulada "Consideraciones de enrutamiento y de puerta de enlace"), un subred remota especificada incorrectamente en la definición de túnel, o un túnel que ha sido deshabilitado.

Algunos servidores funcionan, pero no todos

Si el tráfico entre máquinas más de las funciones de VPN correctamente, pero algunos hosts no, esto es comúnmente una de cuatro cosas.

. 1 Falta, es incorrecto o ignorado puerta de enlace predeterminada - Si el dispositivo no dispone de una puerta de enlace predeterminada o tiene uno que apunta a algo distinto de pfSense, no saber cómo obtener correctamente de nuevo a la red remota en la VPN (véase la sección denominada "Consideraciones de enrutamiento y de puerta de enlace"). Algunos dispositivos, incluso con una puerta de enlace predeterminada especificada, no usan ese gateway. Esto se ha visto en diversos dispositivos integrados, incluyendo cámaras IP y algunas impresoras. No hay nada que pueda hacer al respecto que no sea conseguir el software en el dispositivo fijo. Usted puede verificar esto mediante la ejecución tcpdump en la interfaz en el interior de los cortafuegos conectados a la red que contiene el dispositivo. Solución de problemas con tcpdump se trata en la sección denominada "Uso del comando tcpdump line ", y un ejemplo IPsec-específico se encuentran en la sección llamada" túnel IPsec no lo hará conectar ". Si usted ve el tráfico que va en el interior de la interfaz en el servidor de seguridad, pero no hay respuestas a volver, el dispositivo no está encaminando correctamente su tráfico de respuesta (o potencialmente podría bloqueando a través de un firewall).

. 2 máscara de subred incorrecta - Si la subred en uso en un extremo es 10.0.0.0/24 y la otra es 10.254.0.0/24, y un anfitrión 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 la subred VPN remota es parte de la red local y por lo tanto de enrutamiento no funcionará correctamente.

. 3 Anfitrión firewall - si hay un firewall en el host de destino, no se puede permitir que las conexiones.

4 Las reglas de firewall en pfSense -. Garantizar las reglas en ambos extremos permiten que el tráfico de la red deseada.

Se bloquea la conexión

Históricamente, IPsec no ha manejado con gracia paquetes fragmentados. Muchas de estas cuestiones han sido resueltos en los últimos años, pero puede haber algunos problemas persistentes. Si no se observan bloqueos o pérdida de paquetes sólo cuando se utilizan protocolos específicos (SMB, RDP, etc), es posible que tenga que configurar MSS de sujeción para el VPN. Que se puede activar en Sistema Avanzado en la ficha Varios. En esa pantalla, seleccione Habilitar MSS de sujeción en el tráfico VPN e introduzca un valor. Un buen punto de partida sería 1400, y si eso funciona poco a poco aumentar el valor MSS hasta encontrar el punto de ruptura, luego de vuelta de un poco de allí. Si eso no ayuda, la WAN MTU puede necesitar reducida. Un MTU reducida se asegurarse de que los paquetes que atraviesan el túnel son todos de un tamaño que se puede transmitir toda, de forma similar a MSS de sujeción, sino para todo el tráfico y no sólo para TCP. Asesoramiento valor similar se aplica a la MTU como se aplica a los SMS, comience en 1300 y su forma de trabajo.

"Al azar" Fallas Desconecta Túnel / DPD en Routers Embedded

Si usted experimenta túneles IPsec eliminó en una ALIX u otro hardware integrado, es posible que necesite desactivar DPD en el túnel. Usted puede ser capaz de correlacionar los fracasos a veces de gran ancho de banda uso. Esto sucede cuando la CPU en un sistema de baja potencia está atado con el envío de tráfico IPsec o es ocupada de otro modo. Debido a la sobrecarga de la CPU no puede tomar el tiempo para responder a las peticiones DPD o ver una respuesta a una petición de su propia. Como consecuencia, el túnel fallará un cheque DPD y sea desconectado.

Túneles Establecer y trabajo pero no logran Renegociar

En algunos casos, es posible que un túnel funcionará correctamente, pero una vez que la fase 1 o fase 2 vida útil expira, el túnel no podrá renegociar correctamente. Esto puede manifestarse en pocos diferentes maneras, cada uno con una resolución diferente.

NAT Traversal causando insuficiencia Renegociación

Si ambos lados del túnel tienen IPs públicas y NAT-T está habilitado en uno o ambos lados, hemos visto situaciones en las que esto ha conducido a un problema con la renegociación. Desactive NAT-T en ambos lados y la túneles deberá restablecer correctamente.

DPD no compatible, gotas de un lado, pero el otro permanece

Considere este escenario, que DPD está diseñado para prevenir, pero puede ocurrir en lugares donde la DPD es sin soporte:

• Un túnel se establece desde el sitio A al sitio B, desde el tráfico iniciado en el sitio A.

• Sitio B expira la fase 1 o fase 2 antes del sitio

• sitio se cree que el túnel está en marcha y continuar para enviar el tráfico como si el túnel está trabajando adecuadamente.

• Sólo cuando de sitio fase 1 o fase 2 vida expira va a renegociar como se esperaba.

En este escenario, los dos posibles cosas resoluciones son: Enable DPD o sitio B debe enviar el tráfico a la web A lo que hará que todo el túnel para renegociar. La manera más fácil para que esto suceda es permitir un mecanismo de mantener viva en ambos lados del túnel.

También puede tratar de desactivar Prefiero Antiguo IPsec SA en Sistema Avanzado en la ficha Varios.

Túnel Establece cuando se inicia, pero no cuando Respondiendo

Si el túnel establece correctamente cuando pfSense inicia el túnel, pero no cuando el otro extremo inicia, esto normalmente indica que hay una ligera falta de coincidencia en la configuración de la Fase 1 que fue ignorada porque un
valor más seguro era utilizado por los pares. La forma más sencilla de evitar esto es configurar la Propuesta Comprobación
opción en la fase 1 la configuración del túnel a Obedecer.

Interpretación IPsec Conectarse

Los registros de IPsec disponibles al Estado Registros del sistema, en la pestaña IPsec contendrá un registro del túnel proceso de conexión. En esta sección, vamos a demostrar algunas entradas de registro típicos, tanto buenas como malas. Las principales cosas a tener en cuenta son las frases más importantes que indican qué parte de una conexión realmente trabajadas.
Si ve "ISAKMP-SA estableció", eso significa que la fase 1 se completó con éxito y seguridad Asociación se negoció. Si "IPsec-SA estableció" se ve, a continuación, la fase 2 también se ha completado y el túnel debería estar listo y trabajando en ese momento.

En los siguientes ejemplos, el túnel se inicia a partir del sitio A.

Conexiones correctas

Estos son ejemplos de los túneles de éxito, tanto en el modo principal y agresivo.

El éxito de modo principal Túnel

Registro de resultados de sitio:

```
ERROR: Ya existe esa política. de todos modos reemplazarque: 192.168.30.0/24 [0] 192.168
ERROR: Ya existe esa política. de todos modos reemplazarque: 192.168.30.1/32 [0] 192.168
ERROR: Ya existe esa política. de todos modos reemplazarque: 192.168.30.0/24 [0] 192.168
ERROR: Ya existe esa política. de todos modos reemplazarque: 192.168.32.0/24 [0] 192.168
[ToSiteB]: INFO: IPsec-SA solicitud de 172.16.3.41      en cola debido a que no phase1
                                                        encontrado.
```

```
[ToSiteB]: INFO: iniciar nueva negociación de la fase 1: 172.16.0.40 [500] <=> 172.16.3.
INFO: iniciar el modo de protección de la identidad.
INFO: recibido Vendor ID: DPD
INFO: recibido roto Microsoft ID: FRAGMENTACIÓN
[ToSiteB]: INFO: ISAKMP-SA estableció 172.16.0.40 [500] -172.16.3.41 [500] spi: CC3
[ToSiteB]: INFO: iniciar nuevas negociaciones de la fase 2: 172.16.0.40 [500] <=> 172.16
[ToSiteB]: INFO: IPsec-SA establecida: ESP 172.16.3.41 [0] -> 172.16.0.40 [0] spi = 94
[ToSiteB]: INFO: IPsec-SA establecida: ESP 172.16.0.40 [500] -> 172.16.3.41 [500] sp
```

Registro de resultados de sitio B:

```
ERROR: Ya existe esa política. de todos modos reemplazarlo: 192.168.32.0/24 [0] 192.168
ERROR: Ya existe esa política. de todos modos reemplazarlo: 192.168.32.1/32 [0] 192.168
ERROR: Ya existe esa política. de todos modos reemplazarlo: 192.168.32.0/24 [0] 192.168
ERROR: Ya existe esa política. de todos modos reemplazarlo: 192.168.30.0/24 [0] 192.168
[ToSiteA]: INFO: responder nueva fase 1 de la negociación: 172.16.3.41 [500] <=> 172.16.
INFO: iniciar el modo de protección de la identidad.
INFO: recibido roto Microsoft ID: FRAGMENTACIÓN
INFO: recibido Vendor ID: DPD
[ToSiteA]: INFO: ISAKMP-SA estableció 172.16.3.41 [500] -172.16.0.40 [500] spi: CC3
[ToSiteA]: INFO: responder nueva negociación de fase 2: 172.16.3.41 [500] <=> 172.16.0.4
[ToSiteA]: INFO: IPsec-SA establecida: ESP 172.16.0.40 [0] -> 172.16.3.41 [0] spi = 24
[ToSiteA]: INFO: IPsec-SA establecida: ESP 172.16.3.41 [500] -> 172.16.0.40 [500] sp
```

Exitosa túnel Modo Agresivo

Registro de resultados de sitio:

```
[ToSiteB]: INFO: IPsec-SA solicitud de 172.16.3.41 en cola debido a que no phase1 encont
[ToSiteB]: INFO: iniciar nueva negociación de la fase 1: 172.16.0.40 [500] <=> 172.16.3.
INFO: comienza el modo agresivo.
INFO: recibido roto Microsoft ID: FRAGMENTACIÓN
INFO: recibido Vendor ID: DPD
NOTIFICAR: no se pudo encontrar el pskey adecuado, tratar de conseguir uno por la direcc
los pares.
[ToSiteB]: INFO: ISAKMP-SA estableció 172.16.0.40 [500] -172.16.3.41 [500] spi: fcc
[ToSiteB]: INFO: iniciar nuevas negociaciones de la fase 2: 172.16.0.40 [500] <=> 172.16
[ToSiteB]: INFO: IPsec-SA establecida: ESP 172.16.3.41 [0] -> 172.16.0.40 [0] spi = 19
[ToSiteB]: INFO: IPsec-SA establecida: ESP 172.16.0.40 [500] -> 172.16.3.41 [500] sp
```

Registro de resultados de sitio B:

```
[ToSiteA]: INFO: responder nueva fase 1 de la negociación: 172.16.3.41 [500] <=> 172.16.
INFO: comienza el modo agresivo.
INFO: recibido roto Microsoft ID: FRAGMENTACIÓN
INFO: recibido Vendor ID: DPD
NOTIFICAR: no se pudo encontrar el pskey adecuado, tratar de conseguir uno por la direcc
los pares.
[ToSiteA]: INFO: ISAKMP-SA estableció 172.16.3.41 [500] -172.16.0.40 [500] spi: fcc
[ToSiteA]: INFO: responder nueva negociación de fase 2: 172.16.3.41 [500] <=> 172.16.0.4
[ToSiteA]: INFO: IPsec-SA establecida: ESP 172.16.0.40 [0] -> 172.16.3.41 [0] spi = 11
[ToSiteA]: INFO: IPsec-SA establecida: ESP 172.16.3.41 [500] -> 172.16.0.40 [500] sp
```

Ejemplos de conexión fallidos

Estos ejemplos muestran fallos en la conexión por razones diferentes. Partes Particularmente interesantes del registro Se hará hincapié en las entradas.

Mismatched Fase 1 Encryption

Registro de resultados de sitio:

```
[ToSiteB]: INFO: IPsec-SA solicitud de 172.16.3.41 en cola debido a que no phase1 encont
[ToSiteB]: INFO: iniciar nueva negociación de la fase 1: 172.16.0.40 [500] <=> 172.16.3.
INFO: iniciar el modo de protección de la identidad.
[ToSiteB]: ERROR: Negociación phase2 fracasó por falta de tiempo a la espera de phase1.
INFO: eliminar la fase 2 manejador.
ERROR: Negociación phase1 fracasó por falta de tiempo para arriba. 96f516ded84edfca:
00000000000000
```

Registro de resultados de sitio B:

```
[ToSiteA]: INFO: responder nueva fase 1 de la negociación: 172.16.3.41 [500] <=> 172.16.
INFO: iniciar el modo de protección de la identidad.
INFO: recibido roto Microsoft ID: FRAGMENTACIÓN
INFO: recibido Vendor ID: DPD
ERROR: enctype rechazado: DB (prop # 1: RRT # 1): Peer (prop # 1: RRT # 1) = 3DES-CBC: AES-CB
ERROR: ninguna propuesta adecuada encontrado.
ERROR: no se pudo conseguir propuesta válida.
Error: Error al paquete pre-proceso.
ERROR: Negociación phase1 falló.
```

En este caso, la entrada de registro te dice exactamente cuál era el problema: Este lado se fijó para 3DES cifrado, y el lado remoto se establece para AES. Establezca los valores de juego y vuelva a intentarlo.

Fase Mismatched 1 DH Group

En este caso, las entradas de registro serán exactamente como el anterior, excepto que la línea de subrayado en lugar de otro ser:

ERROR: dh_group rechazado: DB (prop # 1: RRT # 1): Peer (prop # 1: RRT # 1) = 768 bits MODP g

Este error puede corregirse mediante el establecimiento de la configuración en ambos extremos del túnel grupo DH para un juego
valor.

Clave Mismatched precompartida

Una clave pre-compartida coincidentes puede ser un poco más difícil de diagnosticar. Un error que indica el hecho de que esta
valor no coincide, no se imprime en el registro, en lugar usted verá un mensaje como este:

```
[ToSiteB]: Notificar: el paquete es retransmitido por 172.16.3.41 [500] (1).
[ToSiteB]: ERROR: Negociación phase2 fracasó por falta de tiempo a la espera de phase1.
```

Si usted nota un error similar a lo anterior, compruebe que las claves pre-compartidas coinciden en ambos extremos.

Mismatched Fase 2 Encryption

Registro de resultados de sitio:

```
[ToSiteB]: INFO: IPsec-SA solicitud de 172.16.3.41 en cola debido a que no phase1 encont
[ToSiteB]: INFO: iniciar nueva negociación de la fase 1: 172.16.0.40 [500] <=> 172.16.3.
INFO: iniciar el modo de protección de la identidad.
INFO: recibido Vendor ID: DPD
INFO: recibido roto Microsoft ID: FRAGMENTACIÓN
[ToSiteB]: INFO: ISAKMP-SA estableció 172.16.0.40 [500] -172.16.3.41 [500] spi: 196
[ToSiteB]: INFO: iniciar nuevas negociaciones de la fase 2: 172.16.0.40 [500] <=> 172.16
ERROR: NO-fatal-PROPUESTA ELEGIDA mensaje de notificación, phase1 debería suprimirse.
```

Registro de resultados de sitio B:

```
[ToSiteA]: INFO: responder nueva fase 1 de la negociación: 172.16.3.41 [500] <=> 172.16.
INFO: iniciar el modo de protección de la identidad.
INFO: recibido roto Microsoft ID: FRAGMENTACIÓN
```

```
INFO: recibido Vendor ID: DPD
[ToSiteA]: INFO: ISAKMP-SA estableció 172.16.3.41 [500] -172.16.0.40 [500] spi: 196
[ToSiteA]: INFO: responder nueva negociación de fase 2: 172.16.3.41 [500] <=> 172.16.0.4
ADVERTENCIA: trns_id coincidentes: mis compañeros: AES: 3DES
ERROR: no se repite
ERROR: no existe una política adecuada encontrado.
Error: Error al paquete pre-proceso.
```

En estas entradas del registro, usted puede ver que la fase 1 completada con éxito ("ISAKMP-SA estableció"), pero no durante la fase 2. Además, declara que no podía encontrar una propuesta adecuada, y desde el Registros del sitio B podemos ver que esto se debió a los sitios se están estableciendo para los distintos tipos de cifrado, AES en un lado y 3DES en el otro.

Otros Mismatched Fase 2 Información

Alguna otra fase 2 errores tales como los valores de PFS no coincidentes o no coincidentes subredes remotas resultará en la misma salida del registro. En este caso, hay poco remedio que comprobar cada opción para asegurar los ajustes coincidir en ambos lados.

Registro de resultados de sitio:

```
[ToSiteB]: INFO: IPsec-SA solicitud de 172.16.3.41 en cola debido a que no phase1 encont
[ToSiteB]: INFO: iniciar nueva negociación de la fase 1: 172.16.0.40 [500] <=> 172.16.3.
INFO: iniciar el modo de protección de la identidad.
INFO: recibido Vendor ID: DPD
INFO: recibido roto Microsoft ID: FRAGMENTACIÓN
[ToSiteB]: INFO: ISAKMP-SA estableció 172.16.0.40 [500] -172.16.3.41 [500] spi: 2a2
[ToSiteB]: INFO: iniciar nuevas negociaciones de la fase 2: 172.16.0.40 [500] <=> 172.16
[ToSiteB]: ERROR: 172.16.3.41 renunciar para conseguir IPsec-SA por falta de tiempo para
esperar.
```

Registro de resultados de sitio B:

```
[ToSiteA]: INFO: responder nueva fase 1 de la negociación: 172.16.3.41 [500] <=> 172.16.
INFO: iniciar el modo de protección de la identidad.
INFO: recibido roto Microsoft ID: FRAGMENTACIÓN
INFO: recibido Vendor ID: DPD
[ToSiteA]: INFO: ISAKMP-SA estableció 172.16.3.41 [500] -172.16.0.40 [500] spi: 2a2
[ToSiteA]: INFO: responder nueva negociación de fase 2: 172.16.3.41 [500] <=> 172.16.0.4
ERROR: no existe una política encontrado: 192.168.30.0/24 [0] 192.168.32.0/24 [0] = proto cualquier dir = en
ERROR: no se pudo obtener propuesta de respondedor.
Error: Error al paquete pre-proceso.
```

Los errores indican que las propuestas para la fase 2 no estaban de acuerdo, y todos los valores de la sección de la fase 2 debe ser revisado, así como las definiciones de subred remota.

Nota

En algunos casos, si un lado tiene la SLP ajustado a apagado, y el otro lado tiene un conjunto de valores, el túnel seguirá establecer y trabajar. La falta de coincidencia se muestra más arriba sólo se puede ver si los valores falta de coincidencia, por ejemplo 1vs 5.

Otros errores comunes

Algunos mensajes de error se pueden encontrar en los registros de IPsec. Algunas son inofensivas, y otros son indicativa de problemas potenciales. Por lo general, los mensajes de registro son bastante sencillos en su significado, y indicar varios problemas para establecer un túnel con razones. Hay algunos, sin embargo, que son un poco más oscuro.

```
20 de febrero 10:33:41 racoon: [172.16.0.40] ERROR: no se pudo comprobar la validez de proce
                    paquetes ph2 [
```

```
20 de febrero 10:33:41 mapache: ERROR: no pudo conseguir sainfo.
```

Esto se observa con mayor frecuencia cuando las definiciones de subred local y / o remota se especifican de forma incorrecta,
especialmente si la máscara de subred se establece incorrectamente en un lado.

```
mapache: ERROR: El mensaje no debe estar encriptada.
```

Indica que puede haber un problema con el tráfico que llega desde el extremo opuesto del túnel. Intentar reiniciar el mapache servicio en el router extremo más alejado de la navegación a Estado Servicios y clic Reanudar al lado de mapache.

```
mapache: ERROR: no se puede iniciar el modo rápido, no hay ISAKMP-SA.
```

Puede indicar un problema con el envío de tráfico local para el túnel remoto, debido a que una de Seguridad ISAKMP No se ha encontrado asociación. Puede que sea necesario reiniciar el mapache servicio en uno o ambos lados para aclarar esto.

```
mapache: INFO: solicitud para el establecimiento de IPsec-SA se puso en cola debido a qu
fun phase1
```

Esto es normal, y por lo general visto cuando primero se establece un túnel. El sistema primero intentará completar una conexión de la fase 1 a la parte más alejada y luego continuar.

```
mapache: INFO: PF_KEY no soportado mensaje REGISTER
```

Esto es inofensivo, así, y se encuentra típicamente en el registro poco después de la mapache daemon se inicia.

Depuración avanzada

Cuando la negociación está fallando, especialmente cuando se conecta a dispositivos de IPsec de terceros en los que no es tan
fácil de combinar por completo los ajustes entre las dos partes, a veces la única manera de conseguir una adecuada información para resolver el problema es ejecutar mapache en modo de depuración. Para ello, vaya al Sistema de Avanzado en la ficha Varios y verificación Iniciar racoon en modo de depuración. La información de depuración se registrarán en el registro regular de IPsec.

Si no hay información de registro demasiado, puede que tenga que ejecutar mapache en el primer plano en modo de depuración
de la cáscara. Para ello, primero inicie sesión en su servidor de seguridad mediante SSH y la opción de elegir 8en la consola
menú de un símbolo del sistema. Ejecute los siguientes comandos.

```
#killall mapache
```

Ahora esperar unos 5 segundos para que el proceso de cerrar, y poner en marcha de nuevo con el siguiente.

```
#racoon-F-d-v-f / var / etc / racoon.conf
```

La primera línea se detiene el vigente mapache proceso. El segundo comienza mapache en el primer plano (-F), con depuración (-d), el aumento de nivel de detalle (-v), utilizando el archivo de configuración `/ Var / etc / racoon.conf` (-
`f)`. Corriendo en el primer plano hace que muestre sus registros en su sesión de SSH, para que pueda ver lo que está sucediendo en tiempo real. Para salir de mapache, prensa Ctrl-C y se detiene el servicio.
Después de terminar con la depuración, tendrá que empezar a racoon normalmente. La forma más fácil de hacerlo es para navegar a Estado Servicios en la interfaz web y haga clic en al lado de mapache.

Nota

Este método de depuración es perjudicial para todos IPsec en el sistema, cuando matas off mapache usted caerá todas las conexiones IPsec. Debido al volumen de registros que tendrá que resolver a través de múltiples conexiones IPsec habilitados, mientras que la depuración de un problema con una de les es más fácil si usted puede desactivar los demás, mientras que la resolución de problemas. Generalmente este método de
depuración sólo se realiza cuando la educación de una nueva conexión IPsec.

Configuración de dispositivos de terceros IPsec

Puede conectar cualquier dispositivo VPN de apoyo estándar IPsec con pfSense. Se está utilizando en producción en combinación con equipos numerosos vendedores, y debería funcionar bien con cualquier IPsec dispositivos capaces en su red. Conexión de dispositivos a partir de dos proveedores diferentes puede ser un problema independientemente de los proveedores 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. Este sección ofrece una orientación general sobre la configuración de IPsec VPNs con dispositivos de otros fabricantes, así como
ejemplos específicos sobre cómo configurar firewalls PIX de Cisco y los routers IOS.

Orientaciones generales para dispositivos IPsec de terceros

Para configurar un túnel IPSec entre pfSense y un dispositivo de otro fabricante, la principal preocupación es asegurarse de que su fase 1 y 2 parámetros coinciden en ambos lados. Para las opciones de configuración en pfSense, donde se le permite seleccionar múltiples opciones que debe seleccionar por lo general sólo uno de los opciones y asegurar el otro lado se encuentra el mismo. Los puntos finales debería 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. Configure ambos extremos de lo que usted cree son los mismos ajustes y guardar y aplicar los cambios en ambos lados.

Una vez que usted cree que la configuración coincide en ambos extremos del túnel, intentar pasar el tráfico a través de la VPN
para desencadenar su inicio, a continuación, comprobar los registros de IPsec en ambos extremos para revisar la negociación. Dependiente
sobre la situación, los registros de uno de los extremos pueden ser más útiles que las del extremo opuesto, por lo que es bueno comprobar ambos y comparar. Va a encontrar el lado pfSense proporciona una mejor información de alguna escenarios, mientras que en otras ocasiones el otro dispositivo proporciona el registro más útil. Si la negociación falla, determinar si se trataba de la fase 1 o 2, que falló y revisar a fondo la configuración en consecuencia, como se describe en la sección llamada "IPsec Solución de problemas".

Cisco PIX OS 6.x

La siguiente configuración sería para un Cisco PIX se ejecuta en 6.x como sitio B a partir del ejemplo de sitio configuración a sitio anteriormente en este capítulo. Vea la sección llamada "Sitio al ejemplo de configuración de sitio" para la configuración del sitio pfSense.

```
conexión sysopt permiso ipsec
ISAKMP permitirá exterior

! --- Fase 1
Dirección de la identidad del isakmp
política del isakmp 3des 1 encriptación
política de ISAKMP 1 hash SHA
política de ISAKMP 1 grupo 2
política de ISAKMP 1 vida 86400
política de ISAKMP 1 autenticación pre-parte
clave del isakmp abc123% XyZ9 $ 7qwErty99 dirección 172.23.1.3 máscara de red 255.255.25
no-x

! --- Fase 2
transformar-ipsec crypto 3dessha1 esp esp-3des-sha-hmac
access-list permiso PFSVPN IP 10.0.10.0 255.255.255.0 192.168.1.0 255.255.255.0
mapa criptográfico dyn-map 10 ipsec-ISAKMP
mapa criptográfico dyn-map 10 coincidencia de dirección PFSVPN
mapa criptográfico dyn-map 10 conjunto de pares 172.23.1.3
mapa criptográfico dyn-map 10 set set transformar-3dessha1
mapa criptográfico dyn-mapa 10 sistemas de seguridad-asociación de toda la vida segundo
mapa criptográfico dyn-map interfaz exterior

! --- No-nat para asegurarse de que las rutas a través
del túnel
```

```
access-list permiso nonat de ip 10.0.10.0 255.255.255.0 192.168.1.0 255.255.255.0
nat (inside) 0 access-list del nonat
```

Cisco PIX OS 7.x, 8.x y ASA

Configuración de las revisiones más nuevas del sistema operativo PIX y ASA para los dispositivos es similar a la de la mayor
queridos, pero tiene algunas diferencias significativas. El siguiente ejemplo sería que el uso de un PIX funcionamiento Versión OS 7.xo 8.x, o un dispositivo de ASA, como el sitio B en el ejemplo de sitio a sitio, anteriormente en este capítulo.
Vea la sección llamada "Sitio a sitio de ejemplo de configuración" de la configuración correspondiente del sitio A.

```
ISAKMP crypto permite afuera

! --- Fase 1
política de ISAKMP crypto 10
  autenticación de pre-parte
  cifrado 3DES
  hash SHA
  grupo 2
  86,400 de por vida



túnel-grupo 172.23.1.3 tipo ipsec-l2l
túnel-grupo 172.23.1.3 ipsec-atribuye abc123-clave pre-compartida% XyZ9 $ 7qwErty99

! --- Fase 2
transformar-ipsec crypto 3dessha1 esp esp-3des-sha-hmac
access-list PFSVPN permiso extendido del IP 10.0.10.0 255.255.255.0 192.168.1.0 255.25
mapa criptográfico outside_map 20 coincidencia de dirección PFSVPN
mapa criptográfico outside_map 20 conjunto de pares 172.23.1.3
mapa criptográfico outside_map 20 set transformar-3dessha1
mapa criptográfico interfaz outside_map fuera



! --- No-nat para asegurarse de que las rutas a través del túnel
la lista de acceso del permiso extendido el nonat ip 10.0.10.0 255.255.255.0 192.168.1.0
255.255
nat (inside) 0 access-list del nonat
```

Cisco IOS Los routers

Esto muestra un router basado en IOS de Cisco como el sitio B del ejemplo de configuración de sitio a sitio a principios de
el capítulo. Vea la sección de la sección llamada "Sitio al ejemplo de configuración del sitio" para el sitio pfSense ajustes.

```
! --- Fase 1
política de ISAKMP crypto 10
  encr 3des
  autenticación de pre-parte
  grupo 2
clave del isakmp cripto abc123% XyZ9 $ 7qwErty99 dirección 172.23.1.3 no-xauth



! --- Fase 2
access-list 100 permite ip 192.168.1.0 0.0.0.255 10.0.10.0 0.0.0.255
access-list 100 del IP del permiso 10.0.10.0 0.0.0.255 192.168.1.0 0.0.0.255
set-transform ipsec crypto 3DES-SHA esp esp-3des-sha-HMAC
mapa criptográfico PFSVPN 15 ipsec-ISAKMP
  establecer pares 172.23.1.3
  transformar-set 3DES-SHA
  dirección del 100



! --- Asigne el mapa criptográfico para la interfaz WAN
```

```
interfaz FastEthernet0 / 0
  mapa criptográfico PFSVPN


! --- No-Nat lo que este tráfico va a través del túnel, y no la WAN
ip nat dentro de la fuente route-map interfaz Nonat FastEthernet0 / 0 sobrecarga
access-list 110 denyip 10.0.10.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 110 del IP del permiso 10.0.10.0 0.0.0.255 cualquier
permiso de mapa de ruta Nonat 10
  IP address partido 110
```

Capítulo 18. PPTP VPN

pfSense puede actuar como un servidor PPTP VPN como una de sus tres opciones de VPN. Esta es una opción atractiva porque el cliente está integrada en todas las versiones de Windows y OS X lanzado en la última década. Se puede también ofrecen servicios de paso a través de un servidor PPTP interno.

Para una discusión general de los diversos tipos de VPN disponibles en pfSense y sus pros y sus contras, ver Capítulo 16, Redes Privadas Virtuales.

PPTP Advertencia de seguridad

A pesar de la atracción de su conveniencia, PPTP no debe ser utilizado bajo ninguna circunstancia, ya ya no es seguro. Esto no es específico a la aplicación de PPTP en pfSense, cualquier sistema que maneja PPTP ya no es segura. La razón de la inseguridad se debe a que se basa en PPTP MS-CHAPv2 que ha sido completamente comprometida. Si usted continúa usando PPTP ser conscientes de que tráfico interceptado puede ser descifrado por un tercero, el 100% de las veces, por lo que debe ser considerado sin cifrar. Le recomendamos encarecidamente migrar a otro tipo de VPN como OpenVPN o IPsec tan pronto como sea posible. Más información sobre el compromiso de seguridad PPTP se puede encontrar en https://isc.sans.edu/diario / fin + de + Days + de + MS-CHAPv2/13807 y https://www.cloudcracker.com/blog/2012/07/29/cracking-MS-CHAP-V2 /.

Si no lo ha hecho, debería leer la sección llamada "criptográficamente seguro" sobre VPN seguridad. PPTP es ampliamente utilizado, pero no es una solución VPN segura.

PPTP y reglas de firewall

Por defecto, cuando se tiene la redirección PPTP o el servidor PPTP está habilitado, las reglas de firewall ocultos se agregará automáticamente a la WAN para permitir TCP 1723 y el tráfico GRE de cualquier fuente para la dirección de destino. Puede desactivar este comportamiento en pfSense 1.2.3 y versiones posteriores mediante la comprobación
el cuadro de todas las reglas de VPN auto-añadido en Deshabilitar en Sistema Avanzado. Es posible que desee hacer esto si
usted sabe que sus clientes PPTP se conectarán sólo de particulares redes remotas. Esto evita que posibles abusos de los hosts de Internet arbitrarios, pero en implementaciones donde los usuarios son móviles y voluntad se conecta desde numerosos lugares, es imposible conocer a todos los usuarios de subredes vendrán de modo apretando el conjunto de reglas no es práctico y causará dificultades para los usuarios.

PPTP y Multi-WAN

Desafortunadamente debido a la forma de PPTP funciona, y la forma PF funciona con el protocolo GRE, es sólo es posible ejecutar un servidor PPTP en la interfaz WAN que tiene su puerta de enlace predeterminada.

PPTP Limitaciones

El código de seguimiento de estado en el software de cortafuegos PF subyacente para el protocolo GRE sólo se puede realizar un seguimiento de un
sola sesión por IP públicas por servidor externo. Esto significa que si usted utiliza conexiones PPTP VPN, sólo uno interna de la máquina puede conectarse simultáneamente a un servidor PPTP en Internet. Un millar de máquinas se puede conectar simultáneamente a un millar de servidores PPTP diferentes, pero sólo uno a la vez a un de un solo servidor. El único trabajo disponible alrededor es utilizar varias direcciones IP públicas en el servidor de seguridad, uno por
cliente, o para utilizar varias direcciones IP públicas en el servidor PPTP externo. Esto no es un problema con otra tipos de conexiones VPN.

Esta misma limitación también significa que si se habilita el servidor PPTP o la funcionalidad de redirección, ningún cliente
Nados a su dirección IP de WAN será capaz de conectarse a cualquier servidor PPTP exterior. El trabajo en torno a a esto es a Nat acceso de Internet saliente de sus clientes a una dirección IP pública diferente.

Ambas de estas limitaciones son capaces de ser trabajado alrededor en la mayoría de entornos, y PPTP es un viejo, protocolo no seguro que realmente debería ser usada nunca más. Habíamos planeado para abordar esto en un futuro liberar, pero hasta el momento no han llegado a una solución viable, y dado el compromiso total de PPTP como protocolo de VPN, es poco probable que valdría la pena cualquier esfuerzo gastado en intentar arreglar el problema.

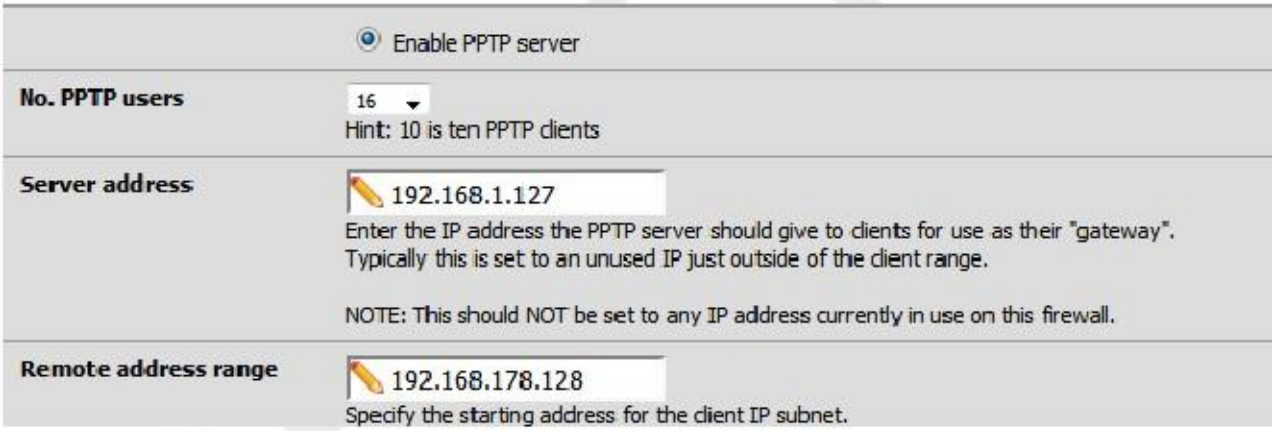
Configuración del Servidor PPTP

Si aún desea utilizar PPTP, a pesar de los problemas de seguridad, y luego configurar el servidor PPTP, primero de exploración para VPN PPTP. Seleccione Activar servidor PPTP.

Direccionamiento IP

Usted tendrá que decidir cuáles son las direcciones IP que puede utilizar para el servidor PPTP y clientes, y ahora muchos clientes simultáneos que desea apoyar. El campo N º usuarios PPTP controla cuántos usuarios PPTP ser permitido para conectar al mismo tiempo, en este ejemplo se seleccionaron 16. El rango de direcciones remota suele ser una parte de la subred LAN, como 192.168.1.128/28 (0.128 a través de 0.143). Estos son los direcciones que se asignará a los clientes cuando se conectan. A continuación, seleccione una dirección IP fuera de ese rango
para la dirección del servidor, tales como 192.168.1.127 como se muestra en la Figura 18.1, "IP PPTP Direccionamiento".

Figura 18.1. PPTP direccionamiento IP



Nota

Esta subred no tiene que estar contenida dentro de una subred existente en su router. Usted puede utilizar un conjunto completamente diferente de direcciones IP si se desea.

Autenticación

Puede autenticar a los usuarios de la base de datos local, o por medio de RADIUS. RADIUS le permite conectarse a otro servidor de la red para proporcionar autenticación. Esto puede ser usado para autenticar Usuarios de PPTP de Microsoft Active Directory (consulte la sección "Autenticación RADIUS con Windows Server "), así como numerosos otros servidores capaces RADIUS.

Si se usa RADIUS, active la casilla Utilizar un servidor RADIUS para la autenticación y el cuadro de rellenar el RADIUS
servidor y el secreto compartido. También puede agregar un segundo servidor RADIUS para usar en caso de que la primera falle.
usuarios en la ficha Usuarios de la VPN Pantalla de PPTP a menos que use RADIUS. Vea la sección llamada Para la autenticación utilizando la base de datos de usuarios local, deje esa casilla sin marcar. Usted tendrá que añadir su "Cómo agregar usuarios" a continuación para obtener más detalles sobre el sistema de autenticación integrada.

Requerir cifrado de 128 bits

Usted debe requerir el cifrado de 128 bits cuando sea posible. La mayoría de los clientes PPTP compatibles con el cifrado de 128 bits,
por lo que este debe estar bien en la mayoría de entornos. PPTP es relativamente débil en 128 bits, y mucho más

por lo que en 40 y 56 bits. A menos que sea absolutamente necesario, nunca se debe utilizar nada menos que 128 bits con PPTP, e incluso entonces tenga en cuenta que el tráfico PPTP puede ser descifrado por un atacante si lo interceptan.

Guardar cambios para iniciar el servidor PPTP

Después de rellenar los elementos antes mencionados, haga clic en Guardar. Esto guardará la configuración y puesta en marcha
el servidor PPTP. Si se autentica a los usuarios con la base de datos de usuarios locales, haga clic en la ficha Usuarios e introduzca sus usuarios allí.

Configurar reglas de firewall para clientes PPTP

Vaya a Cortafuego Reglas y haga clic en la ficha PPTP VPN. Estas reglas controlan lo que el tráfico es permitido de clientes PPTP. Hasta que se agrega una regla de firewall que aquí, todo el tráfico iniciado desde clientes PPTP conectados
será bloqueado. Tráfico iniciada desde la LAN a los clientes PPTP se controla mediante la red LAN
las reglas del cortafuegos. Inicialmente es posible que desee agregar una regla de permitir a todos aquí con fines de prueba, como se muestra en
Figura 18.2, "PPTP VPN Firewall Rule", y una vez que verifica la funcionalidad, restringir el conjunto de reglas como deseada.

Figura 18.2. PPTP VPN Firewall Rule

Adición de usuarios

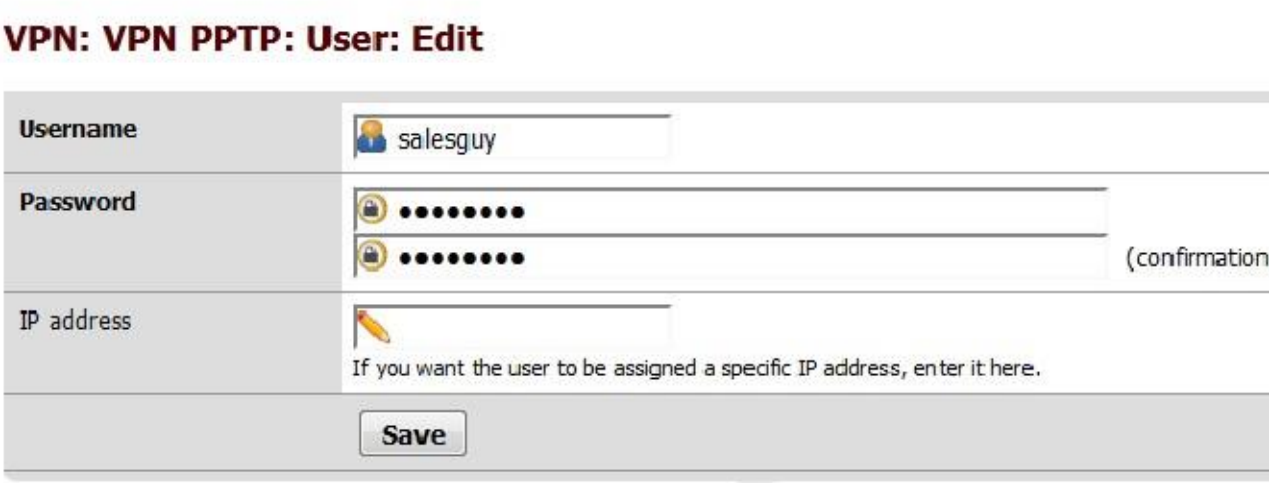
Adición de usuarios a través de RADIUS variará de una aplicación a otra. Este hecho hace que sea más allá
el alcance de esta sección, pero que deberían estar cubiertos en la documentación para el servidor RADIUS en particular tener un empleo.

Adición de usuarios al sistema de usuarios de PPTP integrado de pfSense es bastante fácil. En primer lugar, haga clic en VPN PPTP, y
a continuación, en la pestaña Usuarios. Se le mostrará una pantalla de usuarios vacía como se muestra en la Figura 18.3, "PPTP Usuarios Tab ". Haga clic en el botón para añadir un usuario.

Figura 18.3. PPTP Tab Usuarios

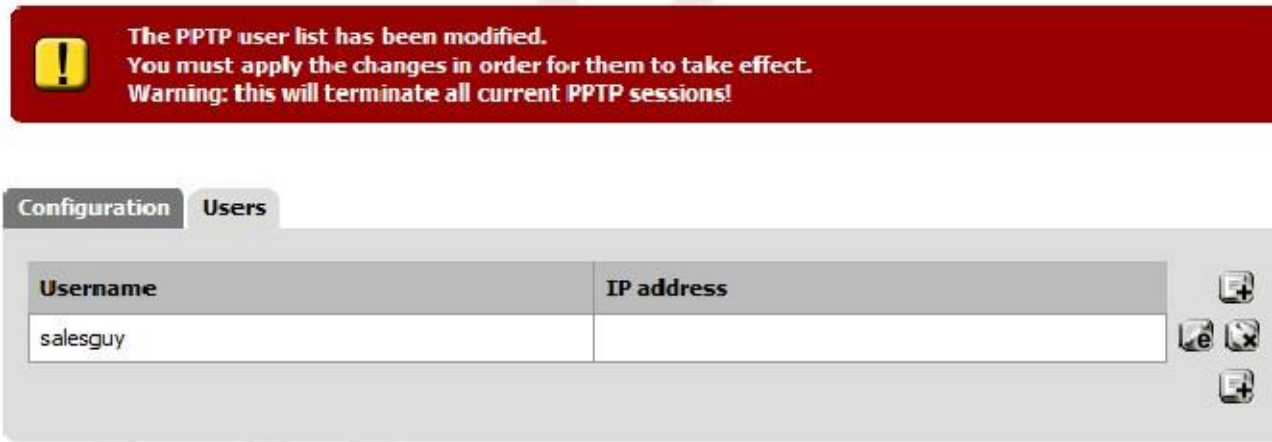
Después de hacer clic, aparecerá la página de edición del usuario. Rellenar con el nombre de usuario y una contraseña para una
usuario, como en la Figura 18.4, "Adición de un usuario PPTP". También puede introducir una asignación de IP estática si se desea.

Figura 18.4. Adición de un usuario de PPTP



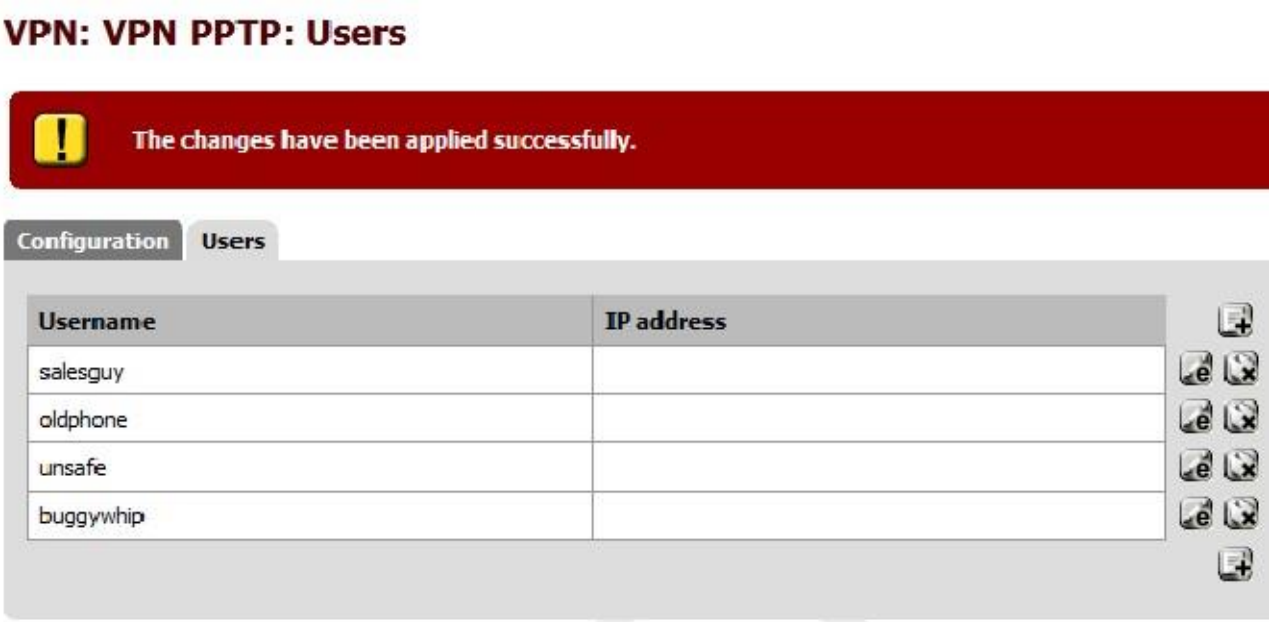
Haga clic en Guardar y, a continuación, la lista de usuarios volverá (Figura 18.5, "Aplicación de PPTP Cambios"), pero antes de la
cambio entrará en vigor, el botón Apply Changes primero hay que hacer clic.

Figura 18.5. Aplicación de cambios PPTP



Repita este proceso para cada usuario que desea agregar, finalmente, tendrá un lugar completo buscando
lista de usuarios, como en la Figura 18.6, "Lista de Usuarios PPTP".

Figura 18.6. Lista de Usuarios PPTP



Si necesita modificar un usuario existente, haga clic en . Los usuarios pueden eliminar haciendo clic .

Configuración del cliente PPTP

Ahora que su servidor PPTP está configurado y listo, tendrá que configurar los clientes PPTP.
Las siguientes secciones proporcionan instrucciones acerca de la configuración de Windows XP, Windows Vista y Mac OS X para conexión a un servidor PPTP.

Windows XP

Abra el Panel de control y haga doble clic en Conexiones de red (Figura 18.7, "Conexiones de red").

Figura 18.7. Conexiones de red

En Tareas de red, haga clic en Crear una nueva conexión (Figura 18.8, "Tareas de red"). En la acogida pantalla del asistente, haga clic en Siguiente.

Figura 18.8. Tareas de red

Seleccione Conectarse a la red de mi lugar de trabajo, como en la Figura 18.9, "Conexión de lugar de trabajo", y haga clic en
Siguiente.
Seleccione Conexión de red privada virtual, como en la Figura 18.10, "Conectar a VPN", a continuación, haga clic en Siguiente.

Introduzca un nombre para la conexión en Nombre de la empresa, al igual que en la Figura 18.11, "Nombre de conexión",
y haga clic en Siguiente.

Introduzca la IP WAN del router pfSense remoto bajo Nombre de host o dirección IP, al igual que la figura 18.12, "Conexión de host", y haga clic en Siguiente, haga clic en Finalizar (Figura 18.13, "Finalización de la conexión").

Ahora dispone de una entrada de acceso telefónico PPTP que funciona como cualquier otro tipo de conexión de acceso telefónico. Un mensaje para el
nombre de usuario y contraseña, al igual que en la Figura 18.14, "Conectar Dialog", se mostrarán cuando el inicial la conexión se intenta. Lo mejor es no conectar aún, sin embargo. Cancelar este cuadro de diálogo si aparece y trata de nuevo después de seguir el resto de esta sección.

Figura 18.15. Propiedades de la conexión

Hay algunos otros ajustes que necesita verificarse y tal vez ajustados. Desde dentro de la Red
Conexiones, haga clic derecho sobre el icono de la conexión PPTP, a continuación, haga clic en Propiedades (Figura 18.15,
"Propiedades de conexión").
Haga clic en la ficha Seguridad (Figura 18.16, "Ficha Seguridad"). Bajo Verificar mi identidad como sigue, hacer se elige una contraseña segura que requieren asegurado. 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 18.17, "Ficha Trabajo en red", el tipo de VPN desplegable defecto Automático. Lo que esto realmente significa es "probar cosas hasta funciona algo." PPTP es lo último que Windows intentará, y habrá una demora de hasta 30 segundos o más, mientras que espera a que el resto de opciones de tiempo de espera, por lo que probablemente desea seleccionar PPTP aquí para evitar que el retraso
y las complicaciones que pueden surgir de la metodología automática de Windows.

Por defecto, esta conexión le enviará todo el tráfico a través de la conexión PPTP como su puerta de enlace. Este puede o no ser deseable, dependiendo de la configuración deseada. Este comportamiento es configurable,
sin embargo. Para cambiar esto, haga doble clic en Protocolo de Internet (TCP / IP) y haga clic en el botón Opciones avanzadas.
Usar Ahora desmarque puerta de enlace predeterminada en la red remota como en la Figura 18.18, "Gateway Remote Setting",
a continuación, haga clic en Aceptar en todas las ventanas abiertas. Con esta opción desactivada, sólo el tráfico con destino a la subred
de la conexión PPTP atraviese el túnel.

Ahora la conexión PPTP sólo enviará el tráfico destinado a su subred a través de la VPN. Si usted necesita para enrutar el tráfico de forma selectiva, vea la sección "Trucos PPTP de ruta".

Windows Vista

Figura 18.19. Conexiones de red Vista

Haga clic en el icono indicador de conexión de red en la bandeja del sistema junto al reloj, a continuación, haga clic en Conectar
Desconecte o como se ve en la Figura 18.19, "Conexiones de red" Vista.

Haga clic en Configurar una conexión o red (Figura 18.20, "Configuración de una conexión"), a continuación, haga clic en Conectar a un
lugar de trabajo (Figura 18.21, "Conectar a un lugar de trabajo") y luego en Siguiente.

Figura 18.20. Configuración de una conexión

Figura 18.21. Conectarse a un lugar de trabajo

Si se le solicita, elija No, crear una nueva conexión y haga clic en Siguiente.

Haga clic en Usar mi conexión a Internet (VPN) (Figura 18.22, "Conectar vía VPN").

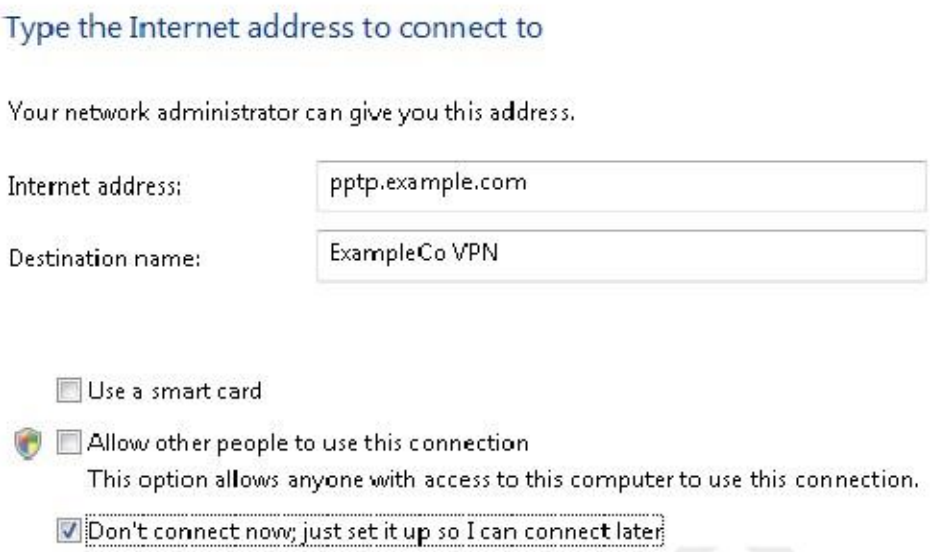
Figura 18.22. Conectar mediante VPN

En la siguiente pantalla, se muestra en la Figura 18.23, "Configuración de la conexión", introduzca la IP WAN del mando a distancia
enrutador pfSense bajo dirección de Internet.

Introduzca un nombre para la conexión con el nombre de destino.

Revise No conecte ahora y haga clic en Siguiente.

Figura 18.23. Configuración de la conexión



Introduzca el nombre de usuario y contraseña, como en la Figura 18.24, "Configuración de autenticación", haga clic en Crear.
Una pantalla similar a la Figura 18.25, "La conexión está listo" debe aparecer lo que indica que la conexión tiene ha creado.

Figura 18.24. Configuración de autenticación

Figura 18.25. La conexión está listo

Ahora debería tener una entrada de acceso telefónico PPTP que funciona como cualquier otro tipo de conexión de acceso telefónico. Rápidamente
acceder haciendo clic en el icono indicador de conexión de red en la bandeja del sistema, haga clic en Conectar o Desconectar, seleccione la conexión VPN, y haga clic en Conectar.

Sin embargo, antes de conectar por primera vez, hay algunos otros ajustes a comprobarlo. 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 en la conexión VPN que se acaba de crear, haga clic en Propiedades como se demuestra en Figura 18.26, "Get Propiedades de la conexión".

Cambie a la ficha de seguridad (Figura 18.27, "Configuración de VPN de seguridad"). Bajo Verificar mi identidad como siguiente, asegúrese de que se selecciona Requerir una contraseña segura. Asegúrese también de que Requerir cifrado de datos
(Desconectar si no hay) esté marcada.

Figura 18.27. Configuración de VPN de seguridad

Ahora cambie a la pestaña Funciones de red (Figura 18.28, "Configuración de red VPN"). Es probablemente el mejor para
desmarque Protocolo de Internet versión 6 (TCP/IPv6) en este punto.

El Tipo de VPN desplegable defecto Automático. Lo que esto realmente significa es "probar cosas hasta algo que funciona ". PPTP es lo último que Windows intentará, y habrá un retraso de hasta 30 segundo o más mientras espera a que el resto de opciones de tiempo de espera, por lo que probablemente desea seleccionar PPTP aquí
para evitar que el retraso y las complicaciones que pueden surgir de la metodología automática de Windows.

Al igual que con Windows XP, esta conexión le enviará todo el tráfico a través de la conexión PPTP como su puerta de enlace. Esto puede o no puede ser conveniente, dependiendo de la configuración deseada. Si desea todo el tráfico para ir a través del túnel, omita el resto de esta sección. De lo contrario, haga clic en Protocolo de Internet Versión 4 (TCP/IPv4) y, a continuación, haga clic en Propiedades.

Figura 18.28. Configuración de red VPN

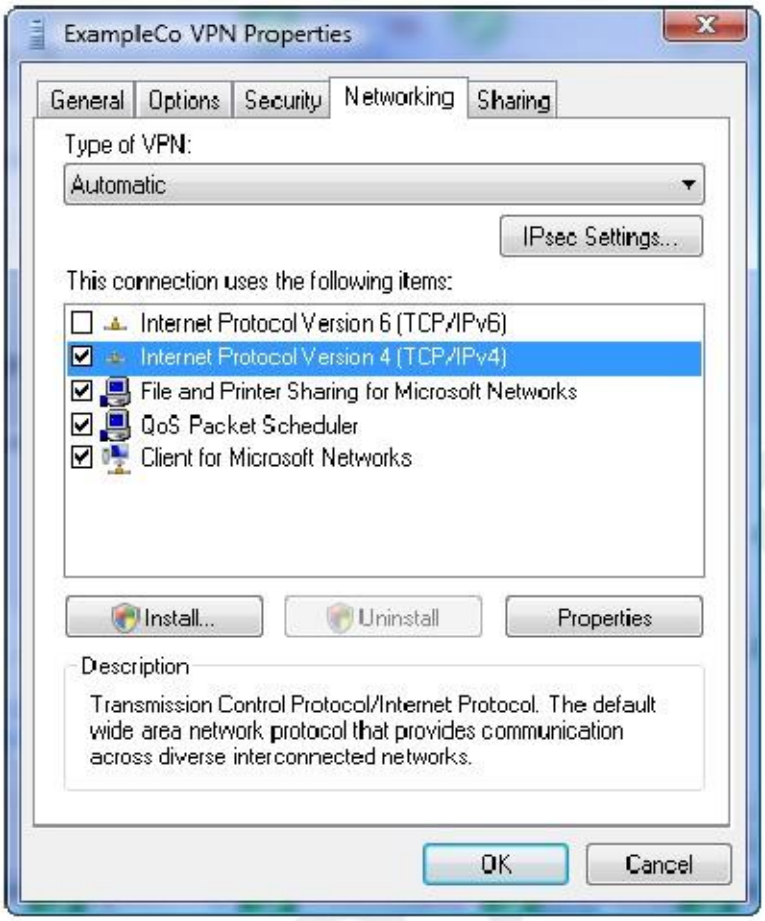
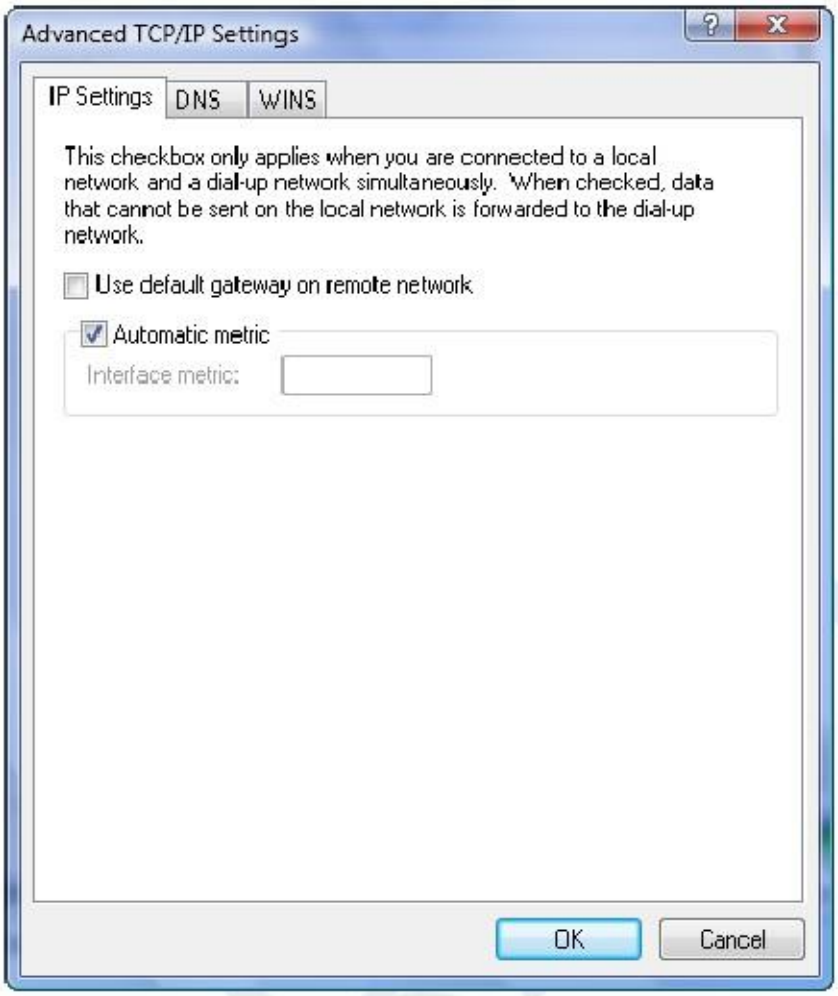


Figura 18.29. Gateway VPN



Haga clic en el botón Opciones avanzadas y, a continuación, desactive la casilla Usar puerta de enlace predeterminada en la red remota como se muestra en
Figura 18.29, "VPN Gateway". Haga clic en Aceptar o en Cerrar en todas las ventanas que se acaban de abrir.

Ahora la conexión PPTP sólo enviará el tráfico destinado a su subred a través de la VPN. Si usted necesita para enrutar el tráfico de forma selectiva, vea la sección "Trucos PPTP de ruta".

Windows 7

El procedimiento de instalación del cliente PPTP en la versión de lanzamiento (RTM) de Windows 7 es prácticamente idéntico al
Windows Vista.

Mac OS X

Abra Preferencias del Sistema, 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 se puede ver en la Figura 18.30, "Agregar red conexión ".

Figura 18.30. Añadir conexión de red

En la caída de la interfaz de abajo, seleccione VPN y para Tipo de VPN seleccione PPTP. Escriba el nombre de servicio como
que desee y haga clic en Crear. Estas opciones se muestran en la Figura 18.31, "Agregar conexión PPTP VPN"

Figura 18.31. Agregar conexión PPTP VPN

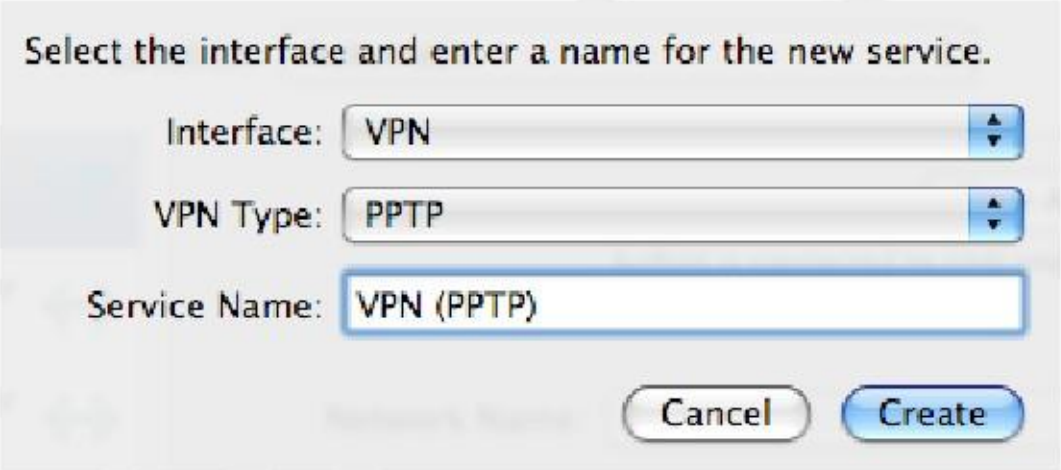
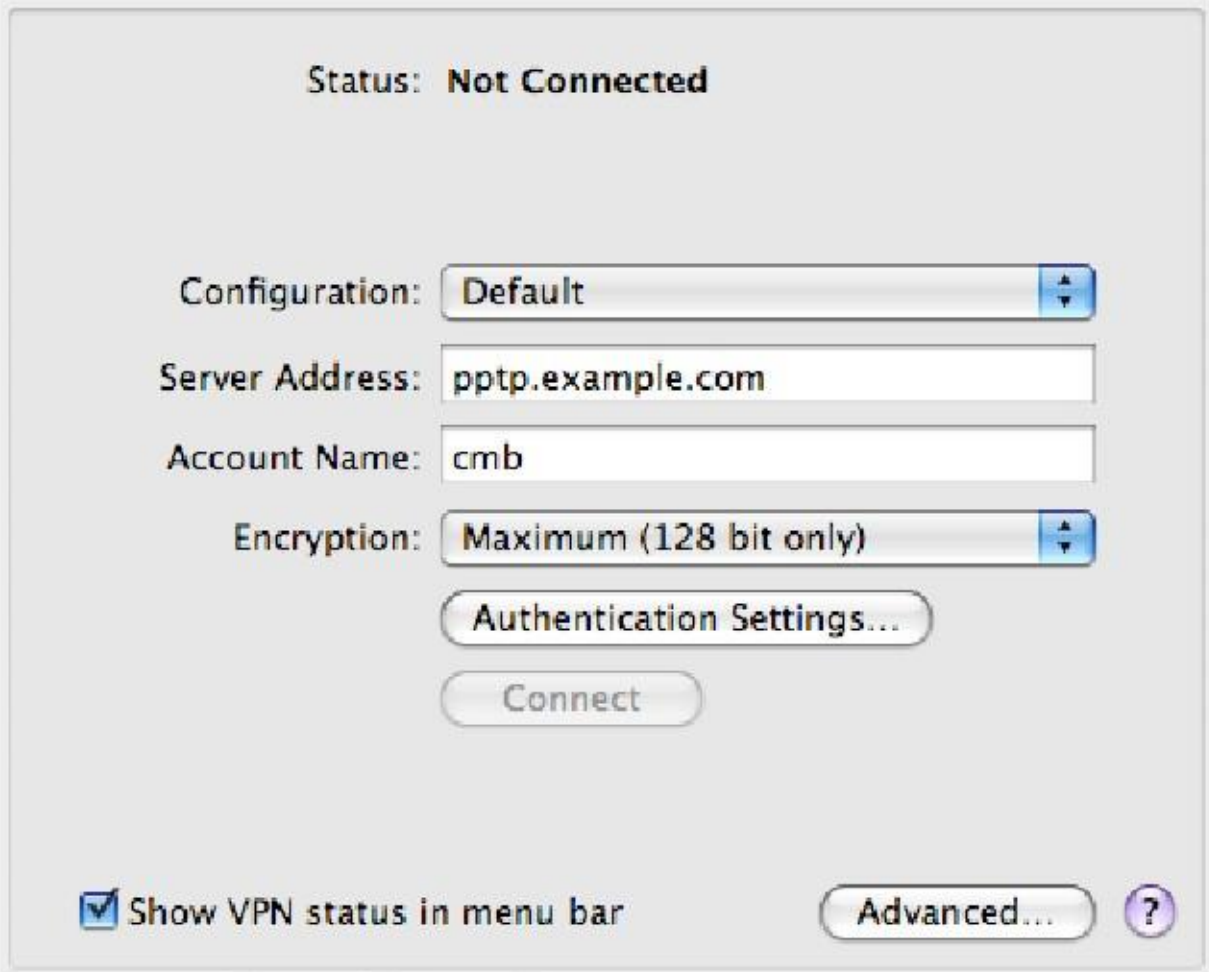


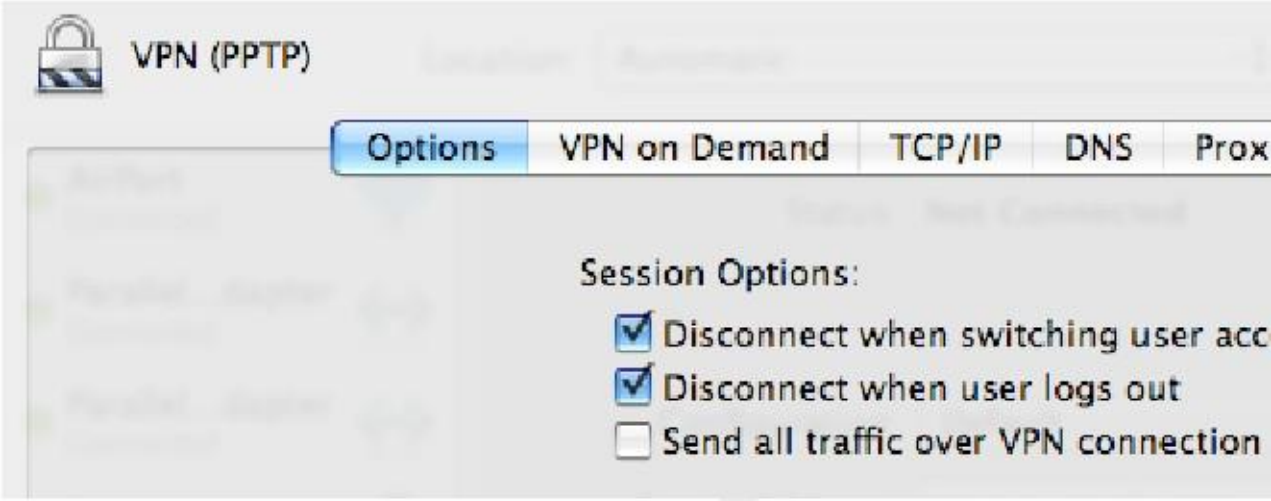
Figura 18.32. Configurar la conexión PPTP VPN



Esto le llevará de nuevo a la pantalla de la red en la que termine de configuración para el PPTP VPN conexión. Introduzca la dirección del servidor, nombre de cuenta y elija máxima (128 bits) para Cifrado. Un ejemplo se muestra en la Figura 18.32, "Configuración PPTP VPN de conexión". Luego, haga clic el botón Opciones avanzadas.

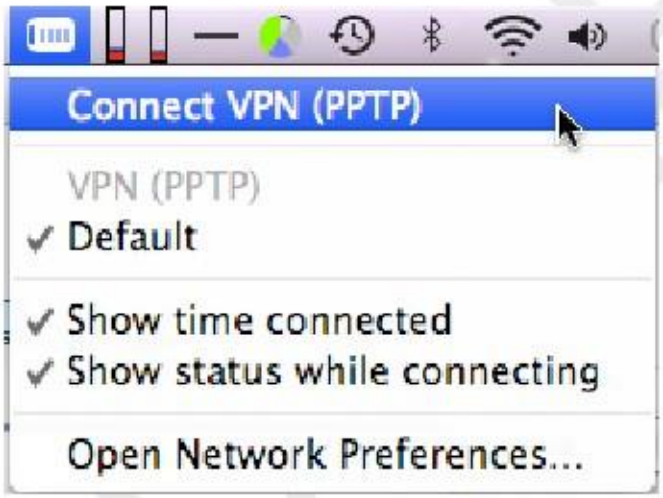
La pantalla avanzada tiene un número de opciones, algunos de ellos se muestra en la Figura 18.33, "avanzada opciones ", aunque sólo uno es posible que desee considerar el cambio. La función Enviar todo el tráfico a través de VPN caja de conexión está desactivada de forma predeterminada. Si usted quiere todo el tráfico desde el cliente al atravesar la VPN
mientras está conectado, marque esta casilla. Haga clic en Aceptar cuando haya terminado.

Figura 18.33. Opciones avanzadas



Desde que me registré Mostrar estado de VPN en la barra de menú, tal como se muestra en la Figura 18.32, "Configuración PPTP VPN
conexión ", mi conexión ahora muestra en la parte superior de la pantalla. Para conectar, haga clic en el nombre de su conexión como la que se observa en la Figura 18.34, "Conectar a PPTP VPN".

Figura 18.34. Conecte con PPTP VPN



Redirección PPTP

Redirección PPTP permite reenviar el tráfico PPTP destinado a su WAN IP a una PPTP interno
servidor. Para activarla, seleccione Redirigir conexiones PPTP entrantes e introduce tu PPTP interno
IP del servidor en el cuadro de redirección PPTP. Esto es funcionalmente equivalente a la adición de las entradas de Port Forward
para el puerto TCP 1723 y el protocolo GRE a su servidor PPTP interno, que se puede hacer en su lugar si
lo prefiere. Su existencia es en gran parte un control sobre de m0n0wall, donde el IPFilter subyacente no lo hace
admite el reenvío del protocolo GRE. Se ha conservado debido a la familiaridad de los usuarios con m0n0wall
la función, y algunos usuarios prefieren la facilidad de una sola entrada en lugar de dos entradas delanteras portuarias.

Las reglas de firewall para el protocolo GRE y el puerto TCP 1723 se añaden automáticamente en la WAN. Haces
es necesario introducir cualquier regla de firewall utilizando la redirección PPTP, a menos que tenga Deshabilitar todos
añaden reglas VPN comprobados en Sistema Avanzado.

PPTP Solución de problemas

Esta sección cubre los pasos para solucionar los problemas más comunes que encuentran los usuarios con PPTP.

No se puede conectar

En primer lugar, asegurar el equipo cliente está conectado a Internet. Si esto tiene éxito, tome nota del error que está recibiendo por parte del cliente. De Windows (excepto Vista) proporcionará un código de error que le ayudará considerablemente en la reducción a los problemas potenciales. Windows Vista elimina este y por lo tanto hace dificultades para solucionar adecuadamente los fallos de conexión, pero por suerte los mismos códigos de error que tienen
estado alrededor por más de una década están de vuelta en Windows 7. No se recomienda la solución de problemas con Vista.
Para aquellos que utilizan clientes que no son Windows, las áreas problemáticas son generalmente los mismos, aunque es posible que
tiene que tratar a todos ellos para determinar el problema específico.

Error 619

Error 619 significa algo en el camino se está rompiendo su tráfico GRE. Esto casi siempre se debe por el firewall del cliente está detrás. Si el cliente también está detrás de pfSense, primero asegúrese de que ninguno de los
escenarios descritos en la sección titulada "Limitaciones" PPTP aplican. Si el firewall del cliente está detrás es otro producto, es posible que tenga que habilitar passthrough PPTP o un ajuste similar para PPTP para funcionar, si se puede en absoluto. En algunos casos, como proveedores de servicios inalámbricos 3G asignación de IPs privadas a los clientes, lo harás
estar pegado a elegir otra opción de VPN.

Error 691

Error 691 se produce por un nombre de usuario o contraseña no válidos. Esto significa que el usuario no está entrando en la correcta
nombre de usuario o contraseña en el cliente PPTP. Corrija el nombre de usuario y / o contraseña, en correspondencia con
la información configurada en la base de datos de usuario local para PPTP, o en el servidor RADIUS.

Error 649

Usted puede ver el error 649 al autenticarse en el servidor RADIUS de Microsoft Windows con las NIC. Esto significa que la cuenta no tiene permiso para marcar, y la causa probable que sea uno de los tres cosas.

. 1 Marque en el permiso establecido en "Denegar acceso" - vaya a las propiedades de la cuenta del usuario en Active Usuarios y equipos y haga clic en la ficha Marcado. Dependiendo de su NIC preferida configuración, tendrá que ya sea Permitir el acceso o Controlar el acceso a través de control remoto política de acceso.

. 2 la contraseña del usuario ha caducado - si ha caducado la contraseña del usuario, que no pueden iniciar sesión en más de PPTP.

3 Configuración incorrecta NIC -. Usted puede haber configurado directivas de acceso remoto en IAS como tal que los usuarios no están autorizados a conectarse.

Conectado con PPTP, pero no puede pasar tráfico

Asegúrese de que ha añadido reglas de firewall para la interfaz PPTP VPN como se describe en la sección llamada "Configurar normas 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 conectado es También 192.168.1.0/24, el tráfico destinado a esa subred nunca atravesar el VPN, ya que está en la red local. Es por esto que es importante elegir una subred LAN relativamente oscuro cuando se utiliza VPN, como se discutió en la sección llamada "Configuración de la interfaz LAN".

Trucos PPTP enrutamiento

Si sólo desea subredes seleccionadas para ser enrutados a través del túnel PPTP, todavía se puede hacer con un poco de Comandos de ruta personalizada en el cliente. La siguiente técnica funciona bajo Windows XP, Vista, y

De Windows 7, pero probablemente se puede alterar para trabajar en la mayoría de cualquier plataforma. Esto supone que tiene
ya configurado el cliente no envía todo el tráfico a través de la conexión (es decir, no con el control remoto puerta de enlace).

En primer lugar, es necesario que el cliente PPTP para asignar una dirección estática en el perfil de usuario. Esto se puede hacer usando el
autenticación integrada, o por medio de RADIUS. Esta dirección estática debe ser fuera de la asignación general de piscina ya que esta no es una reserva.

El truco consiste en dirigir el tráfico con destino a las subredes remotas a la dirección PPTP asignado. Esta voluntad causar tráfico para esas subredes para viajar en el túnel hasta el otro lado. No se limita a las subredes que están inmediatamente accesible en el otro lado, o bien, como cualquier subred puede ser utilizado. Esto es útil si desea también acceso a la ruta a 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 apagado
ruta   añadir 192.168.210.0 enmascarar 255.255.255.0 192.168.1.126
ruta   añadir10.99.99.0 enmascarar 255.255.255.0 192.168.1.126
ruta   añadir172.16.1.0 enmascarar 255.255.252.0 192.168.1.126
pausa
```

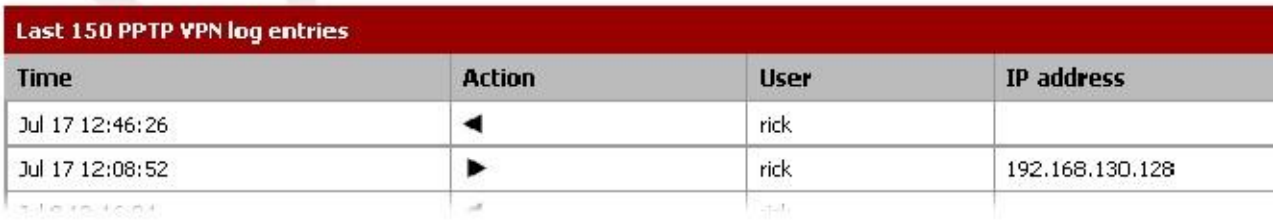
En ese ejemplo, 192.168.1.126 es la IP estática asignada a este nombre de usuario especial del cliente PPTP. Estos comandos haría la ruta de los tres subredes especificadas a través de la conexión PPTP, además de la subred para la conexión en sí. La pausa es opcional, pero puede ayudar a asegurar que todas las rutas se han añadido correctamente. Necesitará el archivo por lotes que se ejecute cada vez que se establezca la conexión.

> **Nota**
>
> En Windows Vista y Windows 7, será necesario ejecutar como Administrador estos comandos. Si que ha creado un acceso directo a este archivo de proceso por lotes, sus propiedades pueden ser alterados por lo que siempre se ejecuta en ese
> manera. Alternativamente, puede hacer clic derecho sobre el archivo por lotes y seleccione Ejecutar como administrador.

Registros PPTP

Un registro de inicio de sesión y cierre de sesión de eventos se mantiene en estado Registros del sistema, en la ficha PPTP.

Figura 18.35. Registros PPTP



Como se observa en la Figura 18.35, "Registros PPTP", cada inicio de sesión y cierre de sesión se deben registrar con una marca de tiempo
y nombre de usuario, y cada inicio de sesión también se mostrará la dirección IP asignada al cliente PPTP.

Capítulo 19. OpenVPN

OpenVPN es un código abierto solución SSL VPN que puede ser utilizado tanto para el acceso remoto de clientes y sitio para la 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 posteriores. Cada conexión OpenVPN, si el acceso remoto o un sitio a otro, se compone de un servidor y un cliente. En el caso de VPNs de sitio a sitio, un servidor de seguridad actúa como el servidor y el otro como el cliente. No importa que posee firewall estos roles. Normalmente el firewall de la ubicación principal proporcionará conectividad de servidor remoto para todos lugares, cuyos firewalls están configurados como clientes. Esto es funcionalmente equivalente a la opuesta configuración - la ubicación principal configurado como un cliente que se conecta a los servidores que se ejecutan en el firewalls en las ubicaciones remotas.

Hay varios tipos de métodos de autenticación que se pueden utilizar con OpenVPN: clave compartida, X.509 (También conocido como SSL / TLS o PKI), autenticación de usuario a través de locales, LDAP, y RADIUS, o una combinación de X.509 y la autenticación de usuario. Para clave compartida, se genera una única clave que se utilizará en ambos lados. SSL / TLS implica el uso de un conjunto de confianza de certificados y claves. La autenticación de usuarios puede ser configurado con o sin SSL / TLS, pero su uso es preferible, cuando sea posible debido a la mayor seguridad es ofertas.
En este capítulo, la configuración de una instancia OpenVPN están cubiertos, así como un repaso a la Asistente OpenVPN servidor de acceso remoto, configuraciones de cliente, así como ejemplos de otro tipo de conexión escenarios.

Tenga en cuenta que mientras que OpenVPN es una SSL VPN, no es un "sin cliente" SSL VPN en el sentido de que comercial fabricantes de firewall comúnmente se refieren a ella. Usted tendrá que instalar el cliente OpenVPN en toda su cliente dispositivos. En realidad hay una solución VPN es verdaderamente "sin cliente", y esta terminología no es más que una estratagema de marketing. Para obtener más en profundidad el debate sobre SSL VPN, este post de Mateo novios, un Herramientas de IPsec y desarrollador de pfSense, desde los archivos de las listas proporciona alguna información excelente:
http://marc.info/?l=pfsense-support&m=121556491024595&w=2.
Para una discusión general de los diversos tipos de VPN disponibles en pfSense y sus pros y sus contras, ver Capítulo 16, Redes Privadas Virtuales.

OpenVPN y Certificados

Uso de certificados es el medio preferido para correr las VPN de acceso remoto, ya que le permite revocar el acceso a las máquinas individuales. Con claves compartidas, que o bien tienen que crear un servidor único y el puerto para cada cliente o distribuir la misma clave para todos los clientes. El primero llega a ser una gestión pesadilla, y este último es problemático en el caso de una clave comprometida. Si una máquina cliente es comprometido, robado o perdido, o de lo contrario desea revocar el acceso de una persona, debe volver a emitir la clave compartida para todos los clientes. Con las necesidades de un despliegue de PKI, si un cliente está en peligro, o tener acceso a ser revocado por cualquier otra razón, simplemente puede revocar el certificado de ese cliente. No hay otros clientes se ven afectados.

En las versiones de pfSense anteriores a 2.0, los certificados tienen que ser manejados fuera de la WebGUI. Comienzo con pfSense 2.0, la interfaz gráfica de usuario ahora incluye una interfaz de gestión certificado que está totalmente integrado con OpenVPN. Autoridades de certificación (CA) y los certificados de servidor se gestionan en el Administrador de certificados en la interfaz web, que se encuentra en el Sistema Administrador de Cert. Los certificados de usuario también se gestionan en la web interfaz, como parte de la administración de usuarios integrada encontrar en Sistema Administrador de usuarios. Los certificados pueden generarse para cualquier cuenta de usuario creada localmente en el router a excepción de la cuenta de administrador por defecto.
Para más información sobre la creación de una autoridad de certificación, los certificados y listas de revocación de certificados, consulte el Capítulo 8, Gestión de certificados.

OpenVPN e IPv6

OpenVPN es la solución más completa para la VPN IPv6 hasta ahora. Es posible conectar un OpenVPN a sitio túnel de sitio ya sea a una dirección IPv4 o una dirección IPv6, y el uso de declaraciones remotas adicionales,

puede tener que probar ambos. Puede pasar IPv4 e IPv6 en el interior de un túnel OpenVPN. IPv6 es soportado tanto en-sitio a sitio y los clientes móviles, y que puede ser utilizado para entregar IPv6 a un sitio que tiene sólo IPv4 conectividad. Con el fin de asegurar el apoyo de cliente móvil para IPv6, obtener el software de cliente de la Paquete OpenVPN cliente de exportación, o descargar un cliente basado en OpenVPN 2.3-BETA o más reciente. Como Al escribir estas líneas, el cliente 2.3 beta funcionaba bien, y algún cliente tales como la viscosidad fueron construyendo su
software en dicha versión del código.

Opciones de configuración de OpenVPN

En esta sección se describen todas las opciones disponibles con OpenVPN y cuando usted puede desear o necesitar para utilizarlos. Las secciones siguientes cubren ejemplos de configuración de sitio a sitio y acceso remoto VPN con OpenVPN, utilizando las opciones más comunes y una configuración mínima.

Opciones de configuración del servidor

En esta sección se describe cada opción de configuración en la pantalla del servidor OpenVPN Editar.

Deshabilitar este servidor

Marque esta casilla y haga clic en Guardar para conservar la configuración, pero no permitir que el servidor. El proceso para
se detiene este ejemplo, y todos los peers / clientes se desconectará de este servidor. Cualquier otro servidores activos se ven afectados.

Modo de servidor

Este es el papel para el servidor, que especifica cómo los routers o los usuarios se conectan a esta instancia del servidor. Cambiar esto también afectará a lo que van a aparecer las opciones en el resto de la página, así que las opciones sólo pertinentes
se muestran.

Peer to Peer (SSL / TLS)

Una conexión entre las redes locales y remotas que está garantizado por SSL / TLS. Esta opción ofrece aumento de la seguridad, así como la capacidad para el servidor para empujar comandos de configuración para el control remoto
pares router (Cuando se utiliza un 1: muchos setup estilo). Peer routers remotos también pueden tener certificados revocados
eliminar el acceso si se ve comprometida.

Peer to Peer (Shared Key)

Una conexión entre las redes locales y remotas que está garantizado por clave compartida. Esta elección es más fácil de instalar, pero es menos seguro. Si está en peligro una clave compartida, cualquier router o cliente utilizando esa clave compartida
tendrá que obtener una clave recién generada.

Acceso remoto (SSL / TLS)

Históricamente, la opción más común para OpenVPN, esta elección es una instalación de cliente móvil con per-certificados X.509 usuario. Al igual que con el tipo de conexión peer-to-peer SSL / TLS, utilizando este método ofrece aumento de la seguridad, así como la capacidad para el servidor de empujar comandos de configuración a los clientes. Los clientes móviles también se han revocado las claves para eliminar el acceso si está en peligro una clave, como un robo
o extraviado portátil.

Acceso remoto (Aut usuario)

Un servidor de acceso de cliente que no utiliza certificados, pero requiere que el usuario final para suministrar un nombre de usuario
y la contraseña al realizar una conexión. Esto no es recomendable a menos que su autenticación es manejados externamente por LDAP o RADIUS.

Acceso remoto (SSL / TLS + autenticación de usuario)

Esta es la opción más segura que se ofrece. No sólo obtener los beneficios de otra SSL / TLS opciones, pero también requiere un nombre de usuario y la contraseña desde el cliente cuando se conecta. Acceso de cliente

se puede quitar no sólo mediante la revocación del certificado, sino también por el cambio de la contraseña. Además, si un
clave comprometida no se descubre inmediatamente, el peligro se reduce debido a que es poco probable que el atacante tiene las claves y la contraseña. Cuando se utiliza el Asistente OpenVPN, este es el modo que es configurado durante ese proceso.

Protocolo

Seleccione TCP o UDP aquí. A menos que haya una razón que usted debe usar TCP, tales como la capacidad de pasar por alto muchos
firewalls mediante la ejecución de un servidor OpenVPN en el puerto TCP 443, debe utilizar UDP. Siempre es preferible utilizar los protocolos sin conexión cuando un túnel de tráfico. TCP es orientado a la conexión, con garantía entrega. Cualquier pérdida de paquetes se retransmiten. Esto puede sonar como una buena idea, pero la voluntad de rendimiento
degradar significativamente en las conexiones a Internet con mucha carga, o aquellos con pérdida de paquetes consistente,
debido a las retransmisiones TCP. Usted con frecuencia tienen el tráfico TCP en el túnel. Donde
usted ha TCP envuelto alrededor de TCP, cuando se pierde un paquete, tanto de los paquetes TCP perdidos exteriores e interiores
será re-transmitido. Ocurrencias infrecuentes de esto será imperceptible, pero la pérdida recurrente causarán significativamente menor rendimiento que si estuviera usando UDP. Usted realmente no desea la pérdida de paquetes de tráfico de la VPN encapsulado a ser retransmitido. Si el tráfico dentro del túnel requiere una entrega fiable,
seleccione un protocolo como TCP y que asegura que se encargará de sus propias retransmisiones.

Modo de Dispositivo

OpenVPN puede funcionar en uno de dos modos de dispositivo tun o tap. En versiones anteriores de pfSense, tun era supone, y sólo una configuración de enrutado era posible. En pfSense 2.0 y superiores, se puede elegir entre
el modo clásico enrutado tun, y el modo tap, que es capaz de cualquiera de enrutamiento o de puente. La primaria diferencia entre los dos es que tun trabaja en la capa 3 del modelo OSI, mientras que la llave es capaz de trabajar a OSI capa 2. No todos los clientes admiten el modo tap, usando tun es recomendable.

Interfaz

Esto le permite seleccionar qué interfaz, VIP, o grupo de conmutación por error que la instancia del servidor OpenVPN se
escuchar a las conexiones entrantes, y también que la interfaz del tráfico desde saldrá del servidor.
Si selecciona un tipo de carpa VIP, se detendrá la instancia OpenVPN cuando la CARPA VIP está en
modo de copia de seguridad. Esto se hace para evitar que la unidad de copia de seguridad desde el mantenimiento de las rutas no válidas o intentar
para hacer las conexiones de salida.

Puerto local

El puerto local es el número de puerto OpenVPN utilizará para escuchar. Sus reglas de firewall deben permitir el tráfico a este puerto, y se debe especificar en la configuración del cliente. El puerto para cada servidor debe ser único.

Descripción

Escriba una descripción para esta configuración del servidor, para su referencia.

Configuración de cifrado

Esta sección controla cómo se cifra el tráfico hacia y desde los clientes y validado.

Shared Key

Cuando se utiliza una instancia de clave compartida, puede comprobar el generar automáticamente un cuadro clave compartida
para hacer un duplicado de la llave, o desactive esa casilla para pegar en una clave compartida desde un túnel OpenVPN existente.
Si opta por generar la clave automáticamente, vuelva a la pantalla de edición para este túnel después de obtener
la clave que puede ser copiado en el router remoto.

TLS Autenticación

TLS o Transport Layer Security, proporciona autenticación de sesiones para garantizar la validez tanto del cliente y el servidor. Marque la casilla para habilitar la autenticación de paquetes TLS si se desea. Si usted no tiene un

clave TLS existente, puede dejar automáticamente generar una clave de autenticación TLS compartida facturado. Si usted tiene una clave existente, desactive esa opción y luego pegarlo en el cuadro que aparece. Si ha elegido para generar la clave automáticamente, vuelva a la pantalla de edición de este túnel más tarde para obtener la clave que pueden ser copiados al router remoto o cliente.

Peer entidad emisora de certificados

Aquí usted debe elegir la autoridad certificado utilizado para firmar el certificado de servidor para este OpenVPN instancia del servidor. Si no aparece ninguno en la lista, primero debe importar o generar una autoridad de certificación bajo el Sistema □ Administrador de Cert, en la ficha CA.

Peer lista de certificados revocados

Este campo opcional es para la lista de revocación de certificados (CRL) para ser utilizado por este túnel. Una CRL es básicamente una lista de certificados elaborados a partir de una CA, dado que ya no deberían ser considerados válidos. Esto podría ser debido a un certificado sean comprometidos o se pierde, por ejemplo, de un ordenador portátil robado, software espía
infección, etc Una CRL se crea ni se gestiona desde System □ Cert Manager, en el Certificado Ficha Revocación.

Certificado de servidor

Un certificado de servidor debe ser elegido para esta instancia del servidor OpenVPN. Si no aparece ninguno en la lista, primero debe importar o generar una autoridad de certificación bajo el Sistema □ Cert Manager, en los Certificados tab.

Parámetros DH Longitud

El Diffie-Hellman (DH) parámetros de intercambio de claves se utilizan para establecer un canal de comunicaciones canal. Ellos se pueden regenerar en cualquier momento, y no son específicos de una instancia de OpenVPN. Es decir, si va a importar una configuración de OpenVPN existente, no es necesario replicar los parámetros de DH desde el servidor anterior, se puede generar un nuevo conjunto de parámetros de DH. La longitud de la DH deseada parámetros pueden ser seleccionados desde el cuadro desplegable, ya sea 1024, 2048 o 4096.

Algoritmo de cifrado

Aquí es donde se selecciona el sistema de cifrado de cifrado que se utilizará para esta conexión. El valor predeterminado es
AES-128-CBC, que es AES 128 bit Cipher Block Chaining. Esta es una buena opción para la mayoría de los escenarios. Una situación común donde es posible que desee considerar la cifra a fondo esto es cuando usted está utilizando un acelerador de cifrado de hardware, tales como `glxsb` integrado en el hardware ALIX, o una `hifn` tarjeta. En estos casos, verá un mayor rendimiento mediante el uso de un hardware acelerado en cifra. Para ALIX u otro de hardware con `glxsb`, elegir AES-CBC-128. Para `hifn` hardware, escogió ninguna de las 3DES o Opciones AES. Vea la sección llamada "Crypto Hardware" para obtener más información sobre el uso de criptografía aceleradores.

Configuración de túnel

La sección de configuración del túnel rige cómo los flujos de tráfico entre el servidor y los clientes, incluyendo enrutamiento
y la compresión.

IPv4/IPv6 Túnel Red

Estos son los conjuntos de direcciones que se asignan a los clientes a conectar. Extremo del servidor de la Configuración OpenVPN utilizará la primera dirección en este grupo por su extremo de la conexión, y asignar direcciones adicionales a clientes conectados según sea necesario. Estas direcciones se utilizan para la comunicación directa
entre extremos del túnel, incluso cuando se conectan dos redes remotas existentes. Usted puede elegir cualquier que la subred como el tiempo que no está en uso a nivel local o en cualquier sitio remoto. Usted puede llenar ya sea en una IPv4
Túnel de red, una red de túneles de IPv6, tanto de ellos, o en el caso de un puente del grifo, ni.

Redireccionar pasarela

Al seleccionar esta opción obligará a todo el tráfico generado por el cliente para pasar a través del túnel VPN, tomando el relevo
como puerta de enlace predeterminada del cliente.

IPv4/IPv6 red local

Estos campos especifican qué redes locales deben ser accesible por los clientes VPN, si los hubiere. Una ruta para estas redes se empuja a los clientes que se conectan a este servidor. Si necesita rutas de más de una subred
de una familia en particular (IPv4 o IPv6), ingrese la primera subred aquí y vea la sección llamada "Custom Opciones de configuración "para obtener información sobre la adición de las subredes restantes. Esta función se basa en la
capacidad de empujar rutas para el cliente, por lo que para IPv4 sólo es válido en el contexto de SSL / TLS cuando un túnel
red más grande que un / 30 está en uso. Siempre se debe trabajar para IPv6 proporciona una demasiado pequeña máscara similares
no de lo establecido.

IPv4/IPv6 red remota

Esta opción sólo aparece si está utilizando una conexión de igual a igual tipo, y no se utiliza para móviles clientes. Si se especifica una subred aquí, una ruta a la subred a través del otro lado de esta conexión OpenVPN será añadido. Sólo puede entrar en una subred aquí. Si es necesario agregar más de una red remota
subred, introduzca la primera aquí y vea la sección llamada "Opciones de configuración personalizada" para obtener información
en la adición de las subredes restantes.

De conexiones concurrentes

Aquí usted puede configurar el número de clientes se pueden conectar simultáneamente a esta instancia del servidor OpenVPN
en cualquier momento dado.

Compresión

Esta casilla de verificación permite la compresión LZO para su tráfico OpenVPN. Si esta casilla está marcada, el tráfico que cruza la conexión OpenVPN se comprime antes de ser encriptado. Esto ahorra en
uso de ancho de banda para muchos tipos de tráfico, a expensas de una mayor utilización de la CPU tanto en el servidor y el cliente. Generalmente este impacto es mínimo, y se sugiere la habilitación de esta para casi cualquier uso de OpenVPN a través de Internet. Para conexiones de alta velocidad, tales como el uso de OpenVPN a través de una LAN, baja latencia alta velocidad WAN o red inalámbrica local, esto puede ser indeseable, ya que el retraso añadido por la compresión puede ser más que el retardo de salvado en la transmisión del tráfico. Si casi todos del tráfico que cruza la conexión OpenVPN ya está encriptada (como SSH, SCP, HTTPS,
entre muchos otros protocolos), no debe habilitar la compresión LZO porque los datos encriptados es no compresible y la compresión LZO causará un poco más de datos a transferir lo que lo haría
sin compresión. Lo mismo es cierto si tu tráfico VPN es casi en su totalidad los datos que ya es comprimido.

Tipo de Servicio

Si se elige esta opción, OpenVPN establecerá el valor de encabezado TOS IP de los paquetes de túnel para que coincida con el
Valor paquete encapsulado. Esto puede causar algo de tráfico importante ser manejado más rápido sobre el túnel,
a costa de algún menor de divulgación de información.

Comunicación Inter-Client

Si los clientes necesitan comunicarse entre sí, marque esta opción. Sin esta opción, pueden
sólo enviar tráfico al servidor (y de cualquier red conectada para los que tienen una ruta).

Duplicar Conexiones

Por defecto, OpenVPN asociará la dirección IP de su red de túneles con un certificado determinado
para una sesión dada. Si el mismo certificado se conecta de nuevo, se le asignará la misma dirección IP
y, o bien desconecte el primer cliente, o provocar un conflicto de IP donde recibirá adecuado ni cliente
datos. Esto es sobre todo por razones de seguridad, por lo que el mismo certificado no puede ser utilizado por varias personas

simultáneamente. Recomendamos que un certificado único ser utilizado para cada usuario que se conecta. De lo contrario,
si el cliente de un usuario se ve comprometida, no hay manera de revocar que un cliente solo, usted tendría que emitir certificados a todos los clientes. Si tiene que continuar con un juego que utiliza el mismo certificado en varios lugares, comprobar las conexiones duplicadas para permitir que el comportamiento no estándar de múltiples clientes usando
el mismo certificado.

Configuración del cliente

Estos ajustes se refieren a cómo los clientes se conectan a esta instancia Sever se comportarán.

IP dinámica

Al marcar esta casilla añade la flotador opción de configuración para la configuración de OpenVPN. Esto permite clientes conectados a retener su conexión si sus cambios de IP. Para los clientes en las conexiones a Internet donde los cambios de IP con frecuencia, o los usuarios móviles que normalmente se mueven entre diferentes Internet conexiones, tendrá que marcar esta opción. Cuando la IP del cliente es estática o rara vez cambia, no usando esta opción ofrece una mejora de seguridad mínimas.

Dirección piscina

Si marca esta opción, el servidor asignará una dirección IP del adaptador virtuales a los clientes de la subred especificada por la opción de túnel de red anteriormente. Si no selecciona esta opción, las direcciones IP se No se asignará de forma automática, y los clientes tendrán que establecer sus propias direcciones IP estáticas manualmente en
sus archivos de configuración del cliente.

DNS Dominio predeterminado

Si marca esta opción, aparecerá un campo donde se puede especificar el nombre de dominio DNS para ser asignado a los clientes. Para garantizar la resolución de nombres funciona correctamente para hosts de la red local donde Se utiliza la resolución de nombres DNS, debe indicar su nombre interno de dominio DNS aquí. Para Microsoft Entornos de Active Directory, esto por lo general debe ser su nombre de dominio de Active Directory.

Los servidores DNS

Si marca esta opción, puede especificar hasta cuatro servidores DNS para ser utilizada por el cliente, mientras que conectado a este servidor. Para los entornos de Microsoft Active Directory, este debe especificar su activo Los servidores DNS Directorio para la resolución de nombres correcta y autenticación cuando se conecta a través de OpenVPN.

Servidores NTP

Al marcar esta casilla le permitirá especificar hasta dos servidores NTP para sincronizar la hora en los clientes. Se puede ser una dirección IP o nombre de dominio completo.

Opciones NetBIOS

Cuando el NetBIOS sobre está marcada la opción TCP / IP, varios otros NetBIOS y WINS relacionada Activar Aparecerán opciones. Si la casilla no está seleccionada, se desactivan estas opciones. Las opciones adicionales están cubiertos a continuación.

Tipo de nodo

El tipo de nodo NetBIOS controla cómo funcionarán los sistemas Windows al resolver NetBIOS nombres. Por lo general es bien dejar que esto ninguno para aceptar el valor predeterminado de Windows. Las opciones disponibles incluyen
b-nodo (transmisiones), p-nodo (consultas de punto a punto de nombres a un servidor WINS), m-nodo (Broadcast a continuación, el nombre del servidor de consultas), y h-node (Servidor de nombre de la consulta, a continuación, de difusión).

Ámbito ID

A NetBIOS Scope ID proporciona un servicio de nombres extendida para NetBIOS sobre TCP / IP. Los NetBIOS ID de ámbito aísla el tráfico NetBIOS en una sola red sólo a los nodos con el mismo NetBIOS identificador de ámbito.

Servidores WINS

Al marcar esta casilla le permite configurar hasta dos servidores WINS para proporcionar a los clientes para acceder y navegar por los recursos de NetBIOS por nombre a través de la VPN.

Opciones personalizadas

Mientras que la interfaz web pfSense es compatible con todas las opciones más comúnmente utilizadas, OpenVPN es muy
potente y flexible y en ocasiones puede querer o necesitar usar opciones que no están disponibles en
la interfaz web. Usted puede completar estas opciones personalizados aquí. Estas opciones se describen adicionalmente en
la sección titulada "Opciones de configuración personalizada".

Uso del Asistente OpenVPN Server para De acceso remoto

El asistente OpenVPN es una forma cómoda de configurar una VPN de acceso remoto para clientes móviles. Lo le permite configurar todos los requisitos previos necesarios para un servidor de acceso remoto OpenVPN: Una fuente de autenticación, una autoridad de certificación, un certificado de servidor, y una instancia del servidor OpenVPN. Al final del asistente, usted debe tener un sever en pleno funcionamiento, listo para aceptar conexiones desde los usuarios. Un ejemplo de configuración se utiliza para ayudar en la explicación de las opciones disponibles en el asistente.

Antes de iniciar el asistente

Antes de iniciar el Asistente para configurar su servidor de acceso remoto, hay algunos detalles que usted necesita para planificar de antemano.

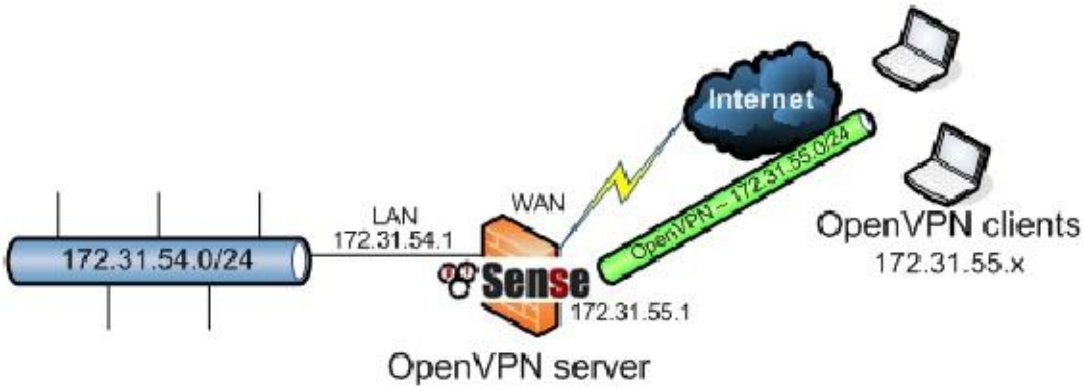
Determinar un esquema de direccionamiento IP

Además de las subredes internas que usted querrá clientes de acceso, tiene que elegir una subred IP
que se utilizará para las conexiones OpenVPN. Esta es la subred de lleno en menos de Dirección de la piscina en el servidor
configuración. Clientes conectados recibirán una dirección IP dentro de esta subred y el servidor final del
conexión también recibe una IP en esta subred, donde el cliente dirige el tráfico para las subredes enrutadas a través
la conexión de OpenVPN. Como siempre que la elección de las subredes internas para una sola ubicación, idealmente esta
subred debe ser summarizable CIDR con las subredes internas. La red de ejemplo representado aquí
utiliza 172.31.54.0/24 para LAN y 172.31.55.0/24 para OpenVPN. Estas dos redes se resumen
con 172.31.54.0/23, haciendo de enrutamiento más fácil de manejar. CIDR resumen se discute en
la sección llamada "CIDR Summarization".

Ejemplo de red

Figura 19.1, "Ejemplo de OpenVPN red de acceso remoto", muestra la red configurada en esta ejemplo.

Figura 19.1. Ejemplo OpenVPN red de acceso remoto



Seleccione Tipo de autenticación

En la primera pantalla del asistente del servidor de acceso remoto de OpenVPN, usted tiene que elegir un método para la autenticación de usuario. Las opciones disponibles para la autenticación backend tipo son de acceso de usuario local, LDAP y RADIUS. Si usted tiene un sistema de autenticación existente en el lugar, como Active Directory, es posible que desee elegir LDAP o RADIUS, dependiendo de cómo ese sistema está configurado. Usted puede elegir Acceso de usuario local si desea administrar los usuarios, contraseñas y certificados en el router pfSense. Si LDAP o RADIUS son elegidos, no se puede utilizar certificados por usuario sin generar externamente. Cuando se utiliza el acceso de usuarios local, puede usar certificados por usuario fácilmente, logró por completo en el GUI pfSense. Esto es mucho más seguro, pero dependiendo del número de usuarios que tendrá acceso a la servicio, puede ser menos conveniente que el uso de un sistema central de autenticación.

La opción de acceso de usuario local es el equivalente a la elección de acceso remoto (SSL / TLS + autenticación de usuario)
mencionado anteriormente en este capítulo. LDAP y RADIUS son equivalentes a los de acceso remoto (autenticación de usuario).
Después de seleccionar el tipo de servidor de autenticación, pulse Siguiente. Si se eligieron LDAP o RADIUS, el configuración del servidor para esas opciones aparecerá al lado. Si el acceso de usuarios local fue elegido, el LDAP y los pasos del asistente de RADIUS se omiten. Para nuestro ejemplo, será elegido de acceso de usuario local, pero la otras opciones son discutidos por la totalidad también.

La elección de un servidor LDAP

Si hay un servidor LDAP existente definido en el sistema de pfSense, usted puede elegir de la lista. Si desea utilizar un servidor LDAP diferente, es posible que en lugar de elegir Agregar nuevo servidor LDAP. Si no hay LDAP
servidores se definen en pfSense, este paso se omite.

Adición de un servidor LDAP

Si no existe ningún servidor LDAP o elige crear un nuevo servidor LDAP, una pantalla le presentará las opciones necesarias para agregar un nuevo servidor. Muchas de estas opciones dependerá de su LDAP específica configuración del directorio y estructura. Si no está seguro de cómo establecer un valor determinado, consulte a su LDAP administrador del servidor, proveedor de software o la documentación.

Nombre

Nombre descriptivo para este servidor LDAP, para su referencia.

Nombre de host o dirección IP

El nombre de host o dirección IP del servidor LDAP. Este servidor puede ser alcanzable en cualquier interfaz, lo hace no tiene que ser interno o conectado directamente.

Puerto

El puerto en el que puede estar en contacto con el servidor LDAP. El puerto por defecto es 389 para el estándar Conexiones TCP, y 636 para SSL, pero dependiendo de su implementación del servidor LDAP y configuración local, este puerto puede ser diferente. Consulte con su administrador de LDAP o software documentación para determinar el puerto adecuado.

Transporte

Los medios por los que se hará una consulta LDAP. Esto se puede configurar para TCP - Norma para cifrar conexiones o SSL - encriptado para conexiones seguras. Si el servidor LDAP se conecta localmente, es posible que prefiera utilizar una conexión estándar. Si el servidor es remoto o cruza cualquier red no confiable enlaces, que pueden preferir usar SSL. También debe asegurarse de que el servidor LDAP está configurado para escuchar para el tipo de conexión elegido.

Nivel ámbito de búsqueda

Selecciona la profundidad que desea buscar en el directorio LDAP. Usted puede elegir un nivel o en todo el Subárbol. Dependiendo de los otros parámetros escogidos, y la estructura de su directorio LDAP, puede que desee restringir las búsquedas a un nivel específico.

Search Scope Base DN

El nombre completo para que la búsqueda se basará a partir. Por ejemplo DC = ejemplo, DC = com

Contenedores de autenticación

Estos valores especifican qué parte del directorio que los usuarios se encuentran. Por ejemplo, puede ser CN = Users, DC = ejemplo.

Bind DN LDAP del usuario

El nombre completo de un usuario que se puede utilizar para enlazar con el servidor LDAP y realizar la la autenticación. Si se deja en blanco, se realizará un enlace anónimo, y la configuración de la contraseña a continuación se ignorarán.

Bind LDAP Contraseña

La contraseña que se utilizará con el Usuario Bind DN LDAP especificado anteriormente.

Nombrar usuario Atributo

Varía dependiendo de su software y estructura de directorios LDAP. Típicamente cn para OpenLDAP y Novell eDirectory y samAccountName para Microsoft Active Directory.

Naming Atributo de grupo

Varía dependiendo de su software y estructura de directorios LDAP, pero es lo más típicamente cn.

Nombrar miembro del atributo

Varía dependiendo de su software y estructura de directorios LDAP. Típicamente miembro en OpenLDAP, memberOf en Microsoft Active Directory, y uniqueMember en Novell eDirectory.

La elección de un servidor RADIUS

Si hay un servidor RADIUS existente definido en el sistema de pfSense, usted puede elegir de la lista.
Si desea utilizar un servidor RADIUS diferente, es posible que en lugar de elegir Agregar nuevo servidor RADIUS. Si hay servidores RADIUS se definen en pfSense, se salta este paso.

Adición de un servidor RADIUS

Si no existe ningún servidor RADIUS, o elige crear un nuevo servidor RADIUS, se presentará una pantalla con las opciones necesarias para agregar un nuevo servidor. Si no está seguro de cómo establecer un valor determinado, consulte a su
Administrador del servidor RADIUS, proveedor de software o la documentación.

Nombre

Nombre descriptivo para este servidor RADIUS, para su referencia.

Nombre de host o dirección IP

El nombre de host o dirección IP del servidor RADIUS. Este servidor puede ser alcanzable en cualquier interfaz, no tiene que ser interno o conectado directamente.

Puerto de autenticación

Puerto utilizado por el servidor RADIUS para la aceptación de solicitudes de autenticación, por lo general 1812, pero en algunos
implementaciones RADIUS antiguos pueden ser 1645.

Secreto compartido

El secreto compartido es la contraseña configurada en el servidor RADIUS para la aceptación de la autenticación las peticiones de la dirección IP de su enrutador pfSense.

La elección de una entidad emisora de certificados

Si hay una entidad emisora de certificados existente definido en el sistema de pfSense, puede elegir desde la lista. Si desea utilizar crear una nueva autoridad de certificación, en su lugar puede elegir Agregar nuevo CA. Si no hay autoridades de certificación se definen en pfSense, se salta este paso.

La creación de una autoridad de certificación

Este paso le permite crear una nueva autoridad de certificación (CA), y presenta todas las opciones que necesita. Se requiere que cada opción en esta página, y todos los campos deberá ser llenada correctamente para proceder. La CA se utiliza para establecer una base de confianza de la que los certificados de servidor se pueden generar y considerará "Confiable" por los clientes. Debido a que esta CA es auto-generada, sólo se puede confiar en los clientes que son También se suministra con una copia de este certificado de CA. Para obtener más información sobre la creación y la gestión de las entidades emisoras,
consulte la sección denominada "Autoridad de Gestión de certificados".

Nombre descriptivo

Un nombre para su referencia, para identificar este certificado. Esta es la misma como nombre de campo común para otros certificados. Por esta CA, llamaremos es ExampleCoCA. Aunque el uso de espacios en este campo es aceptable, no aconsejamos el uso de espacios en un campo Common Name. La razón principal es que
Los clientes tienden a tener problemas con nombres tan comunes.

Longitud de la clave

Tamaño de la clave que se generará. Cuanto mayor sea la clave, más seguridad es ofertas, pero teclas más grandes son generalmente más lento de usar. 2048 es una buena opción.

Vida

El tiempo en días que este CA será válida. En una CA auto-generado como este, se establece comúnmente a 3650, que es de aproximadamente 10 años.

Código País

De dos letras del código ISO del país (por ejemplo, EE.UU., AU, CA). Si no conoce su código de dos letras ISO del país, usted puede encontrarlo aquí http://www.iso.org/iso/english_country_names_and_code_elements. Desde nuestra ExampleCo empresa se encuentra en los Estados Unidos, vamos a entrar EE.UU..

Estado o Provincia

Estado completa del nombre Provincia, no abreviado (por ejemplo, Indiana, California). ExampleCo se encuentra en Kentucky, así que eso es lo que va a ser introducido.

Ciudad

Ciudad u otro nombre Localidad (por ejemplo, Indianapolis, Toronto). La sede de ExampleCo está en Louisville.

Organización

Nombre de la organización, a menudo el nombre de la empresa o grupo. ExampleCo iría aquí. Asegúrese de no utilizar caracteres especiales aquí, incluso puntuacion.

E-Mail

Dirección de correo electrónico para el contacto de certificados. A menudo, el e-mail de la persona que haya generado el certificado,
tal como vpnadmin@example.com.

La elección de un certificado de servidor

Si hay un certificado existente definido en el sistema de pfSense, usted puede elegir de la lista. Si
desean utilizar crear un nuevo certificado, es posible que en lugar de elegir Agregar nuevo Certificado. Si no hay certificados
se definen en pfSense, este paso se omite.

Adición de un certificado de servidor

Esta pantalla le permite crear un nuevo certificado de servidor, que se utiliza para verificar la identidad del servidor al clientes. El certificado de servidor será firmado por la autoridad de certificación elegido o creado previamente
en el asistente. En la mayoría de los casos, al igual que con nuestro ejemplo, la misma información de la etapa anterior es utilizado. Para obtener más información sobre la creación y administración de certificados, consulte la sección denominada "Certificado
Gestión ".

Nombre descriptivo

Este es el campo Common Name (CN) para el certificado de servidor, y también se utiliza para hacer referencia al certificado
en pfSense. Aunque el uso de espacios en este campo es aceptable, no aconsejamos el uso de espacios en un Campo Common Name. La razón principal es que los clientes tienden a tener problemas con nombres tan comunes.

Longitud de la clave

Tamaño de la clave que se generará. Cuanto mayor sea la clave, más seguridad que ofrece, pero teclas más grandes son generalmente más lento de usar.

Vida

Vida en día. Esto se establece comúnmente 3650 (Aproximadamente 10 años).

Código País

De dos letras del código ISO del país (por ejemplo, EE.UU.,
AU, CA)

Estado o Provincia

Estado completa del nombre Provincia, no abreviado (por ejemplo, Kentucky, Indiana, Ontario).

Ciudad

Ciudad u otro nombre Localidad (por ejemplo, Louisville, Indianapolis, Toronto).

Organización

Nombre de la organización, a menudo el nombre de la empresa o grupo. Asegúrese de no utilizar caracteres especiales aquí,
incluso puntuacion.

E-Mail

Dirección de correo electrónico para el contacto de certificados. A menudo, el e-mail de la persona que haya generado el certificado.

Configuración de los ajustes del servidor OpenVPN

Esta pantalla configurar cada aspecto de cómo el servidor OpenVPN en sí se comportará, así como opciones que se transmiten a los clientes. Las opciones que se presentan aquí son las mismas que las descritas anteriormente en la sección "Opciones de configuración de OpenVPN", que puede referirse a esa sección para obtener detalles sobre cada campo y la forma en que debe establecerse. Debido a que las opciones se han explicado en detalle anteriormente, sólo
se darán los ajustes para nuestro ejemplo.

General de OpenVPN Information Server

Estas opciones controlan las opciones específicas a la forma en que se ejecuta la instancia de OpenVPN en este router.

Interfaz

Dado que las conexiones entrantes serán desde el lado WAN, seleccione WAN.

Protocolo

El valor predeterminado de UDP es aceptable.

Puerto local

Esta será la primera instancia del servidor OpenVPN, por lo que el valor por defecto de 1194 se prefiere. Si usted tiene una
VPN existente, utilice un número de puerto diferente. El asistente le sugerirá un número de puerto no utilizado.

Descripción

Esto sera para el acceso de usuarios remotos, Clientes ExampleCo Mobile VPN es una descripción apropiada.

Configuración de cifrado

Ahora vamos a configurar los ajustes de encriptación para el túnel.

TLS Autenticación

Queremos utilizar TLS, así comprobar Habilitar la autenticación de paquetes TLS.

Generar TLS Clave

No tenemos una clave TLS existente, por lo que comprobar Generar automáticamente una autenticación TLS compartida clave.

TLS Shared Key

Dado que no tenemos una clave TLS existente, déjelo en blanco.

Parámetros DH Longitud

Seleccionar 2048, como debe ser un buen equilibrio entre velocidad y fuerza.

Algoritmo de cifrado

Esto se puede dejar en el valor predeterminado de AES-128-CBC, pero cualquier otra opción también trabajara bien siempre y cuando se establecen los clientes para que coincida.

Crypto Hardware

Si el dispositivo de firewall tiene un acelerador de hardware criptográfico, como un `hifn` tarjeta o el bordo `glxsb` en la plataforma de ALIX, puede elegir aquí. La mayoría de las tarjetas aceleradoras gancho en el uso del BSD motor crytpodev, por lo que en caso de duda, elija eso. Esta configuración permitirá OpenVPN para aprovechar de la aceleración de hardware. También debe utilizar un algoritmo de criptografía compatible con su acelerador. Para `glxsb,` eso es sólo AES-128-CBC. Moderno Tarjetas Hifn como el vpn1411 Soekris 3DES de apoyo y 128, 192 y 256 bits AES.

Configuración de túnel

Esta parte explica cómo se dirigirá el tráfico proveniente de los clientes remotos.

Túnel Red

Como en el diagrama en el inicio de este ejemplo, la subred 172.31.55.0/24 se ha elegido para los clientes VPN.

Redireccionar pasarela

Para los propósitos de ExampleCo, sólo queremos el tráfico en la VPN que está destinado para nuestros subredes en el oficina principal, por lo que este cuadro se dejará sin marcar.

Red Local

Esta sería la principal oficina de subred, que en nuestro ejemplo es 172.31.54.0/24.

De conexiones concurrentes

ExampleCo no quiere limitar el número de clientes que pueden conectarse al mismo tiempo, por lo que este se deja en blanco.

Compresión

Para mejorar el rendimiento del tráfico en el túnel VPN a expensas de algún poder de CPU, este cuadro ser facturado.

Tipo de Servicio

Este cuadro será sin control, como no debería haber ningún tráfico en esta VPN que sería necesario priorización / QoS.

Comunicación Inter-Client

Debido a que los clientes no deberían tener necesidad de conectarse a otros sistemas del cliente, este cuadro será sin marcar.

Duplicar Conexiones

Porque vamos a tener certificados únicos para cada cliente, este permanecerá sin marcar.

Configuración del cliente

Esta parte controla los ajustes específicos que se dan a los clientes que se conectan cuando se establece una conexión.

IP dinámica

Nuestros clientes se conectan desde todas partes del país y las redes de desconocidos, por lo que las direcciones IP son propensos a cambios sin previo aviso, por lo que esta opción debería ser facturado.

Dirección piscina

Queremos que los clientes a asignar direcciones de la red de túneles de arriba, así que esto debería ser facturado.

DNS Dominio predeterminado

Pondremos el dominio para ExampleCo aquí, example.com.

Servidores DNS

Para un servidor DNS para proporcionar el cliente, cualquier servidor DNS interno podría ser utilizado. ExampleCo tiene un
Controlador de dominio de Windows Active Directory, por lo que se utiliza aquí, 172.31.54.5.

Servidores NTP

El servidor de arriba también se puede utilizar para sincronizar los relojes de la PC del cliente, por lo que entrar en él aquí también:
172.31.54.5.

Opciones NetBIOS

Los clientes tendrán acceso a los recursos compartidos de Windows detrás de la VPN, por lo que queremos comprobar Habilitar NetBIOS
a través de TCP / IP.

Tipo de nodo NetBIOS

Porque nosotros también vamos a usar un servidor WINS y no las emisiones televisivas, seleccione
p-nodo.

NetBIOS Scope ID

Esto se deja en blanco, ya que no queremos limitar el alcance de NetBIOS.

Servidores WINS

El servidor de Windows anterior es también un servidor WINS, a fin de utilizarlo también en este caso:
172.31.54.5.

Avanzado

En este momento no se requieren ajustes adicionales, por lo que este puede dejarse en
blanco.

Regla Configuración del cortafuegos

En otras partes del firewall, de forma predeterminada todo el tráfico está bloqueado y no podrá conectarse a redes privadas virtuales o fallecimiento
más de túneles VPN. Esta pantalla le permite agregar reglas de firewall para permitir el tráfico de forma automática para conectarse a
la VPN, y también para los clientes conectados puede pasar el tráfico a través de la VPN.

El tráfico de los clientes al servidor

Marque esta casilla para agregar una regla de firewall en la interfaz elegida para el túnel que permite a los clientes se conectan.
Permite que todos los clientes se conecten de forma predeterminada, por lo que si tiene la intención de que sólo permite conexiones desde un limitado

un conjunto de direcciones IP o subredes, puede hacer su propia regla o marque esta casilla y cambiar la norma que crea. Como en nuestro ejemplo tenemos clientes que se conectan de todo el país, la norma creada
por esta opción es ideal, por lo que se comprobar esta casilla.

El tráfico de los clientes a través de un túnel VPN

Esta configuración permitirá que todo el tráfico para cruzar el túnel OpenVPN, que es lo que queremos hacer para este ejemplo, por lo comprobar esta casilla.

Fin del Asistente de

El asistente se ha completado, y el túnel debe estar completamente configurado y listo para las conexiones de clientes. Desde aquí, los próximos pasos serán para añadir usuarios y configurar los PC clientes. Si usted necesita para hacer cualquier
ajustes a las reglas de firewall generados automáticamente, ahora sería el momento de hacerlo.

Configuración de usuarios

En este punto, usted debe tener un túnel VPN configurado pero hay aún poco conocido pero de cualquier cliente que se puede conectar. El método para añadir usuarios a su VPN dependerá del método de autenticación
elegido al crear la instancia del servidor OpenVPN. Más detalles sobre la adición de usuarios se pueden encontrar en Capítulo 7, Gestión de usuarios y autenticación. Más información sobre la gestión de los certificados de usuario puede pueden encontrar en la sección llamada "Certificados de usuario".

Usuarios locales

Para agregar un usuario que pueda conectarse a OpenVPN, debe agregarlos en Sistema Administrador de usuarios.

Vaya a la página, a continuación, haga clic para agregar un nuevo usuario. Introduzca un nombre de usuario, una contraseña y la confirmación,
Escriba el nombre completo si lo desea. Haz clic en para crear un certificado de usuario, lo que hará que algunos aparecen más opciones. Introduzca el nombre de la conexión VPN o alguna otra información pertinente en
el campo Descripción, seleccione la misma entidad emisora de certificados como se utiliza para crear el servidor OpenVPN
ejemplo, a continuación, elija una clave de longitud, y entrar en un curso de la vida (estos dos pueden dejarse en sus valores por defecto).
Para terminar, haga clic en Guardar.
Para ver o cambiar el usuario, haga clic junto a la fila que contiene el usuario que desea ver / editar. Cerca
el fondo se puede ver hay twoicons, que ofrecen una descripción cuando se cernía el ratón
por encima de ellos. El primer icono se descargará la clave privada para este certificado, y el segundo icono descargará el certificado real. Ambos son necesarios para el software de cliente si va a crear un
configuración del cliente de forma manual. Usted puede saltar esta parte si usted va a utilizar el OpenVPN Client Exportación
El paquete, que se describe en la sección llamada "Paquete exportación OpenVPN Client". El paquete de la exportación del cliente
es una manera mucho más fácil de descargar configuraciones de cliente y los archivos de instalación.

LDAP o RADIUS Usuarios

Adición de usuarios de LDAP y RADIUS dependerá totalmente de su aplicación y gestión del servidor herramientas, que están más allá del alcance de este libro. Póngase en contacto con su proveedor de administrador del servidor o el software
para obtener ayuda. No se pueden crear certificados para los usuarios de LDAP o RADIUS desde la década de los cortafuegos
interfaz web de una manera que refleja una relación usuario-certificado. Sin embargo, puede crear el certificados por su cuenta utilizando el administrador de certificados.

Instalación del cliente OpenVPN

Con la completa configuración del servidor, OpenVPN ahora necesita ser instalado en el sistema cliente. La misma instalación de OpenVPN puede funcionar como un cliente o un servidor, por lo que sólo hay una instalación

de rutina. Funciona como se indica en la configuración proporcionada, que se tratarán en la próxima sección. Esta sección proporciona una visión general de la instalación en varios sistemas operativos comunes.

OpenVPN Client Package Exportación

Con mucho, la forma más fácil de configurar un cliente OpenVPN en Windows, Mac 4.x, o Android es utilizar el cliente OpenVPN Exportar paquete de su firewall. Para instalar el cliente, vaya a Sistema □

Paquetes, localizar OpenVPN Client Exportar en la lista y haga clic en el botón para instalar. Una vez instalado, se encuentra bajo VPN □ OpenVPN, en la pestaña Export Client.

Para utilizar el paquete, primera selección de la instancia del servidor OpenVPN desde el menú Servidor de Acceso Remoto
la lista desplegable. A continuación, en la opción Host Name Resolución, elija cómo desea que la entrada "a distancia" formateado
para el cliente. Por lo general, la dirección IP de interfaz es mejor para instalaciones con una IP estática en la WAN, Nombre de host de la instalación podrá ser utilizado si se desea, pero es especialmente útil si el servidor tiene una dirección IP dinámica
y utiliza DNS dinámico, o puede optar por Otro y escriba manualmente el nombre de host o la dirección IP
Si el nombre común del certificado del servidor contiene un espacio, y usted tiene un cliente que exige que tales un CN ser citado en el archivo de configuración del cliente, comprobar Cita servidor CN.

En Opciones de exportación de certificados, puede utilizar la casilla de verificación Usar Microsoft Certificate Almacenamiento
en lugar de los archivos locales si así lo desea, y si revisas Utilice una contraseña para proteger el contenido del archivo y pkcs12
introduce una contraseña, los certificados y las claves suministradas al cliente estarán protegidos con una contraseña. Si su servidor OpenVPN está configurado para la autenticación de usuarios, esto le dará a sus usuarios dos contraseñas diferentes
Si usted sabe que el cliente se encuentra detrás de un proxy HTTP, puede comprobar Usar proxy HTTP para solicita al cargar el cliente. Esto para descifrar las claves y certificados, y otro sobre la conexión.
comunicarse con el servidor, y luego suministrar una dirección IP, el puerto y la autenticación HTTP Proxy escriba si es necesario. Estos ajustes se configura previamente en el cliente.

Si necesita pasar algún parámetro de configuración adicionales para el cliente, puede hacerlo en el adicional cuadro de opciones de configuración. Esto es más o menos equivalente a la caja de opciones avanzadas en la OpenVPN pantallas de configuración de la instancia, pero desde la perspectiva del cliente.

Bajo Client Instalar paquetes que usted verá una lista de los usuarios del sistema que se han asociado certificados creados. Si no aparecen los usuarios, debe crearlos en el sistema como se describe en el sección llamada "Usuarios locales". Al lado de cada usuario, hay varias opciones para exportar la configuración del cliente.
Si va a ver a un cliente aquí, pero no lo hace, es posible que el certificado de cliente no se ha generado en contra de la misma CA que el servidor OpenVPN.

Configuración

Esta elección descargar sólo el fichero de configuración, no hay certificados o claves. Esto sería principalmente usado para ver el archivo de configuración en sí sin necesidad de descargar la otra información.

Configuración en línea

Esta elección se descargará un archivo de configuración con los certificados y claves en línea. Este formato es ideal para el uso en los clientes de Android, o para copiar manualmente una configuración a un sistema que ya ha instalado un cliente. Esta opción debería funcionar para cualquier tipo de cliente, siempre y cuando sea la versión 2.1 o superior.

Archivo de configuración

Descarga un archivo ZIP que contiene el archivo de configuración, clave TLS del servidor si está definido, y una PKCS # 12 que contiene el certificado de la CA, clave de cliente, y el certificado de cliente. Esta opción es buena para su uso con clientes Linux o Tunnelblick.

SIP archivos del teléfono

Si el servidor OpenVPN está configurado como SSL / TLS sólo - sin autenticación - más opciones se aparecerá para exportar configuraciones de cliente para varios modelos de teléfonos SIP que soportan OpenVPN. Ejemplos notables son los teléfonos Yealink T28 y T38G y SNOM. Instalación del cliente en el teléfono varía según el modelo, consulte la documentación del fabricante para obtener más información.

Nota

Asegúrese de que el teléfono tiene una configuración de reloj adecuada y / o servidor NTP, de lo contrario los certificados se
dejar de validar y de la VPN no conectará.

Windows Installer

Esta opción sencilla descargará un archivo EXE que contiene el instalador de OpenVPN con incrustado archivos de configuración. El instalador se ejecuta igual que el instalador del cliente de Windows normal OpenVPN, pero se
También instalar todos los ajustes necesarios. Por favor, consulte la sección "Instalación de Windows" para obtener algunas notas sobre cómo instalar y ejecutar el cliente de Windows. Actualmente, hay dos opciones disponibles, 2.2 y 2.3 Beta. La versión Beta funciona mejor en Windows Vista / 7, y en algunos casos puede eliminar la necesidad de ejecutar el cliente como Administrador.

Nota

Asegúrese de hacer clic al lado / Caja de todo el camino a través del proceso de instalación. No haga clic en Cancelar o
X cabo la instalación en cualquier paso, o usted puede ser dejado con el cliente instalado, pero sin necesidad de configuración
importados en el interior.
En Windows Vista y Windows 7 con OpenVPN versión 2.2 (o inferior) y UAC (User Control de cuentas) habilitado, debe hacer clic derecho en el icono de OpenVPN GUI y haga clic en Ejecutar como
Administrador para que funcione. Se puede conectar sin derechos administrativos, pero no se puede añadir la ruta necesaria para dirigir el tráfico a través de la conexión OpenVPN, dejándolo inutilizable. Usted puede también ajustar las propiedades del acceso directo para iniciar siempre el programa como administrador. Este opción se encuentra en la ficha Compatibilidad de las propiedades del acceso directo. El cliente 2.3 mejora en este comportamiento, pero en algunos casos todavía pueden requerir acceso de administrador.

Viscosidad Bundle

Esto funciona igual que el archivo de configuración anterior, pero es que el cliente Viscosidad OpenVPN utiliza en OSX. Si ya ha instalado el cliente de viscosidad, puede descargar este paquete, y haga clic en él para importarlo en el cliente.

Instalación del cliente

Si decide realizar una instalación manual del cliente, en lugar de utilizar el OpenVPN Client Exportación El paquete se ha mencionado anteriormente, hay más pasos implicados en conseguir el software y la configuración en la PC clientes.

Instalación de Windows

El proyecto OpenVPN ofrece un instalador para Windows 2000 hasta Windows 7, descargable desde http://openvpn.net/index.php/open-source/downloads.html. En el momento de escribir estas líneas, el mejor versión para la mayoría de los usuarios de Windows es de 2.3. La serie 2.3 está todavía en beta, pero varios otros clientes como
Viscosidad están enviando sobre la base de 2,3 debido a su mayor soporte para IPv6. En nuestras pruebas se ha realizado así. La actual versión estable 2.2 es una buena alternativa para aquellos que no necesitan las características adicionales o no desea ejecutar un cliente Beta. La instalación es muy sencillo, simplemente aceptar todos los valores predeterminados.
La instalación creará una nueva conexión de área local en el sistema para la `tonel` interfaz. Este interfaz se conecta cuando el VPN está conectado, y de otra manera muestran como desconectado. No

la configuración de esta interfaz es necesario, ya que su configuración se sacó de la OpenVPN servidor.

> **Nota**
>
> En Windows Vista y Windows 7 con OpenVPN versión 2.2 (o inferior) y UAC (User Control de cuentas) habilitado, debe hacer clic derecho en el icono de OpenVPN GUI y haga clic en Ejecutar como Administrador para que funcione. Se puede conectar sin derechos administrativos, pero no se puede añadir la ruta necesaria para dirigir el tráfico a través de la conexión OpenVPN, dejándolo inutilizable. Usted puede también ajustar las propiedades del acceso directo para iniciar siempre el programa como administrador. Este opción se encuentra en la ficha Compatibilidad de las propiedades del acceso directo. El cliente 2.3 mejora en este comportamiento, pero en algunos casos todavía pueden requerir acceso de administrador.

Mac OS X Los clientes y de instalación

Hay tres opciones de cliente para Mac OS X. Uno es el simple OpenVPN cliente de línea de comandos. Más los usuarios prefieren un cliente gráfico, y hay dos opciones disponibles para OS X. Tunnelblick es un país libre opción disponible para su descarga en http://www.tunnelblick.net. Lo he utilizado en el pasado con éxito. Otra opción es que el cliente GUI Viscosidad comercial disponible en http://www.viscosityvpn.com. En el momento de escribir estas líneas, que cuesta $ 9 USD para un solo asiento. Si utiliza OpenVPN con frecuencia, Viscosidad es un cliente mucho más agradable y bien vale la pena el costo.

Tanto Tunnelblick y viscosidad se instalan fácilmente, sin opciones de configuración durante la instalación.

Instalación de FreeBSD

Si usted tiene una instalación de FreeBSD acción, usted puede encontrar OpenVPN en los puertos. Para instalarlo, basta con ejecutar:

```
#cd / usr / ports / security / openvpn && make install clean
```

Instalación de Linux

Instalación de Linux variará dependiendo de la distribución y el método de gestión de software preferido instalaciones. OpenVPN está incluido en los repositorios de paquetes de la mayoría de las principales distribuciones de Linux.
Con todas las diversas posibilidades entre un sinnúmero de distribuciones, y la información adecuada ya disponible en otras fuentes en línea, este libro no cubre cualquier información específica. Basta con buscar en Internet la distribución de la elección y "la instalación de OpenVPN " para encontrar información.

Android 4.x

A partir de Android 4.0 (Ice Cream Sandwich, ICS), hay una API VPN que permite Android para ejecutar un Cliente OpenVPN sin privilegios de root. Para los dispositivos con ICS, Android 4.1 (Jelly Bean), o más reciente, hay una aplicación gratuita OpenVPN en la tienda de Google Play que funciona de manera excelente en todas nuestras pruebas. Lo se llama OpenVPN para Android [https://play.google.com/store/apps/details?id=de.blinkt.openvpn] por Arne Schwabe. Hay otros clientes OpenVPN por ahí, pero la mayoría requieren las raíces de su Android dispositivo, lo que le permitirá trabajar OpenVPN en versiones anteriores de Android, pero está lejos fuera del alcance de este libro.

Usted puede utilizar el paquete de exportación del cliente OpenVPN en pfSense para exportar una configuración en línea, y a continuación, transferir el archivo resultante `. Ovpn` presentar al dispositivo de destino. Puede copiar directamente, enviarlo por correo electrónico a ti mismo, etcétera.
Abre la aplicación OpenVPN, y haga clic en Todos sus VPNs preciosos. Luego haga clic en Importar (icono de la carpeta de archivos en la parte superior derecha), busca la `. Ovpn` el archivo que guardó anteriormente y haga clic en él. Haga clic en Seleccionar y, a continuación, haga clic en el icono Guardar.
Ahora que ya se ha guardado, tiene que decirle que su nombre de usuario si está utilizando un tipo de autenticación del usuario. En la lista de VPN, haga clic en el icono para editar el VPN (se parece a tres deslizadores). Haga clic en Editar en la barra superior (lápiz icono).
Haga clic en Basic, y rellenar el nombre de usuario. Haga clic repetidamente hasta que regrese a la lista de VPN.

Ahora debería ser capaz de conectarse a la VPN.

Android 2.1 a 3.2

Para los usuarios de Android 2.1 a 3.2, hay una que no sea root cliente OpenVPN llamada HAZAÑA VPN [https://play.google.com / store / apps / detalles? id = com.featvpn.app.lite]. Algunos usuarios han reportado éxito con usarlo en lugares donde no es posible ejecutar Android 4.x o raíz del dispositivo.

iOS

iOS también es capaz de ejecutar OpenVPN, pero primero debe jailbreak a tu dispositivo iOS. Al igual que con el enraizamiento
Android se ha mencionado anteriormente, es decir mucho más allá del alcance de este libro. Si usted decide ir por ese camino, nos
tienen informes de los usuarios que el cliente GuizmoVPN [http://www.guizmovpn.com] funciona bien.

Configuración del cliente

Después de instalar OpenVPN, tiene que copiar los certificados para el cliente y crear el cliente archivo de configuración.

Certificados de copia

Se necesitan tres archivos de su servidor de seguridad para cada cliente: el certificado de la CA, el certificado de cliente, y la clave de cliente. El certificado de CA se puede exportar y salvó de Sistema Cert Manager en el Pestaña CAs, salva esto como `ca.crt`. Certificado y la clave del cliente se pueden descargar como se describe en el sección llamada "Usuarios locales", guarde éstos como username.crt y username.key. Ahora copiar estos archivos en el OpenVPN `config` directorio en el cliente. Si está utilizando la autenticación TLS en esta Servidor OpenVPN, copie y pegue la clave de TLS desde la pantalla de configuración del servidor en un nuevo texto archivo llamado `tls.key` e incluirlo en el `config` carpeta también.

Crear configuración

Una vez copiados los certificados en el cliente, el archivo de configuración del cliente OpenVPN debe ser creado. Esto se puede hacer con cualquier editor de archivos de texto sin formato, como el Bloc de notas en Windows. A continuación se muestra
las opciones de uso más frecuente.

```
cliente
dev tun
udp proto
remoto openvpn.example.com 1194
ping-10
resolv-reintentar infinita
nobind
persistir-key
tun-persistir
ca.crt ca
cert username.crt
clave username.key
verbo 3
comp-lzo
tls.key tls-auth 1
-pass auth-user
```

La remoto línea especifica el host y el puerto del servidor OpenVPN remoto. Una dirección IP o nombre de dominio completo
se puede especificar aquí. La proto línea especifica el protocolo utilizado por la conexión OpenVPN.
Cambie esta línea proto tcp si elige TCP en vez de UDP para el servidor OpenVPN. La
ca, cert, y clave líneas deben ser modificados en consecuencia para cada cliente. Si usted no está utilizando TLS autenticación, puede omitir la línea tls-auth. Si usted no está utilizando una configuración de acceso remoto que incluye contraseñas, pueden omitir la línea-user-pass auth también.

La distribución de la configuración y las claves a los clientes

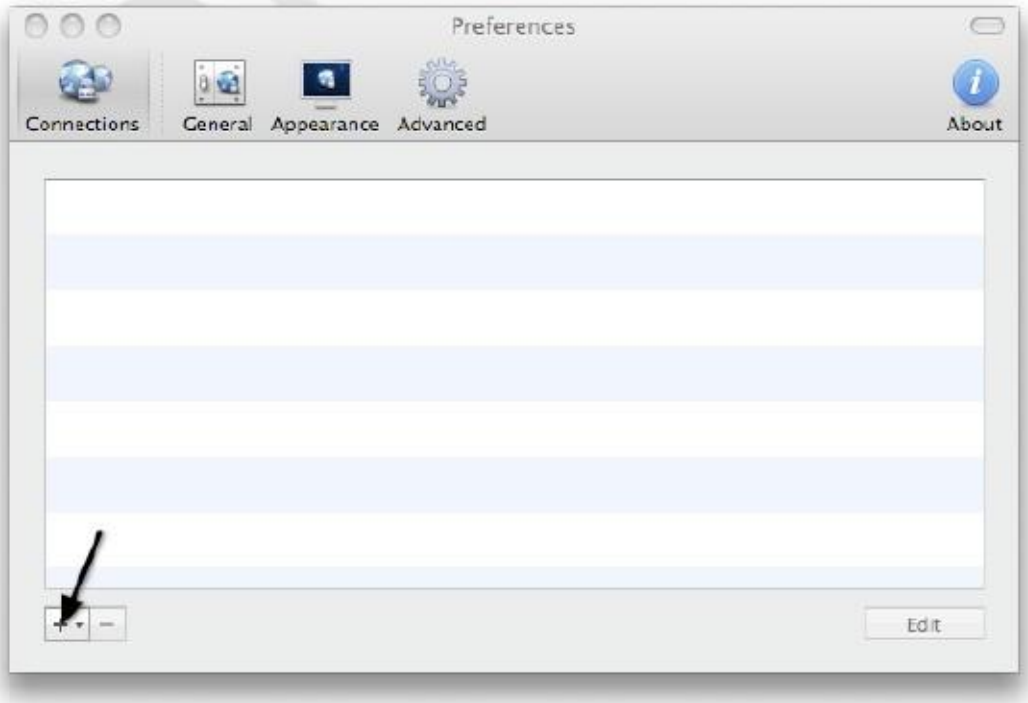
La forma más fácil de distribuir las claves y la configuración de OpenVPN para clientes es a través del cliente de OpenVPN
Paquete de exportación. Si usted no puede utilizar ese paquete, puede colocar los archivos necesarios en un archivo ZIP, o ZIP autoextraíble extraer automáticamente a `C: \ Archivos de programa \ OpenVPN \ config`. Este debe ser transmitida de forma segura para el usuario final, y nunca debe ser pasado a través de redes no confiables sin cifrar.

Configuración de Viscosidad

Cuando se utiliza el cliente de viscosidad, no es necesario crear manualmente la configuración del cliente OpenVPN presentar como se describe en la sección anterior. Viscosidad proporciona una herramienta de configuración GUI que se utiliza para
generar la configuración del cliente OpenVPN subyacente se muestra en la sección anterior. En primer lugar, copie el Certificado de la CA, el certificado de cliente y clave de cliente a una carpeta de su elección en el MAC. Si está utilizando
Autenticación TLS, copiar esa clave también. Estos archivos se importarán a la viscosidad, y después
que se pueden eliminar. Asegúrese de que esta carpeta se mantiene segura, o tiene los archivos borrados una vez finalizada la configuración de
Viscosidad. A continuación, inicie Viscosidad para comenzar la configuración.
Haga clic en el icono de candado añadido a la barra de menú en la parte superior de la pantalla y haga clic en Preferencias para comenzar la
configuración como se muestra en la Figura 19.2, "Preferencias Viscosidad".

Figura 19.2. Preferencias Viscosidad

Figura 19.3. Viscosidad Agregar conexión



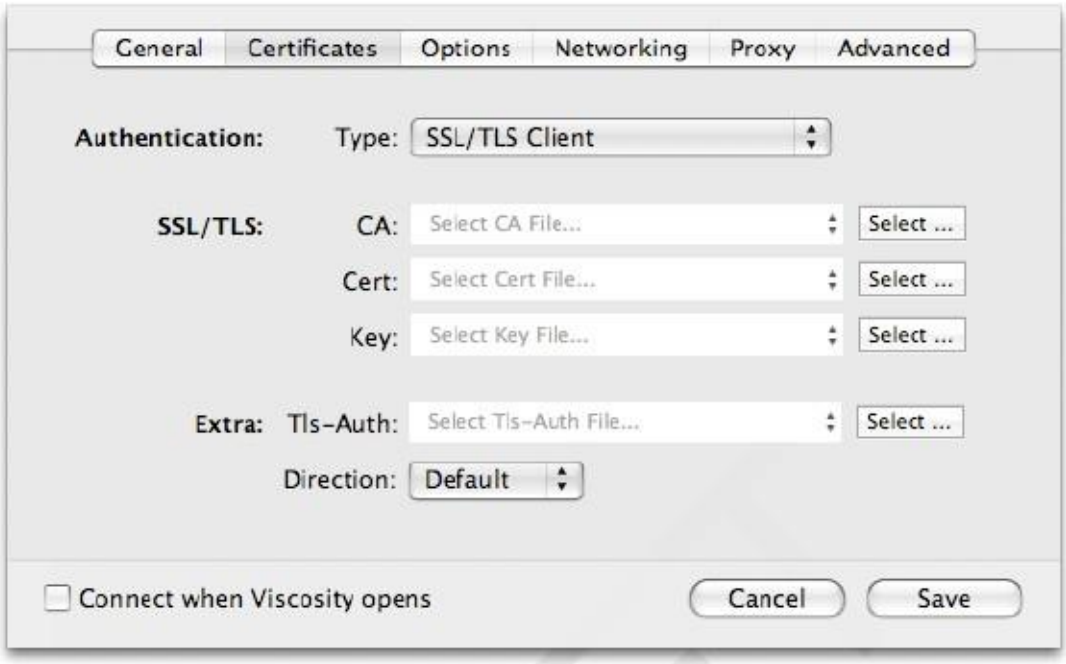
Haga clic en el signo más en la parte inferior derecha de la pantalla Preferencias y haga clic en Nueva conexión como se muestra en
Figura 19.3, "Viscosidad Agregar conexión".

En la primera pantalla de configuración (Figura 19.4, "Configuración de Viscosidad: General"), introduzca un nombre para
la conexión, la dirección IP o nombre de host del servidor OpenVPN, el puerto que se utiliza, y la
protocolo. Marca Habilitar el soporte de DNS si ha especificado servidores DNS en la configuración del servidor. Clic
la ficha Certificados cuando haya terminado.

Figura 19.4. Configuración Viscosidad: general

En la ficha Certificados (Figura 19.5, "Configuración de Viscosidad: Certificados"), el CA y el usuario
certificados y clave de usuario se deben especificar. Los archivos se pueden descargar en cualquier lugar de la
Sistema de archivos de Mac. Después de descargarlos, haga clic en Seleccionar junto a cada una de las tres casillas para elegir el
archivo adecuado para cada uno. El cuadro Tls-Auth se deja en blanco a menos que utilice la autenticación TLS en
cuyo caso deberá seleccionar el archivo donde guardó la llave TLS. Haga clic en la ficha Opciones cuando termine.

Figura 19.5. Configuración Viscosidad: Certificados



En la ficha Opciones (Figura 19.6, "Configuración de Viscosidad: Opciones"), marque la casilla Usar compresión LZO si lo ha activado en el lado del servidor. Si ha OpenVPN configurado para la autenticación de usuarios, Cheque Usar nombre de usuario / contraseña de autenticación. Las opciones restantes pueden dejarse en sus valores por defecto. Haga clic en el
Ficha Redes para continuar.

Figura 19.6. Configuración Viscosidad: Opciones

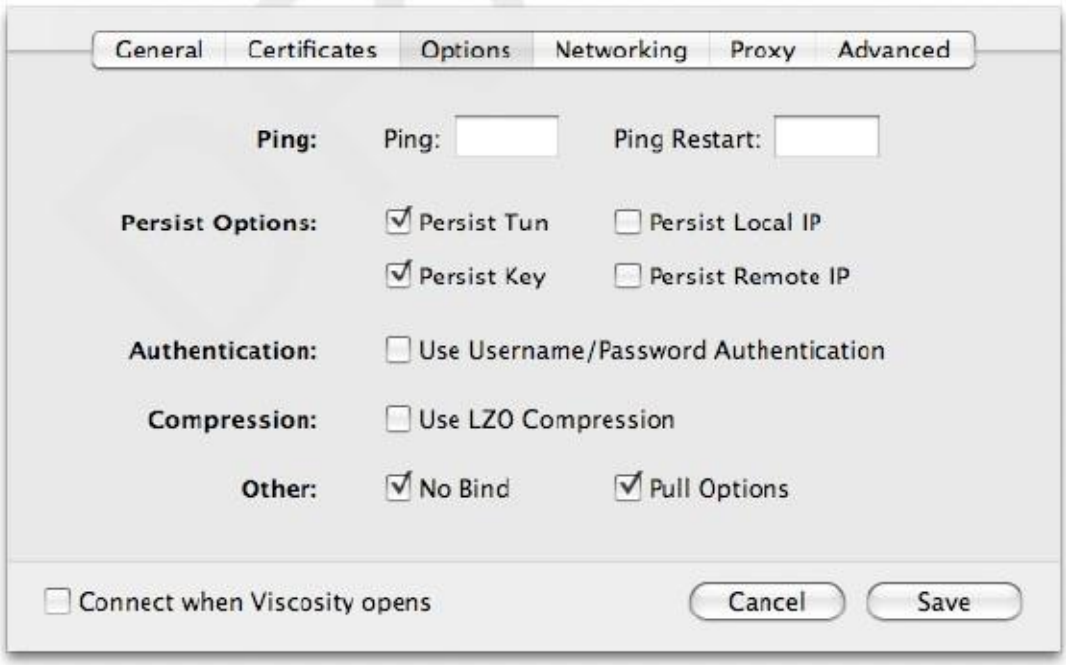
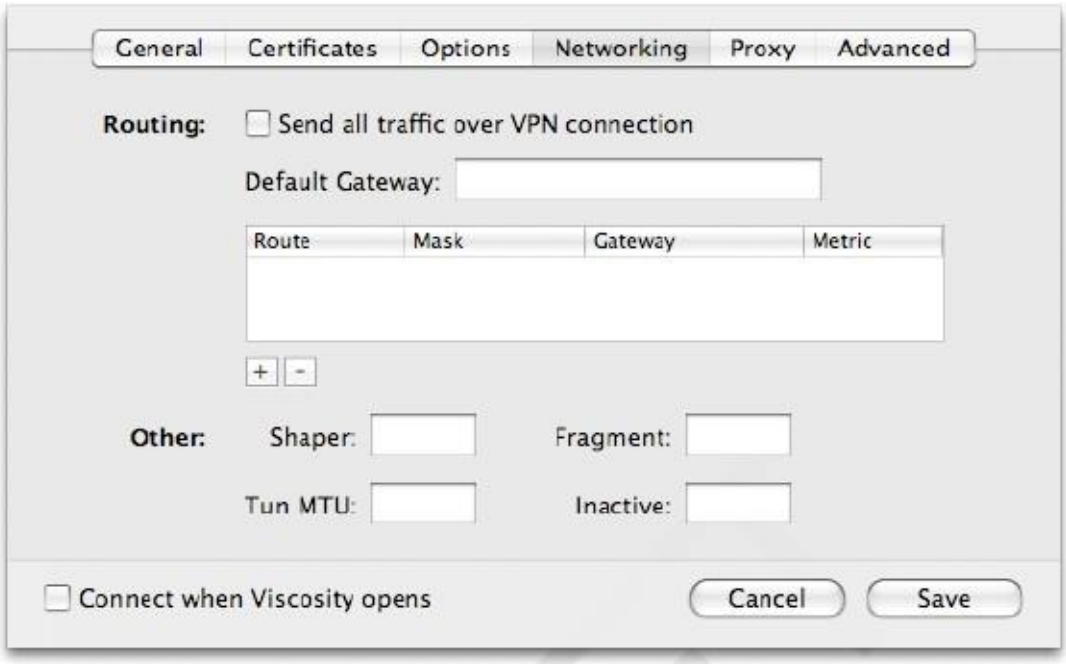


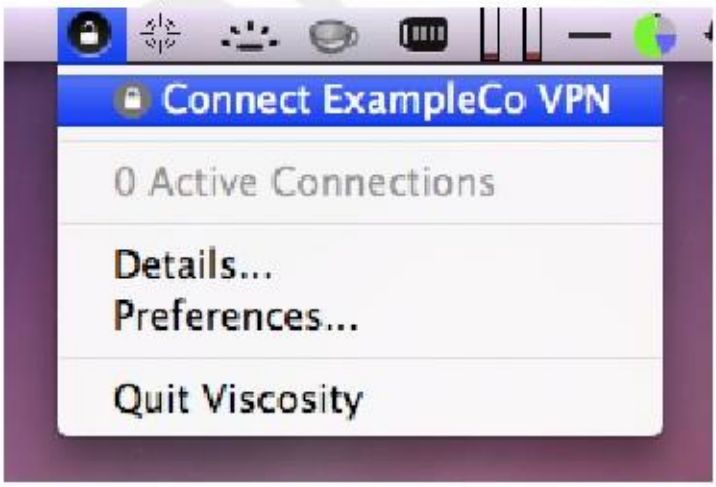
Figura 19.7. Configuración Viscosidad: Networking



En la ficha Redes (Figura 19.7, "Configuración de Viscosidad: Networking"), la opción principal de interés es la opción Enviar todo el tráfico casilla conexión VPN a través. Si usted desea enviar todo el tráfico a través de la VPN, marque esta casilla. Las pestañas de configuración restantes pueden descartarse en casi todas las configuraciones. Cuando haya terminado, haga clic en Guardar para finalizar la adición de la nueva configuración de OpenVPN.

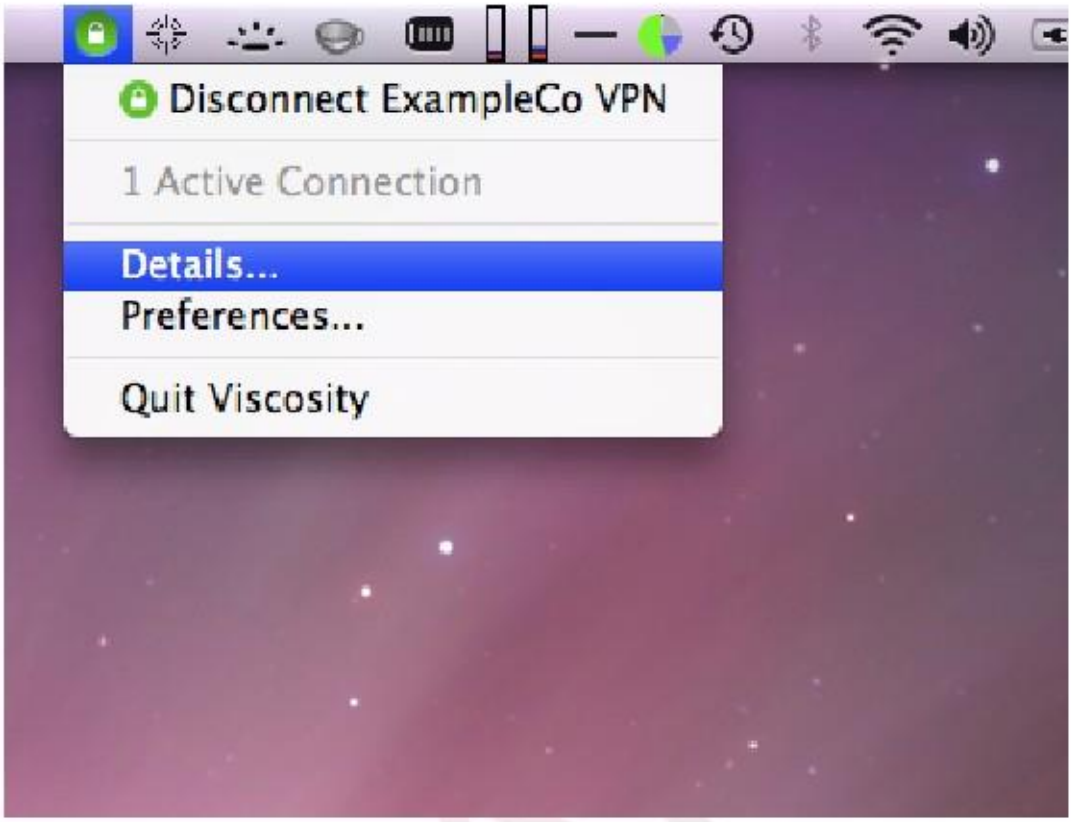
Ahora vas a tener la configuración de OpenVPN acaba de agregar se muestra en la pantalla Preferencias. Cerca En la pantalla Preferencias, haga clic en el candado en la barra de menú, y el nombre de la conexión VPN para conectar, como se muestra en la Figura 19.8, "Viscosidad conectar".

Figura 19.8. Viscosidad conectar



Después de unos segundos, el bloqueo en la barra de menú cambiará a verde para mostrar que ha conectado correctamente. Por al hacer clic en él, y haciendo clic en Detalles como se muestra en la Figura 19.9, "Menú de Viscosidad", se puede ver información en la conexión.

Figura 19.9. Menú Viscosidad



En la primera pantalla (Figura 19.10, "detalles de viscosidad"), verá el estado de la conexión, tiempo de conexión, 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, que muestra el rendimiento en y fuera de la interfaz de OpenVPN.

Figura 19.10. Detalles Viscosidad

Al hacer clic en el botón de flechas arriba / abajo en el medio de la pantalla de detalles, se puede ver más Estadísticas de la red de tráfico. Esto muestra el tráfico enviado dentro del túnel (TUN / TAP entrada y salida), como así como el protocolo TCP o UDP del tráfico enviado incluida la tara del túnel y cifrado. Para conexiones que utilizan paquetes principalmente pequeños, la sobrecarga es considerable con todas las soluciones de VPN. La Estadísticas muestran en la Figura 19.11, "detalles Viscosidad: Estadísticas de tráfico" son de sólo unos pings que atraviesan la conexión. El tráfico enviado en la educación de la conexión también se incluye aquí, por lo que el inicial sobrecarga es más alto que lo que será después de haber sido conectada durante algún tiempo. Además, el típico VPN tráfico tendrá tamaños de paquete más grande que 64 pings bytes, por lo que la sobrecarga total y diferencia entre estos dos números considerablemente menos.

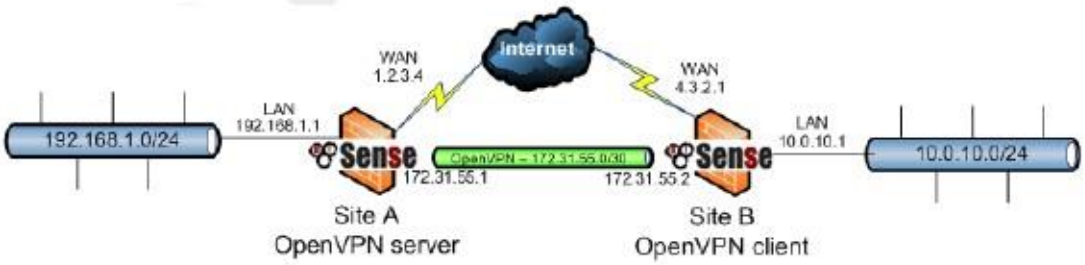
Figura 19.11. Detalles Viscosidad: Estadísticas de Tráfico

Al hacer clic en el tercer icono en el medio de la pantalla de detalles muestra el archivo de registro de OpenVPN (Figura 19.12, "Detalles Viscosidad: Logs"). Si usted tiene algún problema de conexión, revise los registros de aquí a ayudar a determinar el problema. Ver también la sección titulada "Solución de problemas de OpenVPN".

Figura 19.12. Detalles Viscosidad: Registros

Sitio de Ejemplo de configuración del sitio (Compartido Clave)

Figura 19.13. OpenVPN ejemplo el sitio de red del sitio



En esta sección se describe el proceso de configuración de un sitio para conexión al sitio utilizando claves compartidas. ¿Cuándo
la configuración de un sitio a otro de conexión OpenVPN, un servidor de seguridad será el servidor y la otra voluntad
ser el cliente. Por lo general, su ubicación principal será el lado del servidor y las oficinas remotas actuará
como clientes, aunque lo contrario es funcionalmente equivalente. Además de las subredes en ambos extremos,
Al igual que con la configuración de acceso remoto de OpenVPN, habrá una subred dedicada en uso para el
OpenVPN interconexión entre redes. La configuración de ejemplo que se describe aquí se representa
En la Figura 19.13, "Ejemplo de sitio OpenVPN para red de sitios".

172.31.55.0/30 se utiliza como el grupo de direcciones. El túnel OpenVPN entre los dos servidores de seguridad obtiene una IP en cada extremo de esa subred, como se ilustra en el diagrama. Las siguientes secciones describen cómo configurar los lados de servidor y cliente de la conexión.

Configuración de Server Side

Busque VPN OpenVPN y clic en la pestaña Servidor. Los siguientes campos están configurados, con todo lo demás deja a los valores predeterminados.

• Modo de servidor - Seleccione Peer to Peer (Shared Key).

• Descripción - Escriba algo aquí para describir la conexión.

• Clave compartida - Comprobar automáticamente generar una clave compartida, o puede pegar en una compartida preexistente
clave para esta conexión aquí.
• Red Tunnel - Intro 172.31.55.0/30 aquí.

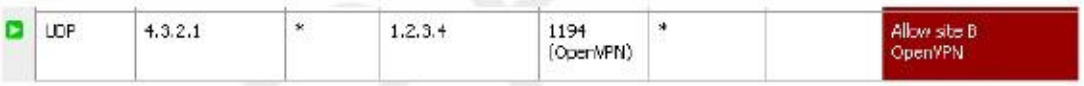
• Red remota - Ingrese 10.0.10.0/24 aquí.

Eso es todo lo que se debe configurar para el servidor OpenVPN para funcionar en este escenario. Clic Guardar.

Usted tendrá que copiar la clave compartida que se acaba de generar, para su uso en el sistema cliente. Desde lista de las instancias del servidor OpenVPN, clickNext a la que se acaba de crear. Encuentra la clave compartida caja y seleccionar todo el texto dentro, y luego copiar el texto en el portapapeles. Puede guardar a un archivo, o pegarlo en un editor de texto como el Bloc de notas de forma temporal.

A continuación, tendrá que añadir una regla de firewall en WAN que permite el acceso 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 dirección IP es dinámica.
El destino es el WAN Dirección, y puerto de destino es 1194 en este caso. Figura 19.14, "OpenVPN ejemplo un sitio a otro de reglas de firewall WAN" muestra la regla de firewall utilizado para este ejemplo.

Figura 19.14. OpenVPN ejemplo un sitio a otro de reglas de firewall WAN



Aplicar los cambios a partir de la regla de firewall se añade, y la configuración del servidor está terminado.

Configuración del lado del cliente

En el lado del cliente, vaya a VPN OpenVPN y clic en la ficha de cliente. Los siguientes campos se configuran, con todo lo demás a la izquierda en los valores predeterminados.

• Modo de servidor - Seleccione Peer to Peer (Shared Key).

• Server de host o la dirección - Introduzca la dirección IP pública o nombre de host del servidor OpenVPN aquí.

• Descripción - Escriba algo aquí para describir la conexión.

• Clave compartida - Desmarque generar automáticamente una clave compartida, a continuación, péguelo en la clave compartida para el
conexión aquí, con la tecla de copiado de la instancia de servidor creada anteriormente.
• Red remota - Ingrese 192.168.1.0/24 aquí.

Después de rellenar los campos, haga clic en Guardar. La configuración del cliente es completa. No hay reglas de firewall son requeridos en el cliente porque el cliente sólo inicia las conexiones salientes. El servidor nunca inicia conexiones con el cliente.

Nota

Con configuraciones de acceso remoto de PKI, con frecuencia no te defines rutas y otros opciones de configuración en la configuración del cliente, sino más bien empujar esas opciones desde el servidor

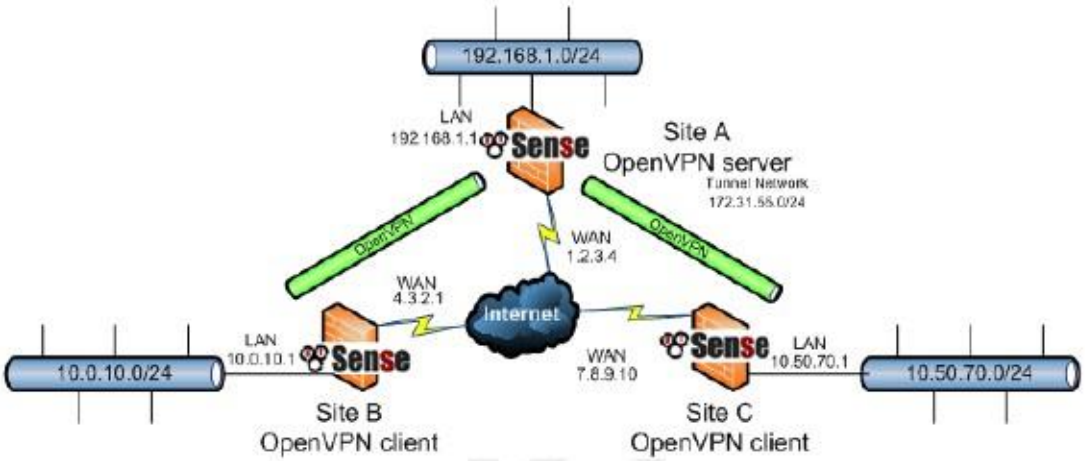
para el cliente. Con despliegues claves compartidas, debe definir las rutas y otros parámetros
en ambos extremos si es necesario (como se ha descrito anteriormente, y más adelante en la sección llamada "Custom
Opciones de configuración "), no se puede empujar desde el cliente al servidor cuando se utiliza claves compartidas.

Prueba de la conexión

La configuración se ha completado y la conexión debe ser activa inmediatamente después de guardar el
el lado del cliente. Intente hacer ping a través al extremo remoto para verificar la conectividad. Si surge algún problema, consulte
la sección "Solución de problemas de OpenVPN".

Sitio de Ejemplo de configuración del sitio (SSL / TLS)

Figura 19.15. OpenVPN ejemplo un sitio a otro de la red SSL / TLS



En esta sección se describe el proceso de configuración de un sitio para conexión al sitio con SSL / TLS. Este método puede ser más conveniente para la gestión de un gran número de sitios remotos que se conectan de vuelta a un centro sitio de una manera hub-and-spoke. Puede ser utilizado para un sitio a sitio entre dos nodos, pero dada la aumento de la complejidad de configuración, la mayoría de la gente prefiere utilizar la clave compartida en lugar de SSL / TLS para
ese escenario. Al configurar un sitio para localizar la conexión OpenVPN usando SSL / TLS, un servidor de seguridad ser el servidor y los otros serán clientes. Por lo general, su ubicación principal será el lado del servidor y el oficinas remotas actuarán como clientes, aunque si un lugar tiene una dirección IP estática y más ancho de banda que el oficina principal, que puede ser un lugar más deseable para el servidor. Además de las subredes en tanto extremos, como con la configuración de acceso remoto de OpenVPN, habrá una subred dedicada en uso para el OpenVPN interconexión entre redes. La configuración de ejemplo que se describe aquí se representa
En la Figura 19.15, "OpenVPN ejemplo un sitio a otro de la red SSL / TLS".

172.31.55.0/24 se utiliza como el grupo de direcciones. La forma de OpenVPN asigna direcciones IP es la misma que para
los clientes de acceso remoto, cada cliente que se conecta consigue un / 30 de subred para la interconexión con el servidor.
Las secciones siguientes describen cómo configurar los lados de servidor y cliente de la conexión. Cualquier subred se puede utilizar para este con tal de que no se superpone cualquier otra subred actualmente en uso en su red.
Para que el servidor para llegar a las redes de clientes detrás de cada conexión, se necesita tanto un ruta a la red para indicar al sistema operativo que OpenVPN sabe de esa red, y también un
iroute que dice OpenVPN a la que pertenece una conexión específica determinada subred. Más detalles sobre este seguirá en el ejemplo.

Configuración de SSL / TLS Server Side

Antes de que la VPN se puede configurar, es necesario crear una CA y la estructura de certificados para este VPN.
En primer lugar, crear un CA exclusivo de esta VPN. A partir de ese CA, crear un certificado de servidor y, a continuación, un usuario
certificado para cada sitio remoto. Para los sitios del cliente, utilice un CN que los identifica de forma única en algunos

Así, por ejemplo, su nombre de dominio completo o un sitio acortada o nombre de host. Para los detalles de la creación de una CA y certificados, consulte el Capítulo 8, Gestión de certificados. Para este ejemplo, la CA ser llamado S2SCA, la CN servidor será Servera, los clientes serán clienteB y clientC.

Busque VPN OpenVPN y clickon la pestaña servidor. Los siguientes campos están configurados, con todo lo demás deja a los valores predeterminados. Estas opciones se discuten en detalle en este capítulo. Uso valores adecuados para su red, o los valores predeterminados si no está seguro.

• Modo de servidor - Seleccione Peer to Peer (SSL / TLS).

• Protocolo - Seleccione UDP.

• Modo de dispositivo - Seleccione tun.

• Interface - Seleccione WAN.

• Puerto local - Intro 1194 a menos que tenga otro servidor OpenVPN activo, en cuyo caso se debe utilizar un puerto superior.

• Descripción - Escriba algo aquí para describir la conexión.

• Autenticación TLS - Marque esta casilla si desea también hacer la autenticación TLS y SSL. Esto es opcional, pero añade otra capa de seguridad. Al igual que en el modo de clave compartida, después de que el ahorro puede volver atrás y copiar esta clave, a continuación, pegarlo en los clientes después.

• Peer Certificate Authority - Seleccione la CA creado en el inicio de este proceso.

• Peer lista de certificados revocados - Si ha creado una CRL, seleccione aquí.

• Certificado de servidor - Seleccione el certificado de servidor creado en el inicio de este proceso.

• Red Tunnel - Intro 172.31.55.0/24 aquí.

• Red Local - Intro 192.1668.1.0/24 aquí.

• Opciones avanzadas - En esta casilla, tendrá que agregar una ruta para cada subred del cliente que será accesible a través de este VPN. También es probable que desee para empujar rutas para esas mismas redes para asegurar que los sitios remotos pueden llegar a unos de otros. Siguiendo el esquema de ejemplo anterior, esto se vería como:

```
ruta 10.0.10.0 255.255.255.0;
ruta 10.50.70.0 255.255.255.0;
empujar "ruta 10.0.10.0 255.255.255.0";
empujar "route 10.50.70.0 255.255.255.0";
```

Si hay más redes en el servidor que debe estar accesible a través de los clientes, tales como las redes accesible a través de rutas estáticas, otras VPNs, y así sucesivamente, es posible añadirlos rutas empujados adicionales.

Eso es todo lo que se debe configurar en esta pantalla para OpenVPN. Haga clic en Guardar.

Si decide utilizar la autenticación TLS, Usted tendrá que copiar la clave TLS que se acaba de generar para su uso en el sistema cliente. En la lista de instancias de servidor OpenVPN, ClickNext a la que se acaba de crear. Encontrar la caja TLS Autenticación y seleccionar todo el texto dentro, y luego copiar la texto en el portapapeles. Puede guardar a un archivo, o pegarlo en un editor de texto como el Bloc de notas temporalmente.

A continuación, tendrá que añadir una regla de firewall en WAN que permite el acceso 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 dirección IP es dinámica.
El destino es el WAN Dirección, y puerto de destino es 1194 en este caso. Figura 19.14, "OpenVPN ejemplo un sitio a otro de reglas de firewall WAN" muestra la regla de firewall utilizado para este ejemplo.

Se añade Aplicar cambios después de la regla de firewall.

La última pieza del rompecabezas es agregar valores específicos de cliente para cada sitio del cliente. Estos cambios son necesarios para
atar una subred del cliente al certificado de ese sitio para que pueda ser bien colocado. Bajo VPN OpenVPN,

haga clic en la ficha Específico del cliente omitida, y haga clic para agregar una nueva anulación. En esta pantalla, rellene los campos como se indica a continuación:

• Nombre Común - Introduzca el CN del primer sitio del cliente. En nuestro ejemplo, es decir clienteB.

• Avanzado - Introducir una iroute declaración de subred del primer sitio del cliente. En nuestro ejemplo, es decir de clienteB subred, 10.0.10.0, que se verá como:

```
iroute 10.0.10.0 255.255.255.0;
```

Añadir otra anulación para el segundo sitio, el ajuste de la CN y iroute declaraciones, según sea necesario.

A continuación, tendrá que exportar los certificados y las claves que necesita. Estos pueden ser obtenidos por ir a Sistema Cert Manager y haga clic en los vínculos para exportar los siguientes elementos:

• Certificado CA

• certificado de sitio de cliente (. Crt) para cada ubicación del cliente.

• Tecla de sitio de cliente (clave.) Para cada ubicación del
cliente.
Usted ¿no deberá exportar la clave CA, el certificado del servidor, o la clave del
servidor.
Esto completa la configuración del servidor, a continuación, configurar los
clientes.

Configuración de SSL / TLS Client Side

En primer lugar, en el cliente, tendrá que importar el certificado CA junto con el certificado y la clave de ese sitio.
Esto se puede hacer en Sistema Administrador de Cert. Para obtener información específica sobre la importación de la CA y certificados,
consulte el Capítulo 8, Gestión de certificados.

Después de que los certificados hayan sido importados, busque VPN OpenVPN y clic en la ficha de cliente.
Los siguientes campos están configurados, con todo lo demás a la izquierda en los valores predeterminados.

• Modo de servidor - Seleccione Peer to Peer (SSL / TLS).

• Protocolo - Seleccione UDP.

• Modo de dispositivo - Seleccione tun.

• Interface - Seleccione WAN.

• Server de host o la dirección - Introduzca la dirección IP pública o nombre de host del servidor OpenVPN aquí. En nuestro ejemplo se trata de 1.2.3.4.

• Puerto de servidor - Ingrese 1194 o cualquier puerto se ha configurado en el servidor.

• Descripción - Escriba algo aquí para describir la conexión.

• TLS Autenticación - Seleccione Habilitar la autenticación de paquetes TLS si usted eligió en el servidor para También hacer la autenticación TLS y SSL. Esto es opcional, pero añade otra capa de seguridad.
Desmarque automáticamente generar una clave de autenticación TLS compartida, a continuación, péguelo en la clave para TLS
la relación en este caso, utilizando la clave copiado de la instancia de servidor creada anteriormente.

• Peer Certificate Authority - Seleccione la CA importado, en el inicio de este proceso.

• Certificado de cliente - Seleccione el certificado de cliente importado, en el inicio de este proceso.

Después de rellenar los campos, haga clic en Guardar. La configuración del cliente es completa. No hay reglas de firewall son obligatorios en la WAN del cliente porque el cliente sólo inicia las conexiones salientes. El servidor
nunca inicia conexiones con el cliente.

Nota

Con configuraciones de acceso remoto de PKI, con frecuencia no te defines rutas y otros
opciones de configuración en la configuración del cliente, sino más bien empujar esas opciones desde el servidor
para el cliente. Si usted tiene más redes para llegar en el lado del servidor, deben ser empujados
a partir de ahí.

Prueba de la conexión

La configuración se ha completado y la conexión debe ser activa inmediatamente después de guardar el
el lado del cliente. Intente hacer ping a través al extremo remoto para verificar la conectividad. Si surge algún problema, consulte
la sección "Solución de problemas de OpenVPN".

Comprobación del estado de los clientes OpenVPN y Servidores

Alta en pfSense 2.0, la página de estado OpenVPN al Estado OpenVPN muestra el estado de cada
Servidor OpenVPN y el cliente.

Para los servidores OpenVPN en modo de servidor SSL / TLS, el estado le proporcionará una lista de remoto conectado
clientes, junto con sus nombres de usuario o nombres comunes de certificados, como se ve en la Figura 19.16, "OpenVPN
Estado para el servidor SSL / TLS con un cliente conectado ". También puede desconectar clientes de este
pantalla haciendo clic en el al final de la fila cliente.

Figura 19.16. OpenVPN Estado para el servidor SSL / TLS con un cliente conectado

Remote Access UDP:1192 Client connections

Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received
jimp	192.168.20.43:1194	192.168.138.6	Thu Oct 18 13:42:22 2012	7797	6830

Para los servidores OpenVPN en modo de clave compartida, el estado se indicará si se está ejecutando y esperando
en las conexiones, o si el cliente remoto se ha conectado.

Para los clientes OpenVPN, el estado indica si la conexión está pendiente o activo.

Figura 19.17. OpenVPN estado mostrando un servidor a la espera de una conexión y
un cliente que intenta volver a conectarse

Peer to Peer Server Instance Statistics

Name	Status	Connected Since	Virtual Addr	Remote Host	Bytes Sent	Bytes Received
Server A UDP:1194	waiting	Wed Oct 17 16:03:22 2012	10.16.254.5			

Client Instance Statistics

Name	Status	Connected Since	Virtual Addr	Remote Host	Bytes Sent	Bytes Received
Client B UDP	reconnecting; ping-restart	Wed Oct 17 16:04:32 2012				

Permitir el tráfico al servidor OpenVPN

Después de configurar un servidor OpenVPN, se requiere una regla de firewall para permitir el tráfico al servidor OpenVPN.
Vaya a Cortafuego Reglas y a la pestaña WAN, haga clic en. Para la configuración de ejemplo
aquí, el protocolo UDP se elegirá, con cualquier origen, destino WAN Dirección, y puerto de destino
1194. Esta regla se muestra en la Figura 19.18, "regla WAN del servidor OpenVPN".

Figura 19.18. Regla WAN del servidor OpenVPN

Si usted sabe qué fuente se dirige a sus clientes se conectan desde, puede especificar una fuente red o alias en lugar de dejar que el servidor abierto a toda la Internet. Esto es por lo general imposible donde ha clientes móviles. No hay mucho riesgo de dejar este abierto, sin embargo, como con autenticación de certificados basados tiene menor riesgo de compromiso que las soluciones basadas en contraseñas que son susceptibles a la fuerza bruta. Esto supone una falta de agujeros de seguridad en sí mismo OpenVPN, que hasta la fecha tiene un sólido historial de seguridad.

Permitir el tráfico a través de OpenVPN Túneles

Por defecto, todo el tráfico se bloquea la entrada de los túneles OpenVPN. La excepción a esto es cuando un servidor de seguridad se actualizó de pfSense 1.2.3 donde filtrado OpenVPN no era posible. Una norma a permite se añade todo el tráfico OpenVPN durante la actualización desde 1.2.3 2.x para preservar comportamiento anterior del servidor de seguridad después de la actualización. Para permitir el tráfico de los clientes OpenVPN para hacer
conexiones a los recursos del lado del servidor, debe agregar reglas de firewall en Cortafuegos Reglas, por Pestaña OpenVPN. Al igual que con otros aspectos del servidor de seguridad, estas reglas sólo igualará el tráfico que entra en el
sistema de la cliente lado, no el tráfico que sale desde el lado del servidor, por lo que las embarcaciones de sus reglas de manera apropiada.
Si usted necesita para llegar a los dispositivos en el lado del cliente, agregar reglas de la ficha OpenVPN en el firewall del cliente
así.

Clientes OpenVPN y acceso a Internet

Si simplemente quiere hacer NAT sus clientes OpenVPN a su IP WAN para que puedan acceder a Internet utilizando la conexión OpenVPN, las reglas deben permitir automáticamente esta. Si usted desea tener más fino grano control, necesita habilitar Advanced Outbound NAT y editar la regla NAT saliente para subred (s) Dirección piscina, que debería aparecer automáticamente después de cambiar forma automática a Manual. Vea la sección llamada "salida NAT" para más detalles sobre NAT Saliente.

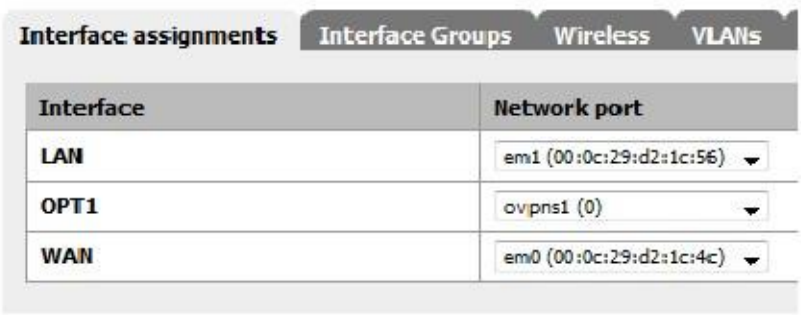
NAT con conexiones OpenVPN

Con el fin de hacer NAT complejo o filtrado túnel específico, debe asignar la interfaz de OpenVPN una interfaz OPT y configurarlo en consecuencia. En esta sección se describe cómo realizar NAT para Clientes OpenVPN.

Misiones y configuración de la Interfaz

Busque Interfaces Asignar y asignar la adecuada `ovpns` o `ovpnc` interfaz como OPT interfaz. El nombre del dispositivo OpenVPN dependerá de cómo se ha configurado. Instancias del servidor son `ovpnsx`, los clientes son `ovpncx`. Usted tendrá una interfaz por servidor OpenVPN y el cliente configurado en el sistema. Figura 19.19, espectáculos de "interfaz Asignar OpenVPN" `ovpns1` asignado como OPT1.

Figura 19.19. Asigne la interfaz OpenVPN



Ahora vaya a la página de interfaz para la interfaz, Interfaces previamente asignados OPT1 para la ejemplo que se muestra en la Figura 19.19, "interfaz Asignar OpenVPN". Comprobar primero la casilla Habilitar interfaz en la parte superior de la página, y escriba una descripción apropiada en el campo Descripción. Seleccionar ninguno en el cuadro Tipo. Esto no va a configurar cualquier información IP en la interfaz, que es necesaria, ya OpenVPN en sí debe configurar estos valores en la `ovpns1` 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 propósitos.

Filtrar con OpenVPN

Ahora que tiene la interfaz OpenVPN asignado, vaya a Firewall Reglas y haga clic en la pestaña para la interfaz que acaba de asignar. Aquí usted puede agregar reglas de firewall como cualquier otra interfaz que se aplicará al tráfico iniciado por los clientes OpenVPN. Para obtener más información sobre las reglas del cortafuegos, consulte
Capítulo 10, Firewall. Las normas sobre la pestaña OpenVPN se seguirán aplicando al tráfico en una OpenVPN asignado interfaz. Las reglas de interfaz se consideran en primer lugar, y luego el grupo de reglas para OpenVPN. Para garantizar que usted no permite que más tráfico de lo deseado, es posible que desee agregar una regla en la parte inferior de la asignada
regla de firewall de interfaz para bloquear todo el tráfico.

NAT con OpenVPN

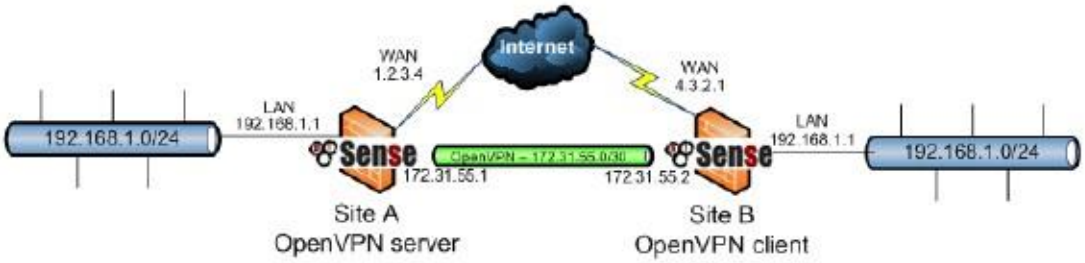
Con la interfaz de OpenVPN asignado, las reglas de NAT también se puede aplicar el mismo que con cualquier otro interfaz. Esto es útil cuando es necesario conectar dos subredes en conflicto. Si dispone de dos redes utilizando una LAN 192.168.1.0/24 subred que usted necesita para conectarse a través de un sitio para localizar VPN, no pueden
comunicarse a través de VPN sin NAT. Los hosts de una subred 192.168.1.0/24 nunca alcanzarán la otra final de la VPN para comunicarse con el control remoto subred 192.168.1.0/24, debido a que la red es siempre tratados como local. Sin embargo, con NAT, usted puede hacer la función de extremo remoto como si estuviera utilizando un
diferente subred IP.

Nota

Esto funciona bien para muchos protocolos, pero para algunos que son comúnmente deseable a través de VPN conexiones, principalmente para compartir archivos SMB / CIFS entre los hosts de Windows, no funcionarán en
combinación con NAT. Si utiliza un protocolo que no es capaz de funcionar con NAT, esto no es una solución viable.

Figura 19.20, "sitio a sitio con subredes en conflicto" muestra un ejemplo en el que ambos extremos están utilizando el misma subred. Después de asignar el `tonel` de interfaz a una interfaz de OPT en ambos lados, como se describe en la sección llamada "asignación de interfaz y configuración", NAT 01:01 se puede aplicar.

Figura 19.20. Un sitio a otro con subredes en conflicto



El tráfico de sitio será traducido a 172.16.1.0/24 y sitio B será traducido a 172.17.1.0/24. Una entrada de NAT 01:01 será agregado en cada extremo de traducir toda la gama / 24. Para llegar Del sitio del sitio B, se utilizarán 172.16.1.x direcciones IP. El último octeto de la IP 192.168.1.x será traducido al último octeto de la IP 172.16.1.x traducido, por lo que para llegar a 192.168.1.10 al sitio de la web B, usted usaría 172.16.1.10 lugar. Para llegar a 192.168.1.50 en el sitio B desde el sitio A, utilizaría 172.17.1.50 lugar. Figura 19.21, "Sitio de configuración A 01:01 NAT" y la Figura 19.22, "Sitio B 01:01 NAT configuración "muestra la configuración de NAT 01:01 para cada lado, donde el `tonel` se asigna interfaz como OPT2.

Figura 19.21. Configuración del sitio 01:01 NAT

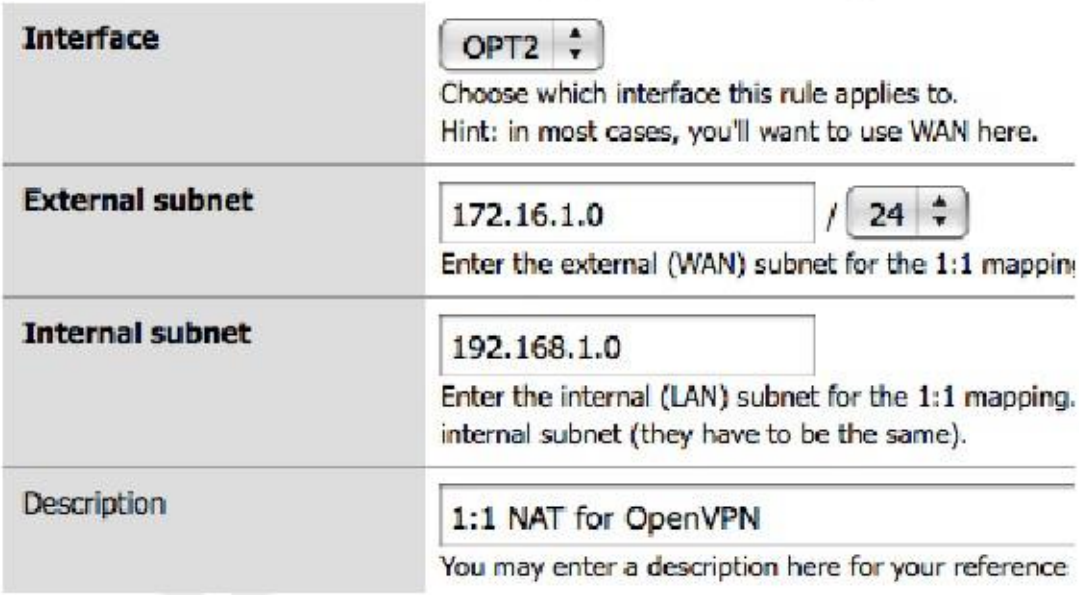
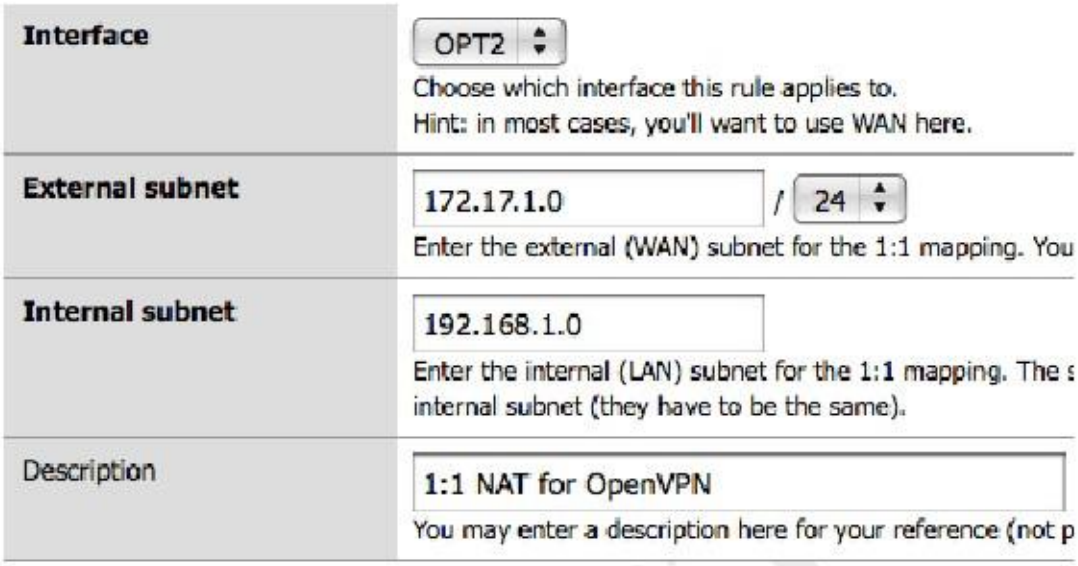


Figura 19.22. Sitio B 1:01 configuración de NAT



En la configuración de OpenVPN en ambos lados, la red remota se debe especificar como el traducido Subred IP, 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 configuración de la red a distancia de acuerdo en ambos lados, las redes serán capaces de comunicarse utilizando las subredes traducidas.

OpenVPN y Multi-WAN

OpenVPN es multi-WAN capaz, con algunas advertencias en algunas circunstancias. Esta sección cubre multi-WAN consideraciones con el servidor OpenVPN y configuraciones de cliente.

OpenVPN asignado a un grupo de puerta de enlace

Comenzando con pfSense 2.1, ahora se puede seleccionar un grupo de Gateway (la sección denominada "Grupos Gateway")
como la interfaz para una instancia de OpenVPN. Tal grupo gateway sólo debe tener una pasarela por nivel.
Al crear el grupo de la puerta de enlace, es posible seleccionar un VIP utilizar para ese nivel también. Cuando se selecciona un
Servidor VPN, interfaz o VIP del grupo gateway de nivel 1 se utilizarán para la unión primero. Si la puerta de enlace se cae, se moverá al nivel 2, y así sucesivamente. Si la puerta de enlace de nivel 1 vuelve a subir, la VPN se reanudará operativo en que la WAN. Cuando se utiliza para un servidor VPN, esto significa que el servidor sólo está activa en una WAN a la vez. Algunos de los otros métodos descritos a continuación pueden ser mejores para ciertas circunstancias, tales como la necesidad de las dos redes WAN utilizables simultáneamente con la VPN. Cuando se usa con los clientes OpenVPN,
la interfaz de salida se cambiará de acuerdo a los niveles del grupo de pasarela.

Servidores OpenVPN y multi-WAN

Servidores OpenVPN se pueden utilizar con cualquier conexión WAN, aunque los medios de hacerlo variará dependiendo de las características específicas de su configuración.

Servidor OpenVPN utilizando TCP

Mientras que TCP no es generalmente el protocolo preferido para OpenVPN, como se describe anteriormente en este capítulo,
utilizando TCP puede hacer multi-WAN OpenVPN más fácil de configurar cuando la VPN está utilizando una interfaz

ajuste de cualquier. Servidores OpenVPN utilizando TCP funcionarán correctamente en todas las WAN donde las reglas de firewall
permitir el tráfico al servidor OpenVPN. Se necesita una regla de firewall en cada interfaz WAN.

Servidor OpenVPN usando UDP

Servidores OpenVPN con UDP son también multi-WAN capaz, pero con algunas advertencias que no son aplicables con TCP, debido a las funciones de enrutamiento multi-WAN de la manera de pf. En algunos casos, cada WAN mosto tener su propio servidor OpenVPN. Puede utilizar los mismos certificados para todos los servidores. Sólo dos partes de la configuración de OpenVPN debe cambiar.

Método de varios servidores

Dirección piscina

Cada servidor debe tener un grupo de direcciones únicas que no se superponga con ningún otro conjunto de direcciones o subred interna.

Interfaz

Cada servidor OpenVPN debe especificar la interfaz de interfaz WAN utilizado por ese servidor.

Método forward Puerto

Una opción algo más fácil puede ser para enlazar el servidor OpenVPN a la interfaz LAN y, a continuación, utilizar un puerto
delante de cada WAN para dirigir el puerto OpenVPN a la IP LAN. Usando este método, pf de respuesta a funcionalidad se asegurará de que el tráfico de retorno fluye de vuelta a la fuente apropiada a través de la interfaz adecuada.
Este método requiere la intervención manual cuando se utiliza con el paquete de exportación del cliente, sin embargo. Usted
debe especificar la IP (s) de la WAN al exportar, como los ajustes por defecto exportadores dejarían de intentar para conectarse a un servidor a través de Internet, que no es enrutable.

Conmutación por error automática para clientes

Servidores remotos múltiples se pueden configurar en los clientes OpenVPN. Si el primer servidor no puede ser alcanzado,
se utilizará el segundo. Esto puede ser usado en combinación con un servidor multi-WAN OpenVPN despliegue para proporcionar conmutación por error automática para los clientes. Si los servidores OpenVPN se están ejecutando en IPs
1.2.3.4 y 4.3.2.1, ambos utilizando el puerto 1194, el remoto líneas en el archivo de configuración del cliente serán de la siguiente manera.

```
1.2.3.4 remoto 1194
4.3.2.1 remoto 1194
```

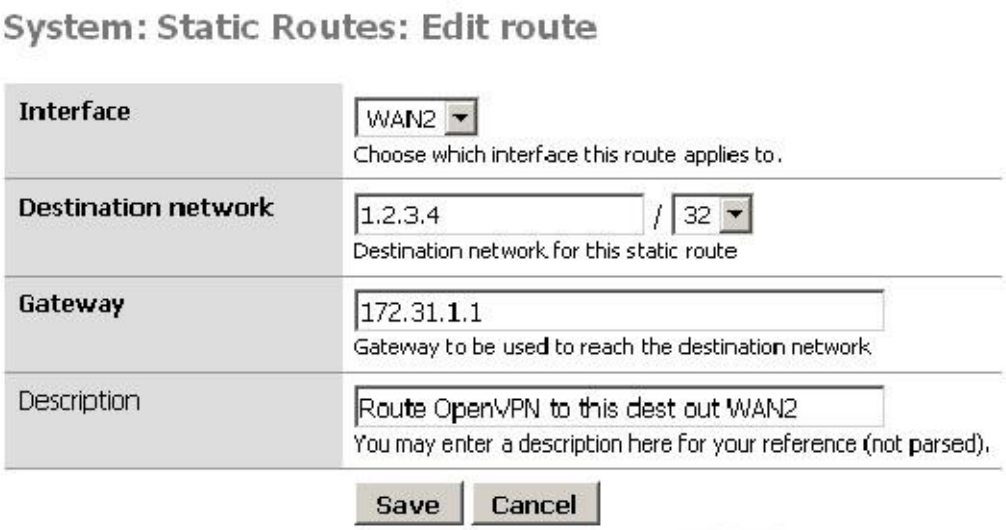
Para los clientes configurados en pfSense, la primera remoto está configurado por las opciones que se ofrecen en la GUI. El segundo remoto se especifica en el campo de opciones personalizadas.

Clientes OpenVPN y multi-WAN

Clientes OpenVPN configuradas en el servidor de seguridad respetarán la interfaz elegida al configurar el cliente, y una ruta estática se agrega automáticamente en segundo plano para que pueda funcionar si lo deseas. Si por alguna razón la interfaz se debe establecer en cualquier, el cliente siga la tabla de enrutamiento del sistema cuando hacer la conexión con el servidor OpenVPN. Este fue el comportamiento predeterminado en pfSense 1.2.3 y antes. Para utilizar una interfaz OPT WAN, seleccione la interfaz según se requiera. Si tiene que configurar el cliente a un Valor Interfaz de ninguno, entonces usted tendrá que introducir una ruta estática para dirigir el tráfico a la terminal remota
de la conexión de OpenVPN.

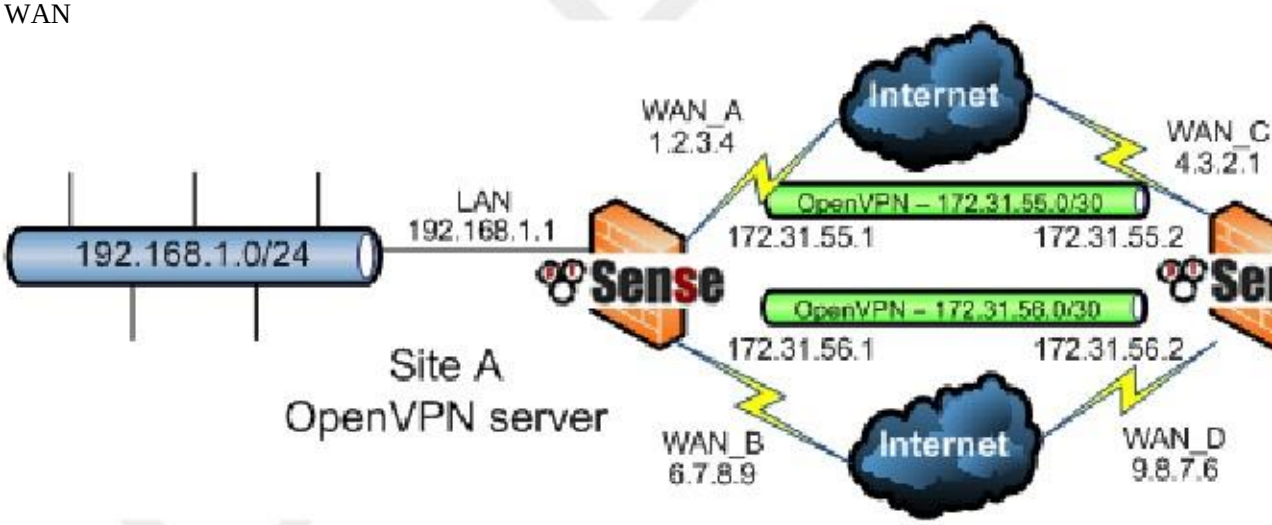
Figura 19.23, "Ejemplo de ruta estática para el cliente OpenVPN en OPT WAN" ilustra la ruta estática necesaria para utilizar la interfaz WAN2 acceder a un servidor OpenVPN se ejecuta en IP 1.2.3.4, donde la puerta de entrada de la interfaz WAN2 es 172.31.1.1. Esto sólo es necesario si el interfaz en el VPN es establece en ninguno. Si se ajusta a la interfaz de salida deseada real, se agregará automáticamente una ruta estática y esto no será necesario.

Figura 19.23. Ejemplo ruta estática para el cliente OpenVPN en OPT WAN



OpenVPN Site-to-Site con Multi-WAN y OSPF

Figura 19.24. Ejemplo de configuración de OpenVPN que implica OSPF a través de múltiples redes WAN



Sobre la base de los conceptos de antes en este capítulo, es posible configurar una configuración redundante VPN utilizando
un protocolo de enrutamiento dinámico, como OSPF, como se ve en la Figura 19.24, "Ejemplo de configuración de OpenVPN que implica
OSPF a través de múltiples redes WAN ".
En primer lugar, los casos de instalación en cada WAN para los sitios remotos. Estos deben ser compartidas clave de sitio a sitio
túneles, sin redes remotas rellenados, aborda sólo Túnel de red.

- En la configuración de servidor de dos servidores, cada uno en un puerto diferente. Utilice dos distintos, no se solapan redes de túneles (por ejemplo, 172.31.55.0/30 y 172.31.56.0/30)

- En la configuración del lado del cliente dos clientes, cada uno emparejado con uno de los servidores anteriores, que coincide con el IP
  direcciones y números de puerto involucrados.
- Asegúrese de que estos se establecen por su específica WAN, seleccione la interfaz en el menú desplegable, o una VIP CARP que está en una de las redes WAN siendo utilizados.

Asegúrese de que estas conexiones OpenVPN se vinculan entre cliente y servidor. Usted debe ser capaz de hacer ping la dirección del túnel en ambos lados. Si los túneles no establecen, consulte la sección "Solución de problemas

OpenVPN "para obtener sugerencias sobre solución de problemas de la conexión. Garantizar en las reglas del firewall OpenVPN
que permite que todo el tráfico, o al menos permitir que el tráfico OSPF de una fuente de las redes de túneles, a un destino de cualquiera. El destino en el tráfico será una dirección de multidifusión, que se puede utilizar para filtrar específicamente si es necesario, pero no hay mucho que ganar en el camino de la seguridad si la fuente es bloqueada por la normativa y el tráfico no puede dejar ese segmento.

Una vez que ambos casos están conectados, se puede pasar a la configuración de OSPF.

En primer lugar, en ambos cortafuegos debe instalar el paquete Quagga-OSPF del Sistema Los paquetes en la

Pestaña Paquetes disponibles. Una vez instalado, vaya a Servicios Quagga ospfd, aquí es donde el OSPF configuración está configurado.

En la ficha Interfaces, agregue cada interfaz de OpenVPN. Establecer el costo de 10 en el enlace de primaria y 20 en la secundaria, y así sucesivamente. Publique sus LAN y otras interfaces como interfaces internas pasivas.

Una vez que se han añadido las interfaces, vaya a la ficha Configuración global. Establezca una contraseña maestra. Lo en realidad no importa lo que se establece en, se utiliza internamente para acceder a la condición de demonio, pero es necesario
a establecer. Establezca el ID del router en un valor IP-dirección-como, con esto queremos decir un valor que se parece a un
Dirección IP, por ejemplo, 192.168.1.1. La ID del router es único en cada dispositivo, por lo que si se establece en dirección IP de LAN del router es una buena práctica. Por último, establezca el ID de área que es también una dirección IP-
como valor. El ID de área se programa es 0.0.0.0 o 0.0.0.1, pero usted puede usar cualquier valor
te gusta. El ID de área es la misma para todos los routers que participan en esta configuración de VPN. Pulse Guardar y, a la
Configuración de OSPF en ese router se ha completado. Una vez que se ha configurado OSPF en todos los routers, que deberían
con cada instancia
puede emparejar correctamente.
Después de OSPF se haya configurado en ambos extremos, en la ficha Estado debe mostrar una interconexión completa en cada wan, y usted debería ver las rutas obtenidas mediante OSPF lista. Una vez que esto sucede, usted puede intentar desenchufando / enchufando WANs y refrescar el estado (será un ping que va entre las redes internas)
para probarlo.

OpenVPN y CARP

OpenVPN es interoperable con CARP. Para proporcionar una solución OpenVPN alta disponibilidad con CARP, configurar los clientes para conectarse a un VIP CARP, y configurar el servidor OpenVPN para usar el CARP
IP con la opción de interfaz. En pfSense 1.2.x, la configuración de OpenVPN no se puede sincronizar con
el servidor de seguridad secundaria, por lo que usted debe introducir manualmente en ambos cortafuegos. En pfSense 2.x, los ajustes se
sincronizar automáticamente. El estado de la conexión no se conserva entre los ejércitos, para que los clientes deben volver a conectar
después se produce la conmutación por error, pero OpenVPN detectará el fallo de la conexión y vuelva a conectar a un minuto o
por lo que la conmutación por error. CARP se discute en el capítulo 24, Firewall de redundancia / alta disponibilidad. A partir de
pfSense 2.0.2, el servidor de seguridad se apagará automáticamente instancias de OpenVPN como sea necesario cuando un CARP
nodo está en un estado de copia de seguridad. Esto evita que OpenVPN de hacer conexiones salientes innecesarios en modo cliente, y en tanto el cliente como el modo de servidor que impide OpenVPN mantengan innecesaria
rutas. Cuando el estado CARP transiciones de dominar, las instancias de OpenVPN se inician automáticamente.

Conexiones OpenVPN puenteados

Las configuraciones OpenVPN discutidos hasta este punto han sido derrotados, utilizando `tonel` interfaces. Este suele ser la forma preferida de conexión de clientes de VPN, pero OpenVPN también ofrece la opción de usar `grifo` interfaces y la reducción de los clientes directamente en su LAN u otra red interna. Esto puede hacer que los clientes remotos parecen ser en su LAN local. La mayor parte de los ajustes para la creación de un mando a distancia con puente
VPN de acceso son los mismos que antes para una VPN de acceso remoto tradicional. Sólo las diferencias serán señalado aquí.

Modo de Dispositivo

El primer paso en la creación de un puente de este tipo es para seleccionar grifo de modo de dispositivo desplegable del servidor.

Túnel Red

Usted también querrá asegurarse de que las cajas de IPv4 e IPv6 Túnel de red Túnel de red son
vacía. La forma en que un `grifo` funciones de puente OpenVPN, que no necesita una red de túneles, como OpenVPN
no utilizar la misma asignación de dirección que lo hace para `tonel` modo.

DHCP Puente

Si se selecciona Puente DHCP, DHCP será pasada a través de la interfaz de puente que se pueden configurar
más tarde. En el escenario más común, esto sería LAN. Usando este método, los clientes de conexión se
recibir IPs desde el mismo pool de DHCP que utilizan los clientes de LAN cableadas directamente.

Puente de interfaz

El desplegable Puente de interfaz no crea realmente el puente, sólo indica que OpenVPN
qué interfaz se utilizará para el puente. En la mayoría de los casos, esto sería LAN. Este ajuste controla
qué dirección IP existente y la máscara de subred se utilizan por OpenVPN para el puente. Fijar esto a ninguno
hará que la configuración del puente servidor DHCP de abajo para ser ignorados.

Puente Servidor DHCP Start / End

Al utilizar `grifo` el modo como un servidor de múltiples puntos, puede opcionalmente suministrar una gama DHCP a utilizar en el
interfaz a la que esta `grifo` se tiende un puente instancia. Si estos valores se dejan en blanco, DHCP será pasada
hasta se omitirán la LAN, y el ajuste por encima de la interfaz. Esto le permite dejar de lado un
rango de IPs para uso exclusivo de los clientes OpenVPN, por lo que pueden estar contenidos en una porción de su
red interna, en lugar de consumir IPs del rango DHCP existente. Introduzca el Puente del servidor
Valores de dirección IP DHCP Start y Puente Servidor DHCP final según sea necesario.

Creación de la Puente

Una vez que el OpenVPN `grifo` servidor se ha creado, la interfaz debe ser asignado y con puentes a su
interfaz interna.

Asigne la interfaz OpenVPN

Con el fin de incluir la interfaz VPN en un puente, se debe asignar. El procedimiento para la asignación de
una interfaz está cubierto anteriormente en este capítulo, en la sección llamada "asignación de interfaz y
configuración ".

Cree Puente

Una vez que la interfaz de VPN se ha asignado, navegue hasta Interfaces □ (Asignar) en la ficha Bridges. Desde

allí, clickto crear un puente. En la pantalla resultante ctrl-click tanto la interfaz de VPN y el
interfaz a la que usted desea que sea un puente (por ejemplo, LAN), a continuación, haga clic en Guardar. Más
información sobre la reducción de
se puede encontrar en el capítulo 13, Tender un puente.

Conéctate con Clientes

Los clientes que se conectan a la VPN también se deben configurar para utilizar `grifo` modo. Una vez que se ha establecido, puede
conectar con un cliente (por ejemplo, uno exportado utilizando el paquete OpenVPN Client Export) y los clientes
deben recibir una IP dentro de la subred interna, como si fueran de su LAN. Ellos recibirán
difusión y el tráfico multicast también.

Opciones de configuración personalizada

OpenVPN ofrece docenas de opciones de configuración, muchos más allá de los campos más utilizados que se presentan en la GUI. Esto es por qué existe el cuadro de opciones de configuración personalizadas. Usted puede rellenar un número ilimitado de opciones de configuración adicionales, separados por punto y coma. Este sección cubre las opciones de personalización de uso más frecuente de forma individual. Hay muchos más, aunque rara vez se necesita. La página de manual OpenVPN [http://openvpn.net/index.php/open-source/documentation/manuals/65-openvpn-20x-manpage.html] a todos los detalles. Tenga cuidado al añadir personalizada opciones, no hay validación de entrada aplicado para garantizar la validez de las opciones utilizadas. Si una opción es emplean de manera incorrecta, el cliente o el servidor OpenVPN no se inicien. Usted puede ver los registros de OpenVPN bajo

Estado Sistema registra en la ficha OpenVPN para garantizar las opciones usadas son válidas. Cualquiera de las opciones no válidas
dará lugar a un mensaje de registro `Opciones error: opción no reconocida o desaparecidos Parámetro (s)` seguido de la opción que ha provocado el error.

Opciones de ruta

Para agregar rutas adicionales para un cliente OpenVPN en particular o servidor, se utiliza el ruta costumbre opción de configuración. El siguiente ejemplo agrega una ruta para 10.50.0.0/24.

ruta 10.50.0.0 255.255.255.0

Para añadir varias rutas, sepárelas con un punto y coma:

ruta 255.255.255.0 10.50.0.0; ruta 10.254.0.0 255.255.255.0

La ruta opción de configuración se utiliza para añadir rutas a nivel local. Para una configuración del servidor OpenVPN utilizando PKI, también puede empujar rutas adicionales a los clientes. Para impulsar las rutas para 10.50.0.0/24 y 10.254.0.0/24 a todos los clientes, utilice la siguiente opción de configuración personalizada.

empuje route10.50.0.0 " 255.255.255.0 "; empuje "Ruta 10.254.0.0 255.255.255.0 "

Reorientación de la puerta de enlace predeterminada

OpenVPN también le permite cambiar la puerta de enlace predeterminada del cliente para la conexión OpenVPN, por lo todo el tráfico desde el cliente es empujado a través de la VPN. Esto es ideal para redes locales no confiables, tales puntos de acceso inalámbricos, como ya que proporciona protección frente a numerosos ataques que hay un riesgo de que no se confía
redes. Esto se puede configurar en la interfaz gráfica de ahora, el uso de la casilla Remitir Gateway en el OpenVPN configuración de la instancia. Si usted desea hacer esto manualmente, añada la siguiente opción de personalización:

empujar "def1 redirigir-gateway"

También puede introducir esto como una opción personalizada en el cliente mediante el uso de redirect-gateway def1 sin especificar empujar. (Tenga en cuenta la opción de las letras "def", seguido por el dígito uno, no la letra "L".)

Especificación de la dirección IP que puede utilizar

La local opción personalizada permite especificar la dirección IP del servicio OpenVPN utilizará. Este ya no es necesario ya que puedes seleccionar una interfaz o VIP desde la interfaz desplegable para realizar esta tarea. Si usted tiene que hacer esto manualmente, puede ser una dirección IP, como 1.2.3.4 locales, o un FQDN tales como:

myopenvpn.dyndns.org locales

Esto se utiliza sobre todo en escenarios multi-WAN, como se describe en la sección llamada "OpenVPN y Multi-WAN ", o en combinación con la carpa VIP.

Compartir un puerto con OpenVPN y Web Servidor

Si quieres ser más astuto / cuidado con el servidor OpenVPN, usted puede tomar ventaja de
De OpenVPN puerto compartido capacidad que le permite pasar a cualquier tráfico no OpenVPN a otra IP
detrás del firewall. El caso de uso habitual para esto sería para ejecutar el servidor OpenVPN en TCP/443 puerto,
y en lugar de un puerto hacia adelante, deje que OpenVPN mano del tráfico HTTPS a un servidor web.

A menudo en las redes bloqueado, sólo los puertos 80 y 443 como se les permitirá por razones de seguridad,
ejecutar instancias de OpenVPN en estos puertos permitidos puede ayudarle a salir de situaciones donde el acceso
de lo contrario puede ser restringido.

Para configurar esto, configurar un servidor OpenVPN para escuchar en el puerto TCP 443, y añadir una regla de firewall para pasar
el tráfico a la IP WAN (o lo que sea IP utilizada para OpenVPN) en el puerto 443. Usted no necesita ningún puerto
hacia delante o reglas de firewall para pasar el tráfico a la IP interna.

En las opciones personalizadas de la instancia de OpenVPN, agregue lo siguiente:

puerto compartido x.x.x.x 443

Donde x.x.x.x es la dirección IP interna del servidor web para que el tráfico no VPN será
reenviado.

Ahora bien, si usted señala que hay un cliente OpenVPN, debe conectar y funcionar bien, y si apunta una web
navegador al mismo IP, debe conectarse al servidor web.

> Nota
>
> Esto requiere el uso de TCP, y puede resultar en la reducción de rendimiento de VPN.

Controlar parámetros del cliente a través de RADIUS

Cuando se utiliza como fuente de RADIUS de autenticación de una VPN, pfSense admite la recepción de algún cliente
parámetros de configuración del servidor RADIUS como atributos respuesta. Estos siguen el avpair de Cisco
estándar. Los valores que puede especificar a través de estos valores avpair son:

• inacl - reglas de firewall de entrada para regular el tráfico desde el cliente al servidor.

• outacl - reglas de firewall de salida para regular el tráfico desde el servidor al cliente.

• dns-servidores - Servidores DNS para empujar al cliente.

• Ruta - instrucciones de ruta adicionales para empujar al cliente.

Solución de problemas OpenVPN

Si encuentra problemas al intentar usar OpenVPN, esta sección ofrece información sobre
solución de problemas de los problemas más comunes se encuentran los usuarios.

Compruebe OpenVPN Estado

El primer lugar para buscar es Estado OpenVPN. El estado de la conexión para cada VPN se mostrará
allí. Si se conecta una VPN, a la espera, volver a conectar, y así sucesivamente, que se indicará en esa pantalla.
Para obtener más información, consulte la sección "Comprobación del estado de clientes y servidores OpenVPN".

Compruebe Firewall Log

Si una conexión VPN no establece o no establecer, pero no pasa tráfico, comprobar el firewall registros bajo Estado Sistema de sesión en la ficha Firewall. Si usted ve el tráfico del túnel el ser mismo bloqueados, tales como el tráfico de la WAN IP en el puerto 1194, y luego ajustar las reglas del firewall WAN en consecuencia.
Si usted ve el tráfico bloqueado en la interfaz de OpenVPN, agregar reglas a la pestaña OpenVPN para permitir el tráfico allí.

Algunos servidores funcionan, pero no todos

Si el tráfico entre máquinas más de las funciones de VPN correctamente, pero algunos hosts no, esto es comúnmente una de cuatro cosas.

. 1 Falta, es incorrecto o ignorado puerta de enlace predeterminada - Si el dispositivo no dispone de una puerta de enlace predeterminada o
tiene uno que apunta a algo distinto de pfSense, no saber cómo obtener correctamente de nuevo a
la red remota en la VPN. Algunos dispositivos, incluso con una puerta de enlace predeterminada especificada, no utilice
que la puerta de enlace. Esto se ha visto en diversos dispositivos integrados, incluyendo cámaras IP y algunos
impresoras. No hay nada que puedas hacer para que no sea conseguir el software en el dispositivo
fijo. Usted puede verificar esto mediante la ejecución 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 la sección llamada
"Uso de tcpdump desde la línea de comandos". Si usted ve el tráfico que va de la interfaz en el interior de la
firewall, pero no hay respuestas a volver, el dispositivo no está encaminando correctamente su tráfico de respuesta (o podría
potencialmente ser bloqueo que 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 la otra es
10.254.0.0/24, y un anfitrión 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 la subred VPN remota es parte de la red local
y por lo tanto de enrutamiento no funcionará correctamente.

. 3 Anfitrión firewall - si hay un firewall en el host de destino, no se puede permitir que las conexiones.

4 Las reglas de firewall en pfSense -. Garantizar las reglas en ambos extremos permiten que el tráfico de la red deseada.

Compruebe los registros de OpenVPN

Vaya a Estado Los registros del sistema y haga clic en la pestaña de OpenVPN para ver los registros de OpenVPN. Sobre
conexión, OpenVPN registrará algo similar a lo siguiente (el número siguiente `openvpn`
será diferente, es el ID de proceso del proceso OpenVPN hacer la conexión).

```
openvpn [32194]: UDPv4 enlace remoto: 1.2.3.4:1194
openvpn [32194]: conexión del mismo nivel Iniciada con 192.168.110.2:1194
openvpn [32194]: Secuencia de inicialización Completado
```

Si usted no ve la `vincular a distancia` y `Conexión del mismo nivel ya iniciada` mensajes sobre intentando conectar, es la causa más probable sea la configuración del cliente incorrecta, por lo que el cliente no está intentando
para conectar con el servidor correcto, o reglas de firewall incorrectas bloqueando la conexión del cliente.

Asegúrese de que no se solapan las conexiones IPsec

Debido a la forma IPsec lazos en el kernel de FreeBSD, cualquier acceso a una conexión IPsec coincide con el subredes locales y remotas que existe cuando IPsec está habilitado (aunque no es hasta) causarán que el tráfico nunca ser enrutados a través de la conexión OpenVPN. Cualquier conexión IPsec que especifican el mismo local, y redes remotas se deben desactivar. Si lo has deshabilitado o quitado un túnel IPsec recientemente,

comprobar que sus entradas SPD se han eliminado examinado Estado IPsec en la ficha SPD. Si se están presentes, sacarlos de esa pantalla.

Compruebe la tabla de enrutamiento del sistema

Busque Diagnóstico Rutas y revisar las rutas añadidas. Para VPNs de sitio a sitio, debe ver rutas para la red remota (s) a la adecuada `tonel` o `grifo` interfaz. Si las rutas están desaparecidos o incorrecta, su red local, de red remota, o las opciones personalizadas no están configurados correctamente. Si está utilizando una configuración de clave compartida y no PKI, asegúrese de que no está utilizando comandos de "presión" se en lugar de añadir rutas a ambos extremos utilizando "ruta" de opciones personalizadas, como en la sección denominada "Enrutamiento opciones ".

Prueba de diferentes puntos de vista

Si la conexión se muestra como en los registros, pero no funciona desde la red LAN, inténtalo de la firewall propio, primero mediante la interfaz en el interior que se utiliza para la conexión OpenVPN (típicamente LAN) como la fuente de ping. Si eso no funciona, SSH en el servidor de seguridad y la opción 8 para elegir un comando pedirá. Carrera ping- x.x.x.x en la línea de comando, reemplazando x.x.x.x con una dirección IP en el control remoto lado de la VPN. Esto hará que el tráfico a iniciarse desde el IP de la `tonel` interfaz está utilizando por OpenVPN. Esto puede ayudar a reducir los problemas de enrutamiento en la red remota.

Trace el tráfico con tcpdump

Uso tcpdump para determinar donde se ve el paso y en donde no es es uno de los más útiles las técnicas de solución de problemas. Comience con la interfaz interna (comúnmente LAN) en el lado donde el se está iniciando el tráfico, el progreso de la `tonel` interfaz en dicho servidor de seguridad, entonces la `tonel` interfaz en el servidor de seguridad remoto, y, finalmente, la interfaz en el interior en el servidor de seguridad remoto. Determinar donde el tráfico se ve y no donde es puede ayudar en gran medida en la reducción a donde se encuentra el problema. Paquete captura se trata en detalle en el Capítulo 29, Captura de paquetes.

Rutas no empujar a un cliente

Si usted está tratando de utilizar la caja de la red local o una empuje declaración para empujar rutas a un cliente, y el cliente no está recibiendo adecuadamente, un par de cosas podrían estar ocurriendo:

• Compruebe que está utilizando una configuración del servidor SSL / TLS con una red de túneles más grande que un / 30.
De OpenVPN servidor único modo entra en vigor si usted está utilizando una subred suficientemente grande para contener múltiples clientes, tales como un / 24.

• Si el cliente se ejecuta en Windows Vista, Windows 7, o similar, intente ejecutar el cliente como Administrador. Algunas versiones del cliente OpenVPN requieren el modo de administrador para aplicar rutas a la tabla de enrutamiento del sistema.

• Si usted está utilizando una configuración de clave compartida, rutas empujando no funcionarán. Utilice las instrucciones de ruta en cada lado (Cliente y servidor) para dirigir el tráfico a subredes en el otro extremo del túnel.

Por qué no puedo hacer ping a algunas direcciones de adaptador OpenVPN?

En el modo de servidor SSL / TLS, OpenVPN no responderá a un ping en ciertas direcciones virtuales utilizados únicamente para los puntos finales de enrutamiento. No se fíe de los ping a direcciones de extremo OpenVPN como un medio de determinar si el túnel está pasando tráfico correctamente. En su lugar, mesa de ping algo en la subred remota, tales como la IP LAN del servidor.

De acuerdo con la OpenVPN FAQ [http://www.openvpn.net/index.php/documentation/faq.html], en el sección titulada ¿Por qué la opción "ifconfig-pool" de OpenVPN utiliza a / 30 de subred (4 direcciones IP privadas por cliente) cuando se utiliza en modo TUN?:

> Como 192.168.1.5 es sólo una dirección IP virtual dentro del servidor OpenVPN, que se utiliza como un punto final para las rutas, OpenVPN no se molesta en responder pings en esta dirección, mientras que la 192.168.1.1 es una dirección IP real en los servidores de O / S, por lo que responderá a los pings.

Esto puede parecer un poco contra-intuitivo, ya que en el servidor se ve algo como esto en el ifconfig salida:

```
tun0: flags = 8051 <UP,POINTOPOINT,RUNNING,MULTICAST> métrica 0 mtu 1500
 inet6 fe80 :: 202: b3ff: fe03: 8028% tun0 prefixlen 64 scopeid 0xc
 inet 192.168.100.1 -> 192.168.100.2 máscara de red 0xffffffff
 Inaugurado por PID 27841
```

Mientras que el cliente muestra:

```
tun0: flags = 8051 <UP,POINTOPOINT,RUNNING,MULTICAST> métrica 0 mtu 1500
        inet6 fe80 :: 202: b3ff: FE24: 978c% tun0 prefixlen 64 scopeid 0xa
        inet 192.168.100.6 -> 192.168.100.5 máscara de red 0xffffffff
        Inaugurado por el PID 1949
```

En este caso, lo más probable es que no puede hacer ping a 0.5 o 0.1. 0.5 porque es una dirección virtual, y 0.1 porque tiene
hay una ruta para llegar a él directamente. Los 0.5 y 0.6 direcciones son parte de un / 30 que va desde 0,4 hasta 0,7, y tratando
hacer ping a 0.1 saldría su ruta por defecto en lugar.
Hay muchos casos en los que puede hacer ping al otro lado de un túnel OpenVPN, pero no el local. Este
También es contrario a la intuición, sino que trabaja sobre todo en los casos en los que tenga un vínculo de sitio a sitio. Si el servidor
muestra sus direcciones tun como "x.x.x.1 -> x.x.x.2 " y el cliente muestra el reverso - "x.x.x.2 -
>x.x.x.1 ", entonces usted puede hacer ping al otro lado de los dos extremos.

El cliente específico entrada iroute Override parece no tener efecto

Si usted está tratando de configurar una configuración de sitio a sitio PKI OpenVPN, es necesario agregar una iroute declaración
de la subred del cliente en el cliente específico juego de separadores invalidaciones para el nombre común del certificado de cliente.
En primer lugar, asegúrese de que los partidos de nombres comunes y que la vía interna se está aprendiendo / añadida, ya que
debería ser. Es posible que necesite aumentar la verbosidad registro de OpenVPN (es decir, verbo 10 en las opciones de personalización)
para ver si esto funciona.
Asimismo, para cada red que desee utilizar un iroute declaración, usted también necesita una instrucción de ruta en opciones de personalización de la definición de servidor. La ruta declaraciones son para el sistema operativo para saber que lo que deberían
encaminarse a OpenVPN desde cualquier otro lugar. La iroute declaraciones son internos a OpenVPN, por lo se sabe que la red va a qué cliente.

¿Por qué mis clientes OpenVPN todos reciben la misma IP?

Si utiliza el mismo certificado para todos sus clientes, que se recomienda en absoluto, entonces usted puede encontrar que los clientes están asignados la misma dirección IP cuando se conectan. Para evitar esto, consulte Duplicar Conexiones en la configuración del servidor.

Importación de los parámetros DH OpenVPN

Si va a importar una configuración existente OpenVPN en pfSense 2.0, es posible que se esté preguntando "¿Dónde está la
Campo Parámetros DH? "Bueno, todo está cuidado detrás de las escenas.

Parámetros de DH no son específicos de una configuración dada en la forma en que sus certificados o claves son. La interfaz gráfica de usuario
en 1.2.3 y por debajo no era lo suficientemente inteligente como para generarlos de forma automática.

En pocas palabras, los parámetros DH son algunos bits adicionales de aleatoriedad que ayudan durante la tecla proceso de intercambio. Ellos no tienen que coincidir en ambos lados del túnel, y los nuevos se pueden hacer en cualquier momento. No hay necesidad de importar un conjunto existente de los parámetros de DH.

Capítulo 20. Traffic Shaper

Limitación de tráfico, o la calidad de la red de servicio (QoS), es una forma de priorizar el tráfico de red atravesar el firewall. Sin limitación de tráfico, los paquetes se procesan en un primer lugar en / primero en salir por la base
el servidor de seguridad. QoS ofrece un medio de dar prioridad a diferentes tipos de tráfico, lo que garantiza que la alta prioridad
servicios reciban el ancho de banda que necesitan antes de los servicios prioritarios menores. El asistente regulador de trafico en
pfSense le da la capacidad para configurar rápidamente QoS para escenarios comunes y reglas personalizadas pueden También se creará para las tareas más complejas. Por simplicidad, el sistema de limitación de tráfico en pfSense también puede
se conoce también como "shaping". El acto de la modulación del tráfico puede ser llamado "dar forma".

Traffic Shaping Basics

Para aquellos de ustedes que no están familiarizados con la modulación del tráfico, es como una especie de guardia de seguridad en un exclusivo
club. Los VIPs (paquetes muy importantes) siempre que sea en el primero y sin esperar. La regularidad
paquetes tienen que esperar su turno en la fila, y los paquetes de "indeseables" pueden ser mantenidos fuera hasta después de la verdadera
fiesta ha terminado. Al mismo tiempo, el club se mantiene a la capacidad y no sobrecargada. Si más VIPs vienen a lo largo de
La forma en que la configuración se lleva a cabo en pfSense puede ser un poco confuso al principio, pero una vez que la mecánica básica es comprendido, puede ser fácil de configurar algunos
paquetes regulares.
porque el tráfico tiene que ser limitada en un lugar donde pfSense en realidad puede controlar el flujo. Entrante
el tráfico de Internet pasa a un host en la LAN (descarga) tiene la forma de realidad que viene fuera de
la interfaz LAN del sistema pfSense. De la misma manera, el tráfico que va desde la LAN a la
Tiene la forma de Internet (carga) cuando dejando la WAN.

Hay colas de tráfico, y las normas de calidad de servicio. Las colas son donde el ancho de banda y
prioridades estan ya asignados. Controlan las reglas de conformación de tráfico cómo se asigna el tráfico en esas colas.
Reglas para el shaper funcionan de manera similar a las reglas del cortafuegos, y permiten a las características similares de búsqueda. Si un
paquete coincide con una regla de la talladora, se le asignará en las colas especificadas por esa regla.

Lo que el Traffic Shaper puede hacer por usted

La idea básica de limitación de tráfico, subir y bajar las prioridades de los paquetes, es simple.
Sin embargo, el número de formas en las que este concepto se puede aplicar es vasta. Estos son sólo algunos común ejemplos que han demostrado ser populares entre nuestros usuarios.

Sigue navegando Smooth

Enlaces asimétricos, en los que la velocidad de descarga se diferencia de la velocidad de subida, son comunes en estos día, especialmente con DSL. Algunos enlaces son tan fuera de balance que la velocidad de descarga máxima es de
casi inalcanzable, porque es difícil enviar suficiente ACK (reconocimiento) los paquetes para mantener
tráfico que fluye. Paquetes ACK se transmiten de vuelta al remitente por el host receptor para indicar que
los datos se ha recibido correctamente, y para señalar que está bien para enviar más. Si el remitente no recibe
ACKs en tiempo y forma, los mecanismos de control de congestión de TCP entrará en funcionamiento y ralentizar el conexión.

Usted puede haber notado esta situación antes: Al cargar un archivo a través de un vínculo, la navegación y
la descarga se desacelera a paso de tortuga o puestos. Esto sucede porque la parte de carga del circuito está lleno
de la carga de archivos, hay poco espacio para enviar paquetes ACK que permiten descargas siguen fluyendo.
Al utilizar el shaper de priorizar los paquetes ACK, se puede lograr, las velocidades de descarga más rápidas más estables en vínculos asimétricos.

Esto no es tan importante en los enlaces simétricos donde la velocidad de carga y descarga son los mismos, pero todavía puede ser desriable si el ancho de banda de salida disponible es muy utilizada.

Mantenga Llamadas VoIP Claro

Si sus Voz sobre IP las llamadas utilizan el mismo circuito que los datos, a continuación, las cargas y descargas pueden degradar
su calidad de la llamada. pfSense puede priorizar el tráfico de llamadas por encima de otros protocolos, y asegurarse de que las llamadas
hacerlo a través de claridad sin romper, incluso si usted está de streaming de vídeo de alta definición de Hulu en el mismo tiempo. En lugar de la llamada ruptura, la velocidad de las otras transferencias se reducirá a dejar espacio para las llamadas.

Reducir Lag Gaming

También hay opciones para dar prioridad al tráfico asociado con los juegos en red. Similar a priorización de llamadas VoIP, el efecto es que, incluso si se descarga durante el juego, el tiempo de respuesta del juego aún debe ser casi tan rápido como si el resto de su conexión fuera de ralentí.

Mantenga las aplicaciones P2P Llegada

Al reducir la prioridad del tráfico asociado a conocidos puertos peer-to-peer, puede estar más tranquilos sabiendo que, incluso si estos programas están en uso, no van a obstaculizar el resto del tráfico en su red. Debido a su menor prioridad, otros protocolos serán favorecidos sobre el tráfico P2P, que se limitará, cuando cualquier otros servicios necesitan el ancho de banda.

Limitaciones de hardware

Conformación del tráfico se lleva a cabo con la ayuda de `ALTQ`. Por desgracia, sólo un subconjunto de todos soportados tarjetas de red son capaces de usar estas características debido a que los conductores deben ser alterados para apoyo conformación. Las siguientes tarjetas de red son capaces de utilizar la modulación del tráfico, según la página de manual para `altq (4)`:

```
edad (4), cerveza inglesa (4), una (4), ATH (4), Aue (4), AWI (4), BCE (4), BFE
(4), BGE (4), DC (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), nfe (4), npe (4), nve (4), RAL (4), re (4), rl
(4),
ron (4), sf (4), hermana (4), sk (4), ste (4), stge (4), UDAV (4), ural (4), vge
(4), vr (4)
wi (4), y xl (4).
```

Limitaciones de la Traffic Shaper implementación en 1.2.x

Envolver un GUI alrededor de los componentes para la conformación de tráfico subyacentes en pfSense demostrado ser un muy difícil
tarea, y carente de funcionalidad en el sistema subyacente en algunas áreas también limita sus capacidades. La aplicación que existe en 1.2.x funciona bien, dentro de sus límites. El regulador de trafico en pfSense 2.0 tiene sido reescrito para hacer frente a estas limitaciones.

Sólo dos soporte de interfaz

El shaper sólo funciona correctamente con las implementaciones que consta de dos interfaces LAN y WAN. Multi-WAN, y redes con otras interfaces OPT no funcionarán si lo deseas. El shaper en 2.0
Cómo acomodar múltiples interfaces correctamente.

El tráfico a la interfaz LAN afectada

El tráfico a la IP LAN está en la cola de la misma manera que el tráfico pasa por el cortafuegos. Así que si tu web interfaz utiliza HTTPS, y su cola regulador de trafico para HTTPS está lleno, se retrasará su tráfico a la gestión de la interfaz lo mismo que si su solicitud HTTPS íbamos a salir a Internet. Si
usar pings a la IP LAN de un sistema de monitoreo, es posible que vea retardo y jitter significativa para este misma razón.

Por extensión también se aplica a otros servicios ofrecidos por el router pfSense. Los usuarios del proxy squid paquete se han dado cuenta de que sus clientes locales reciben datos desde el proxy sólo a la velocidad de su WAN, y por lo que nunca parecía estar el almacenamiento en caché de datos. De hecho, fue el almacenamiento en caché de datos, pero también se perfila
el tráfico al mismo tiempo.

Sin inteligencia de las aplicaciones

La talladora no es capaz de diferenciar realmente entre protocolos. El tráfico que utiliza el puerto TCP 80 es considerado como HTTP, si es realmente HTTP o se trata de una aplicación P2P utilizando el puerto 80. Esto puede ser una
problema importante en algunos entornos.

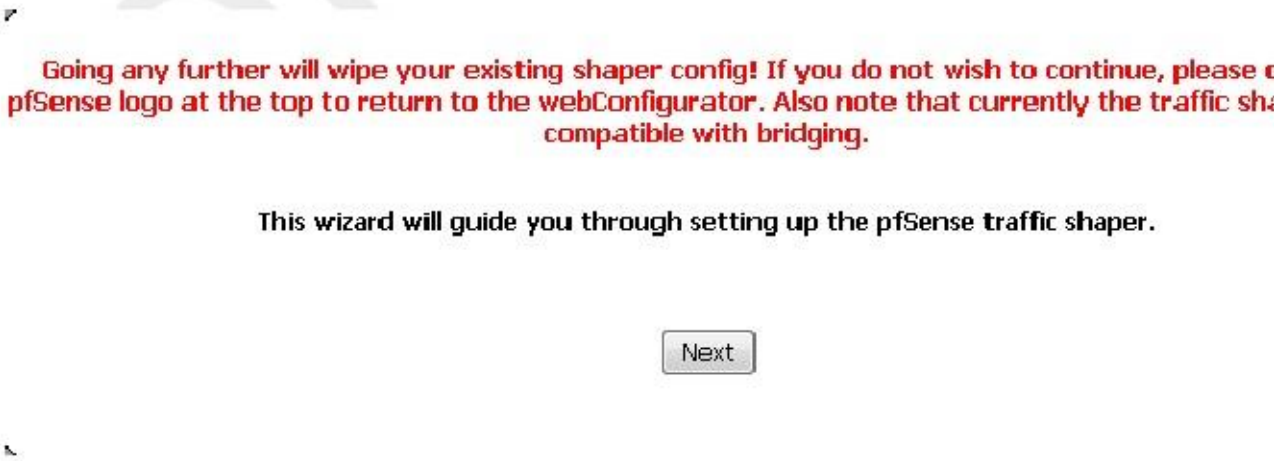
Configuración de la talladora del tráfico con la Mago

Se recomienda que configure el regulador de trafico por primera vez mediante el asistente, que se le guiará a través del proceso. Debido a la complejidad de las colas de la talladora y reglas, que no es un buen idea para intentar empezar de cero en su cuenta. Si necesita reglas personalizadas, con el asistente y aproximarse a lo que se necesita, a continuación, hacer las reglas de encargo después. Cada configuración se proyectará colas únicas, y las reglas que controlarán el tráfico que se asigna a esas colas. Si desea
para configurar todo manualmente, basta con especificar la velocidad WAN en la primera pantalla, haga clic en Siguiente a través de todas las pantallas restantes sin configurar nada.

Inicio del Asistente

Para empezar a utilizar el Asistente para la asignación de tráfico, haga clic en Firewall Traffic Shaper. El asistente debe
iniciará automáticamente como en la Figura 20.1, "Inicio del Asistente de la talladora". Si ha completado la configuración
asistente antes, o tiene reglas personalizadas, verás en su lugar la lista de reglas de la talladora. Para borrar el vigente reglas de la talladora y empezar de cero, haga clic en la ficha Asistente EZ talladora que relanzar el asistente precargada con la configuración actual. Al terminar cada pantalla del asistente, haga clic en Siguiente para continuar a la siguiente página.

Figura 20.1. Inicio del Asistente de la talladora



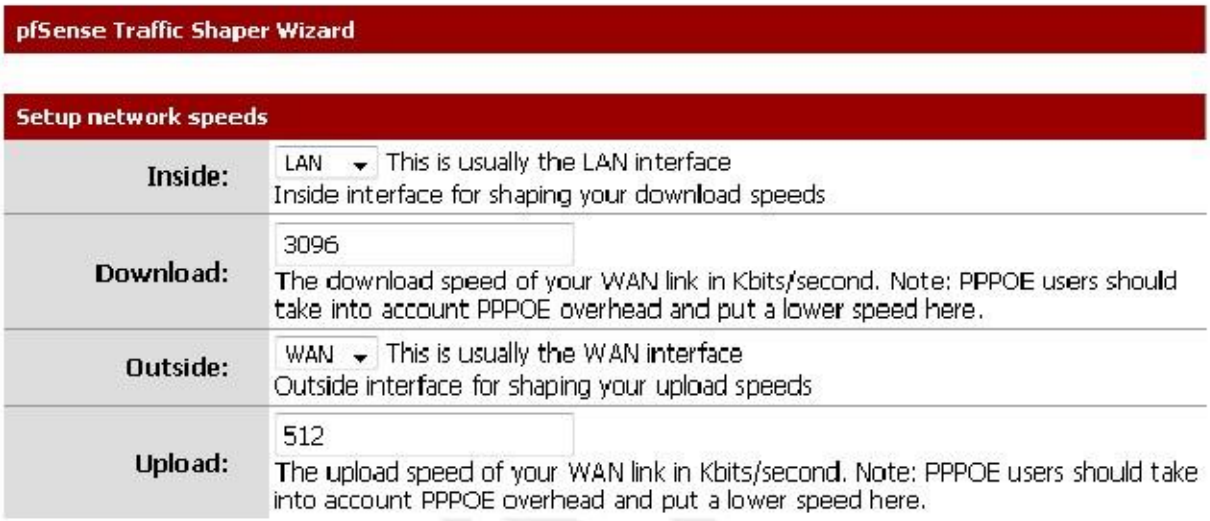
Redes y plazos de envío

Esta pantalla, como se muestra en la Figura 20.2, "Configuración de la talladora", es donde se configura la red interfaces que será el interior y el exterior desde el punto de vista de la talladora, junto con el
Descargar y velocidades de carga. Dependiendo de tu tipo de conexión, la verdadera velocidad del enlace no puede ser el Velocidad real de uso. En el caso de PPPoE, usted tiene no sólo PPPoE gastos generales, sino también de cabeza de

el vínculo subyacente en red ATM se utiliza en la mayoría de las implementaciones de PPPoE. Según algunos cálculos, entre la cabeza de la ATM, PPPoE, IP y TCP, puede perder hasta un 13% de la anunciada velocidad de enlace.

En caso de duda de lo que establezca la velocidad, ser un poco conservador. Reducir en 10 a 13% y el trabajo de su camino de vuelta. Si usted tiene una 3Mbit / s línea, póngalo por alrededor de 2.700 y probarlo. Siempre se puede editar el
cola de matriz resultante después y ajustar la velocidad. Si se establece bajo, la conexión será maximizado en exactamente a la velocidad establecida. Sigue empujando hacia arriba más alto hasta que ya no obtiene ningún beneficio de rendimiento.

Figura 20.2. Configuración de la talladora

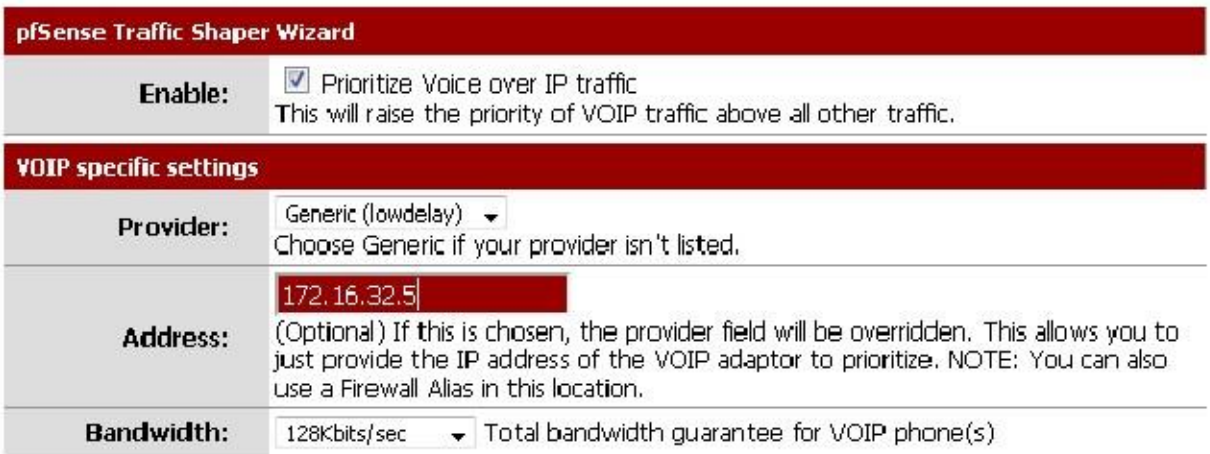


Voz sobre IP

Hay varias opciones disponibles para el manejo de tráfico de llamadas VoIP, que se muestra en la Figura 20.3, "Voz sobre
IP ". La primera opción, priorizar el tráfico de voz sobre IP, es auto-explicativo. Esto permitirá a la priorización del tráfico de VoIP y este comportamiento puede ser afinado por los otros ajustes de abajo. Hay algunos bien-proveedores conocidos que incluyen Vonage, VoicePulse, PanasonicTDA y servidores Asterisk. Si usted tiene un proveedor diferente, puede elegir Genérico, o sustituir este valor con el campo de dirección al introduciendo 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 para sus teléfonos VoIP. Esto variará basa en el número de teléfonos que tiene, y cuánto ancho de banda de cada sesión utilizará.

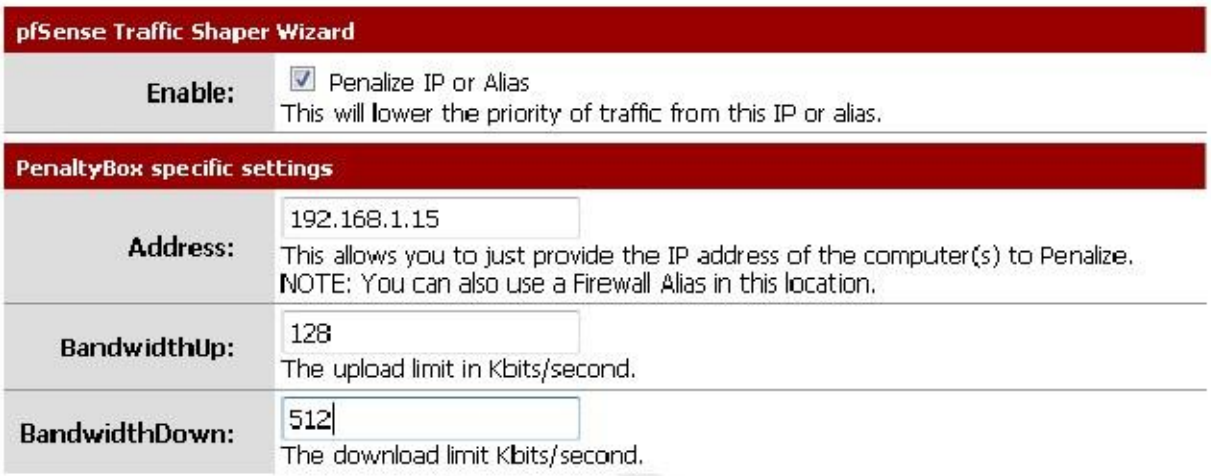
Figura 20.3. Voz sobre IP



Área de castigo

La caja de la pena, se muestra en la Figura 20.4, "Penalty Box", es un lugar al que se puede relegar
mal comportamiento usuarios o dispositivos que de otra manera consumen más ancho de banda de lo deseado. Estos usuarios
se les asigna un ancho de banda de tapa dura, que no pueden exceder. Compruebe la IP Penalizar o Alias para permitir la función, escriba una dirección IP o alias en el cuadro Dirección y, a continuación, introduzca los límites de carga y descarga en
kilobits por segundo en sus respectivas cajas.

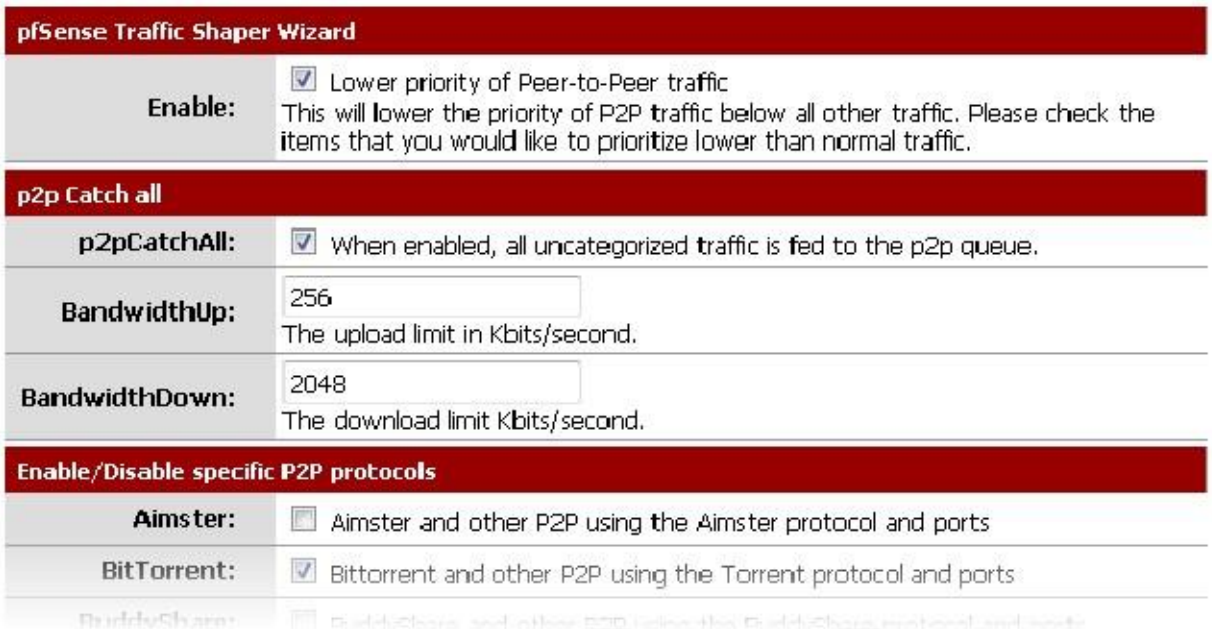
Figura 20.4. Área de castigo



Redes Peer-to-Peer

En la siguiente pantalla, se muestra en la Figura 20.5, "Redes Peer-to-Peer", le permitirá establecer controles sobre muchos
peer-to-peer (P2P) protocolos de red. Por su diseño, los protocolos P2P utilizarán todo el ancho de banda disponible a menos que los límites se ponen en marcha. Si usted espera que el tráfico P2P en la red, es una buena práctica para asegurar
que el resto del tráfico no se degrada debido a su uso. Para penalizar el tráfico P2P, compruebe primero Baja prioridad del tráfico Peer-to-Peer.
Muchas de las tecnologías P2P deliberadamente tratan de evitar la detección. Bittorrent es especialmente culpable de esto comportamiento. A menudo utiliza los puertos no estándar o al azar, o los puertos asociados con otros protocolos.
Puede marcar la opción p2pCatchAll lo que hará que cualquier tráfico no reconocida a asumir en
El tráfico P2P y su prioridad bajaron en consecuencia. Puede establecer límites de ancho de banda de disco para este tráfico
debajo de la regla de cajón de sastre. Los límites de ancho de banda de carga y descarga se encuentran en Kilobits por segundo.
Las opciones restantes se componen de varios protocolos P2P conocidos, más de 20 en total. Comprobar
cada uno que desea ser reconocido.

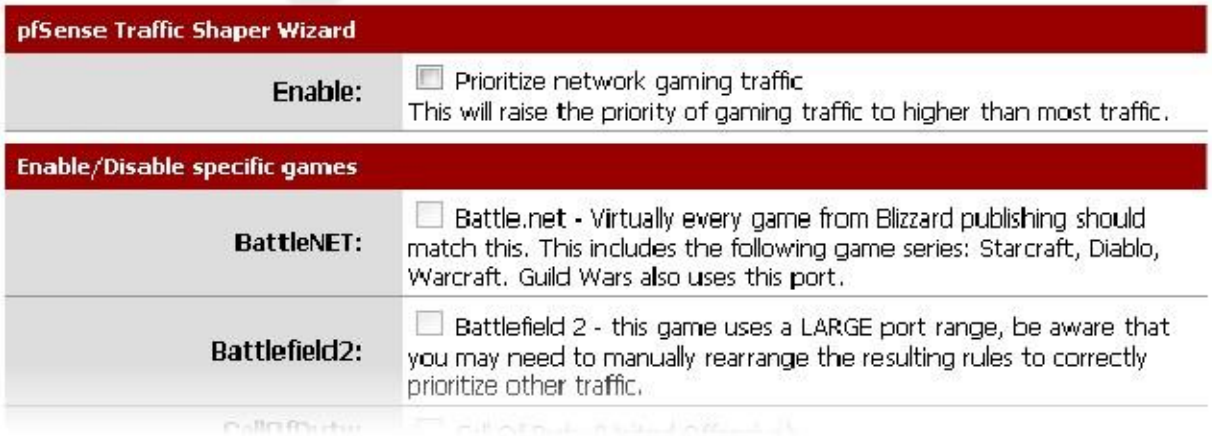
Figura 20.5. Redes Peer-to-Peer



Network Games

Muchos juegos se basan en la baja latencia para ofrecer una buena experiencia de juego en línea. Si alguien trata de descargar archivos de gran tamaño o parches del juego durante el juego, que el tráfico pueda tragar con facilidad hasta los paquetes
asociado con el juego en sí y la causa de retraso o desconexiones. Al marcar la opción de prioridad
tráfico de juegos en red, como se ve en la Figura 20.6, "Juegos de la red", se puede aumentar la prioridad de juego
el tráfico de manera que se transfiere primero y dado un trozo de ancho de banda garantizado. Hay muchos
partidos de la lista, marque todas las que deben priorizarse. Si tu juego no está aquí aún puede
que desee comprobar un juego similar, de modo que va a tener una norma de referencia que podrá ser alterada después.

Figura 20.6. Network Games



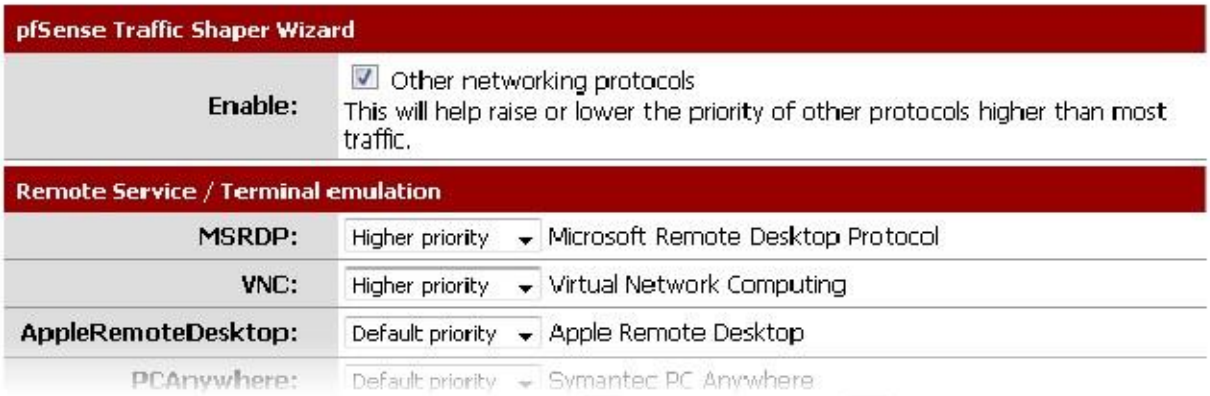
Subir o bajar Otras aplicaciones

La última pantalla de configuración del asistente shaper, se ve en la Figura 20.7, "Subir o Bajar Otros
Aplicaciones ", enumera muchas otras aplicaciones y protocolos comúnmente disponibles. ¿Cómo estos protocolos
se manejan dependerá del entorno que este router pfSense será proteger. Algunos de estos
puede que desear, y que otros no. Por ejemplo, en un entorno corporativo, es posible que desee bajar
la prioridad del tráfico no interactivo, como el correo, donde una desaceleración no es notado por nadie, y
aumentar la prioridad de los servicios interactivos como RDP, donde los malos resultados es un impedimento para la gente

capacidad para trabajar. En una casa, streaming multimedia puede ser más importante, y otros servicios puede ser rebajado. Active la opción para otros protocolos de red, y luego escoger y elegir de la lista.

Hay más de 25 protocolos para elegir, y cada uno se puede dar un Mayor prioridad,
Baja prioridad, o hacia la izquierda en el Prioridad por defecto. Si habilitó p2pCatchAll, lo harás
que desee utilizar esta pantalla para asegurarse de que estos otros protocolos son reconocidos y tratados normalmente, en lugar
que penalizado por la regla p2pCatchAll defecto.

Figura 20.7. Suba o baje Otras aplicaciones



Fin del Asistente de

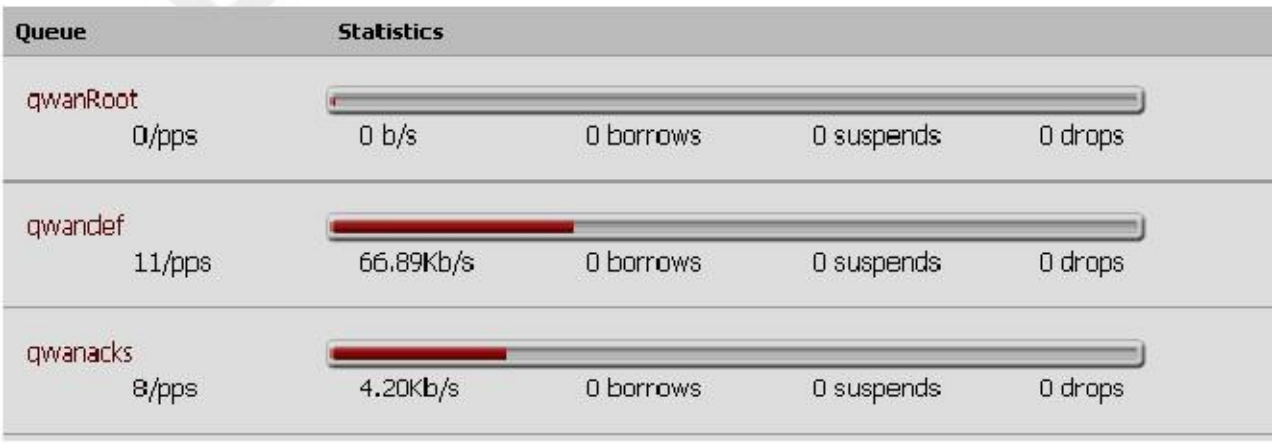
Todas las reglas y las colas se creará ahora, pero aún no está en uso. Al pulsar el botón Finalizar en la pantalla final, las normas se cargará y activa.

Shaping ahora debe estar activada para todas las nuevas conexiones. Debido a la naturaleza de estado del conformador, sólo
nuevas conexiones tendrán limitación de tráfico aplicada. Para que esto sea totalmente activa en todas las conexiones, debe borrar los estados. Para ello, visite Diagnóstico Unidos, haga clic en la pestaña Restaurar Unidos, Cheque Tabla de estado de Firewall, haga clic en Restablecer.

Monitoreo de las colas

Con el fin de estar seguros de que la modulación del tráfico está funcionando como es debido, puede ser controlado por la navegación a
Estado Colas. Como se puede ver en la Figura 20.8, "Basic WAN colas", esta pantalla mostrará cada cola de la lista por nombre, su uso actual, y algunas otras estadísticas relacionadas.

Figura 20.8. Básica WAN Colas



La barra gráfica muestra cómo "full" es una cola. La tasa de datos en la cola se muestra en tanto paquetes por segundo (pps) y bits por segundo (b / s). Pide prestado suceder cuando una cola vecina es

no está lleno y la capacidad es tomada de allí cuando sea necesario. Gotas ocurren cuando el tráfico en una cola es caído a favor del tráfico de mayor prioridad. Es normal ver a gotas, y esto no significa que una completa conexión se interrumpe, sólo un paquete. Por lo general, un lado de la conexión verá que un paquete fue olvidada y vuelva a enviar, a menudo ralentización en el proceso para evitar caídas futuras. El contador se suspende indica cuando una acción de retardo pasa. El contador suspende no se utiliza por el programador de conformación empleado por pfSense en 1.2.x, y probablemente debe ser cero.

Personalización avanzada

Después de utilizar el asistente de la talladora, es posible que las normas que genera no llegan a satisfacer sus necesidades. Usted
lo desea, puede dar forma a un servicio que no está controlada por el asistente, un juego que utiliza un puerto diferente, o puede haber otros servicios que necesitan limitada. Una vez que las reglas básicas han sido creadas por el asistente, se debería ser relativamente fácil de editar o copiar estas normas y crear otros personalizados propios.

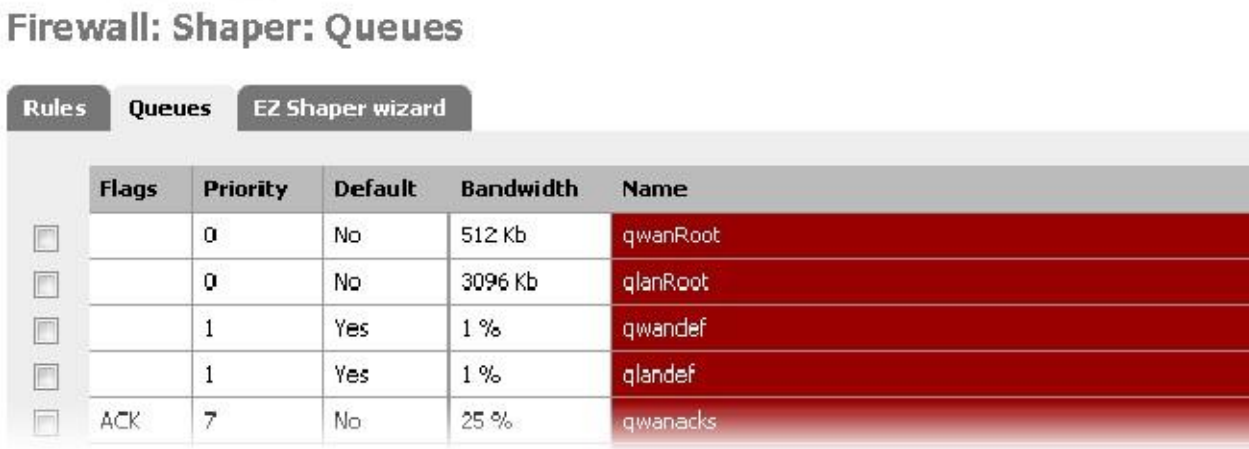
Edición de la talladora Colas

Como se mencionó en el resumen, las colas son donde el ancho de banda y las prioridades se asignan en realidad. Cada cola se le asigna una prioridad, 0-7. Cuando hay una sobrecarga de tráfico, el número más alto
Se prefieren las colas (por ejemplo, 7) sobre las colas de menor número (por ejemplo, 1). Cada cola se asigna ya sea un límite de ancho de banda de disco, o un porcentaje de la velocidad total del enlace. Las colas también se pueden asignar
otros atributos que controlan la forma en que se comportan, como el ser de bajo retardo, o tener cierta congestión algoritmos de evitación aplican. Las colas pueden ser cambiados por ir a Firewall Traffic Shaper, y
al hacer clic en la ficha Colas. Aparecerá una lista de reglas, como que en la Figura 20.9, "Traffic Shaper Colas Lista "

Edición de colas no es para los débiles de corazón. Puede ser una tarea compleja y con resultados de gran alcance, pero sin
conocimiento profundo de la configuración involucrados, lo mejor es seguir con las colas generadas por el asistente y alterar su configuración, en lugar de tratar de hacer otros nuevos desde cero.

Al ver la lista colas, cada cola se mostrará junto con las banderas asociados con el
cola, su prioridad, ancho de banda asignado, y el nombre. Para editar una cola haga clic Y para eliminar una cola clic . Usted no debe tratar de eliminar una cola si todavía está siendo referenciado por una regla. Para reordenar colas de la lista, seleccione la casilla junto a la cola para ser movido, y luego haga clic en el botón en la fila que debe estar por debajo de las colas reubicados. Al pasar el puntero del ratón por encima,
una gruesa barra aparecerá para indicar dónde se insertarán las reglas. El orden de las colas es estrictamente cosmética. Para añadir una nueva cola, haga clic en la parte inferior de la lista.

Figura 20.9. Tráfico lista Colas talladora



Al editar una cola, cada una de las opciones deben ser consideradas cuidadosamente. Si usted está buscando más información sobre estos valores que se menciona aquí, visite el PF paquetes de colas y Priorización

FAQ [http://www.openbsd.org/faq/pf/queueing.html] 0.1 El mejor programador disponible es jerárquica Curva Servicio Fair (HFSC), y que es el único disponible en pfSense 1.2.x.

El ajuste del ancho de banda debe ser una fracción del ancho de banda disponible en la cola de los padres, pero debe También puede definir con una conciencia de las otras colas vecinos. Cuando se utiliza porcentajes, el total de todas las colas bajo un padre determinado no puede superar el 100%. Al utilizar 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. Se prefieren las colas con números más altos cuando hay una sobrecarga, por lo que situar sus colas en consecuencia. Por ejemplo, el tráfico de VoIP debe ser de la más alta prioridad, por lo que se debe establecer en un tráfico de red 7. Peer-to-peer, que se puede retrasar en favor de otro protocolos, deben establecerse a 1.

El nombre de una cola debe tener entre 1-15 caracteres y no puede contener espacios. El más común convención es para iniciar el nombre de una cola con la letra "Q" de manera que se puede identificar con más facilidad en el conjunto de reglas.

Hay seis opciones diferentes de programador que se pueden establecer para una cola determinada:

• Cola predeterminada

  Selecciona esta cola como predeterminado, la que se encargará de todos los paquetes sin igual. Cada interfaz debe tener uno y la cola de un solo defecto.

• ACK / bajo retardo Queue (ACK)

  Al menos una cola por la interfaz debe tener este conjunto. Normalmente, esto se reserva para - como su nombre implica - paquetes ACK que deben ser tratadas de forma especial con una prioridad alta.

• Random Early Detection (RED)

  Un método para evitar la congestión en un enlace; intentará activamente para garantizar que la cola no consigue completo. Si el ancho de banda está por encima del máximo dado por la cola, se producirán gotas. También, gotas pueden
  ocurrir si el tamaño medio de la cola se acerca al máximo. Paquetes perdidos son elegidos al azar, por lo que el más ancho de banda en uso por una conexión determinada, lo más probable es ver gotas. El efecto neto es que el ancho de banda es limitado en una forma justa, fomentando un equilibrio. RED sólo se debe utilizar con Conexiones TCP desde TCP es capaz de manejar la pérdida de paquetes, y pueden volver a enviar cuando sea necesario.

• Detección temprana aleatoria de entrada y salida (RIO)

  Permite la RED con entrada / salida, lo que se traducirá en tener promedios de cola se mantienen y se comprueban en contra de los paquetes entrantes y salientes.

• Notificación explícita de congestión (ECN)

  Junto con RED, que permite el envío de mensajes de control que ACELERADOR conexiones si ambos termina el apoyo ECN. En lugar de dejar caer los paquetes como RED normalmente lo hacen, se sentará un indicador en
  el paquete que indica congestión de la red. Si el otro lado ve y obedece la bandera, la velocidad de la se reducirá la transferencia en curso.

• Se trata de una cola de padres

  Permite que esta cola para ser elegido como uno de los padres de otras colas.

La curva de Servicio (sc) es donde se puede ajustar con precisión los requisitos de ancho de banda para esta cola.

• m1

  Límite de ancho de banda Burstable

[1] http://www.openbsd.org/faq/pf/queueing.html y también está disponible en El PF de OpenBSD Packet Filter libro.

• d

Fecha límite para la explosión del ancho de banda, se especifica en milisegundos. (Por ejemplo, 1000 = 1 segundo)

• m2

Límite de ancho de banda normal

Por ejemplo, usted necesita el ancho de banda m1 dentro del tiempo d, pero un máximo normal de m2. Dentro de la inicial
tiempo fijado por d, m2 no está marcada, sólo m1. Después d ha expirado, si el tráfico está todavía por encima m2, lo hará
se forma. Por lo general, m1 y d se dejan en blanco, de modo que sólo se comprueba m2.
Cada uno de estos valores se puede fijar para los siguientes usos:

• Límite superior

Ancho de banda máximo permitido para la cola. Hará ancho de banda límites forzados. El parámetro M1 aquí también se puede utilizar para limitar la ruptura. En el plazo d no obtendrá más de ancho de banda m1.

• Tiempo real

Garantía de ancho de banda mínimo para la cola. Esto sólo es válido para los niños colas. El parámetro M1 siempre quedará satisfecho en plazo d, y m2 es el máximo que esta disciplina permitirá ser utilizado.

• Enlazar Compartir

La cuota de ancho de banda de una cola atrasados. Compartirá el ancho de banda entre las clases si el real Garantías de tiempo han sido satisfechas. Si se establece el valor de m2 para Link Compartir, prevalecerá la Configuración de ancho de banda para la cola. Estos dos valores son los mismos, pero si se ajustan ambas, Link Compartir de
se utiliza m2.

Mediante la combinación de estos factores, una cola obtendrá el ancho de banda especificado por los factores de tiempo real, además de
los de Enlace Compartir, hasta un máximo de límite superior. Se puede tomar un montón de prueba y error, y tal vez una gran cantidad de aritmética, pero puede valer la pena para asegurar que su tráfico se rige como mejor le parezca. Para más información sobre los valores m1, d, y m2 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 un niño de colas, seleccione la cola de Padres de la lista. Haga clic en Guardar para guardar la cola
ajustes y volver a la lista de la cola y, a continuación, haga clic en Aplicar cambios para volver a cargar las colas y activar la
cambios.

Edición de reglas de la talladora

Controlan las reglas de conformación de tráfico cómo se asigna el tráfico en las colas. Si un paquete coincide con un regulador de trafico
regla, se le asignará a la cola especificada por esa regla. Juego de paquetes se maneja de manera similar a las reglas del cortafuegos, pero con un poco de control de grano fino adicional. Para editar las reglas de la talladora, vaya a Firewall
 Traffic Shaper, y haga clic en la ficha Reglas. En esa pantalla, se muestra en la Figura 20.10, "Traffic Shaper Lista de reglas ", las normas existentes se mostrarán con la dirección de la interfaz, protocolo, origen, destino, colas de destino y el nombre.

En esta pantalla también se encuentra el control maestro para dar forma. Desmarque Habilitar regulador de trafico para desactivar el
regulador de trafico, a continuación, haga clic en Guardar. Para eliminar las reglas y las colas creadas por el regulador de trafico, y restablecer
el formador a los valores predeterminados, haga clic en Asistente para quitar. La próxima vez que visite Firewall
 Traffic Shaper,
el asistente se iniciará de nuevo.

Para editar una regla, haga clic en . Para eliminar una regla click en . Las reglas se pueden mover hacia arriba o hacia abajo una fila a la vez haciendo clic en para desplazarse hacia arriba o en para moverse hacia abajo. Para reordenar varias reglas en la lista, seleccione la casilla junto a las reglas que se deben mover y, a continuación, haga clic en el botón en la fila que debe ser

por debajo de las normas reubicados. Las reglas serán movidos encima de la fila seleccionada. Usted puede hacer una nueva regla basada en otra regla existente, haga clic en junto a la fila con la regla que le gustaría copia. Se le presentará la pantalla de edición de reglas pre-llenado con los detalles de la existente gobernar. Para agregar una nueva regla en en la parte inferior de la lista. blanco, haga clic en

Figura 20.10. Tráfico Lista de reglas de la talladora

Cada regla tiene varios criterios de coincidencia que ayudarán a asegurar que el tráfico adecuado se alimenta en la colas adecuadas. Antes de configurar las opciones a la altura, sin embargo, las colas de destino deben ser definidos. Usted debe establecer tanto una cola de salida y una cola de entrada. Los paquetes que coincidan con esta regla en el saliente dirección caerá en la cola de salida, y los paquetes que coinciden esta regla en la dirección entrante caerá en la cola de entrada. El camino del paquete se establece por la elección de una interfaz de entrada y salida de interfaz.

Ahora los criterios reales que coinciden comienzan. La mayoría de estas opciones le resultará familiar del firewall normas. Para más detalles sobre cómo configurar el protocolo, el Origen y Destino, referirse al Capítulo 10, Firewall. Por ahora nos centraremos en qué se debe establecer estos en lugar de la forma. Qué campos para configurar la voluntad dependerá de la trayectoria implícita en el In y Out Interfaces.

Por ejemplo, si el tráfico se origina a partir de una serie en la LAN, la interfaz debe ser en LAN, y la fuente se establece en la dirección o subred del host LAN. Si el tráfico se va a un lugar específico, establezca el destino en consecuencia, establezca lo contrario a Any. Para relacionar el tráfico de servicios específicos, debe establecer el rango de puerto de destino adecuada. En este ejemplo, para que coincida Tráfico HTTP, deje el conjunto del rango de puertos de origen a Any, y establecer el destino del rango de puertos para HTTP.
Rara vez es necesario establecer un puerto de origen, ya que suelen ser elegidos al azar.

El tráfico será igualada que entra y sale por defecto, pero se puede utilizar la opción de dirección para restringir este comportamiento. Recuerde, sin embargo, que esto se establece desde la perspectiva del firewall.

IP Tipo de Servicio (TOS) "bits de prioridad" se puede utilizar para capturar los paquetes que han sido etiquetados para un manejo especial. Hay tres opciones disponibles aquí, y cada uno de ellos puede tener uno de tres valores. Los tres campos indican una solicitud de baja demora, de alto rendimiento, o de alta fiabilidad. Para cada de estos, sí significa la bandera necesario establecer. No significa la bandera no debe establecer. No importa significa que se ser ignorado.

Un subconjunto de los indicadores TCP también puede ser igualada. Estos indican distintos estados de una conexión (o la falta de de los mismos). Ellos pueden coincidir sobre si o no se establecen explícitamente, borran, o sea (no les importa).

• SYN - Sincroniza los números de secuencia. Indica un nuevo intento de conexión.

• ACK - Indica aceptación de los datos. Como se señaló anteriormente, se trata de respuestas a dejar que el remitente conocer los datos se recibieron en Aceptar.

• FIN - Indica que no hay más datos del remitente, el cierre de una conexión.

• RST - Conexión restablecida. El flag está puesto al responder a una solicitud para abrir una conexión en un puerto que no tiene ningún demonio escucha. También se puede ajustar por el software de servidor de seguridad para alejarse indeseable conexiones.

• PSH - Indica que los datos deben ser empujados o lavarse, incluyendo los datos de este paquete, pasando Los datos hasta la aplicación.

• URG - Indica que el campo urgente es significativo, y este paquete se debe enviar antes de los datos que no es urgente.

El campo final, Descripción, es de texto libre y se utiliza para identificar a esta regla. Puede que le resulte útil para indicar aquí lo que la intención de la cola es (nombre de la aplicación o protocolo), así como la dirección de la regla se ajusta para que coincida.

Mediante la combinación de como muchos de estos parámetros según sea necesario, debería ser posible para que coincida con casi cualquier tráfico lo que tendría que hacer cola. Haga clic en Guardar para terminar y volver a la lista de reglas, haga clic en Aplicar cambios para recargar las normas y activarlos.

Solución de problemas de la talladora Cuestiones

Traffic Shaping / QoS es un tema complicado, y puede resultar difícil de hacerlo bien la primera vez. Hay algunos las trampas más comunes que las personas caen sobre, que están cubiertas en esta sección.

¿Por qué no es 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 están autorizados a declarar que portuarias otros deben utilizar para llegar a ellos, lo que significa el caos para administradores de red que intentan realizar el seguimiento del tráfico basado en el puerto solo. En 1.2.x, pfSense no tiene ninguna manera de examinar los paquetes para saber qué programa el tráfico parece ser, por lo que se ven obligados a depender de los puertos. Es por esto que puede ser un buena idea utilizar la regla P2P Cajón de Sastre, y / o hacer las reglas para cada tipo de tráfico que desea, y tratar su defecto cola de baja prioridad.

¿Por qué no es el tráfico a los puertos abiertos por UPnP correctamente cola?

El tráfico permitido en el daemon UPnP va a terminar en la cola predeterminada. Esto sucede porque el reglas generadas dinámicamente por el daemon UPnP no tienen ningún conocimiento de las colas a menos UPnP está configurado para enviar tráfico a una cola específica. Dependiendo de lo que usted ha utilizando UPnP en su medio ambiente, esto puede ser de bajo tráfico de prioridad como Bittorrent o tráfico de alta prioridad, como consolas de juegos o programas de chat de voz como Skype. La cola se puede ajustar por ir a Servicios UPnP y que entra un nombre de cola en el campo Traffic Shaper Queue.

¿Cómo puedo calcular la cantidad de ancho de banda para asignar a las colas de ACK?

Este es un tema complejo, y la mayoría de la gente disimula y acaba de adivinar un valor suficientemente alto. Para explicaciones más detalladas con fórmulas matemáticas, revise la sección Traffic Shaping de la foros pfSense [http://forum.pfsense.org/index.php/board, 26.0.html] 0.2 Hay un mensaje pegajoso en que

[2] http://forum.pfsense.org/index.php/board, 26.0.html

bordo de la cual se describe el proceso con gran detalle, y también hay una hoja de cálculo descargable que se puede utilizar para ayudar a facilitar el proceso.

¿Por qué es <x> no la forma adecuada?

Al igual que con otras preguntas de esta sección, esto tiende a suceder debido a las reglas entraron ya sea internamente o por otros paquetes que no tienen conocimiento de las colas. Dado que no se especifica ninguna cola para una regla, termina en el valor predeterminado o cola matriz, y no en forma. Puede que tenga que desactivar la WebGUI / ssh reglas anti-bloqueo y tal vez incluso reemplazar el predeterminado LAN # CUALQUIER regla de firewall con más específica
opciones. En el caso de los paquetes, es posible que necesite ajustar la forma en que se maneja su cola predeterminada.

Capítulo 21. Equilibrio de carga del servidor

Hay dos tipos de funcionalidad de balanceo de carga están disponibles en pfSense: Gateway y Server. Entrada balanceo de carga permite la distribución del tráfico de Internet enlazados a través de múltiples conexiones WAN. Para más información sobre este tipo de equilibrio de carga, consulte el Capítulo 15, Múltiples conexiones WAN. Servidor equilibrio de carga permite distribuir el tráfico a múltiples servidores internos para la distribución de la carga y redundancia, y es el tema de este capítulo.

Equilibrio de carga del servidor le permite distribuir el tráfico entre varios servidores internos. Es más comúnmente se utiliza con los servidores web y los servidores SMTP, aunque puede ser utilizado para cualquier servicio que utilice TCP.

Mientras pfSense ha reemplazado gama alta, balanceadores de carga comerciales de alto costo incluidos BigIP, Cisco LocalDirector, y más en entornos de producción graves, pfSense 1.2.x no es tan poderosa y flexible como estas soluciones. No es adecuado para las implementaciones que deben controlarse flexible y configuración de equilibrio. Para la supervisión de TCP, simplemente comprueba que el puerto TCP especificado está abierto. En el caso de un servidor web, el servidor no puede devolver cualquier respuestas HTTP, o los no válidos, y no hay manera de determinar esto. Para implementaciones grandes o complejos, que comúnmente se desea un mayor solución de gran alcance. Sin embargo, para las necesidades básicas, la funcionalidad disponible en pfSense se adapte a un sinnúmero de sitios muy bien.

Actualmente estamos revisando opciones para un equilibrador de carga más capaz para la versión 2.0.

Explicación de las opciones de configuración

Hay dos partes de la configuración para el equilibrador de carga del servidor. Piscinas de servidor virtual definen el lista de los servidores que se utilizarán, qué puerto se escuchan en, y el método de seguimiento aplicable. Virtual Servidores definen la IP y el puerto para escuchar en, y la piscina adecuada para dirigir el tráfico de entrada a la que IP y el puerto.

Piscinas de servidor virtual

Para configurar grupos de servidores virtuales, vaya a Servicios Equilibrador de carga. Clic para agregar una nueva piscina. Cada una de las opciones de esta página se discute aquí.

- Nombre - Introduzca un nombre para el grupo aquí. El nombre es cómo se hace referencia a la piscina más tarde cuando configurar el servidor virtual que utilizará esta piscina.

- Descripción - Opcionalmente ingrese una descripción más larga de la piscina aquí.

- Tipo - Esto debe de forma predeterminada 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 Failover utilizar siempre el primer servidor de la piscina a menos que falle, a continuación, caer de nuevo a la posterior 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 de servidor virtual.

- Monitor - Define el tipo de monitor que se utiliza, que es cómo determina el balanceador si el servidores están en marcha. Selección TCP hará que el equilibrador de conectar con el puerto definido previamente en el puerto, y si no puede conectarse a ese puerto, el servidor se considera baja. Elegir ICMP en su lugar monitorizar los servidores definidos haciendo ping a ellos, y les marcará hacia abajo si no responden a pings.

- IP Monitor - Este campo no es aplicable con el balanceador de carga del servidor y aparece en color gris.

- Dirección IP del servidor - Aquí es donde usted complete la dirección IP interna de los servidores del grupo. Introduzca uno a la vez, hacer clic en Agregar a la piscina después.

• Lista - Este campo muestra la lista de servidores que ha añadido a esta piscina. Puede eliminar un servidor de la agrupación, haga clic en la dirección IP y haga clic en Eliminar de la piscina.

Después de rellenar todos los campos como se desee, haga clic en Guardar. Continuar con la configuración del servidor virtual para este
piscina haciendo clic en la ficha Servidores Virtuales.

Servidores Virtuales

Servidores virtuales es donde se define la IP y el puerto para escuchar en para reenviar el tráfico a la anteriormente piscina configurado. Clic  para agregar un nuevo servidor virtual. Cada una de las opciones de esta página se discute a continuación.

• Nombre - Introduzca un nombre para el servidor virtual aquí. Esto es simplemente para su referencia.

• Descripción - Opcionalmente, introduzca una descripción más larga para el servidor virtual aquí. Esto también es sólo para
con fines de referencia.

• Dirección IP - Aquí es donde se introduce la dirección IP que el servidor virtual se escucha. Es por lo general su IP WAN o una IP virtual en WAN. Debe ser una dirección IP estática. Puede utilizar un CARP VIP aquí para una alta disponibilidad de configuración del equilibrador de carga. Para obtener más información sobre la alta disponibilidad y
CARPA VIP, consulte el Capítulo 24, Firewall de redundancia / alta disponibilidad.

• Puerto - Este es el puerto que el servidor virtual escuchar. Puede ser diferente del puerto sus servidores se escucha en el interior.

• Piscina Servidor Virtual - Aquí es donde se selecciona el grupo configurado previamente. Las conexiones a la dirección IP y el puerto definido en esta pantalla serán dirigidos a las direcciones IP y puertos configurados en la piscina.

• Servidor piscina Down - Este es el servidor que los clientes se dirigen a si todos los servidores de la piscina han bajado. Debe escribir algo aquí. Si usted no tiene un servidor alternativo para enviar solicitudes a, usted puede poner una de las IPs de sus servidores en la piscina aquí, aunque el resultado será inaccesible si todos los servidores del grupo se han reducido.

Después de rellenar los campos correctamente, haga clic en Enviar, luego en Aplicar cambios.

Las reglas de 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 cortafuegos deben permitir el tráfico a las direcciones IP privadas internas de los servidores, así como el puerto que
se escucha en el interior. Debe crear un alias para los servidores de la piscina, y crear un solo
regla de firewall en la interfaz donde el tráfico destinado a la piscina se iniciará (generalmente WAN) permitiendo que la fuente apropiada (por lo general hay) al destino de los alias creados para la piscina. Una específica ejemplo de esto se proporciona en la sección llamada "Configuración de reglas del cortafuegos". Para obtener más información
en las reglas del cortafuegos, consulte el Capítulo 10, Firewall.

Conexiones Sticky

Hay una opción de configuración adicional disponible para el equilibrio de carga del servidor, en el marco del Sistema de
Menú Avanzado. Bajo el equilibrio de carga, encontrará Usar conexiones adhesivas. Al marcar esta casilla, garantizar a los clientes con una conexión activa a la piscina están siempre dirigidos al mismo servidor para cualquier las conexiones posteriores. Una vez que el cliente cierra todas las conexiones activas y los tiempos de estado cerradas por fuera,
la conexión pegajosa se pierde. Esto puede ser deseable para algunas configuraciones de equilibrio de carga web donde peticiones de un cliente en particular sólo deben ir a un solo servidor, para la sesión o por otras razones. Tenga en cuenta este
no es perfecto, como si el navegador web del cliente cierra todas las conexiones TCP con el servidor después de cargar un
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. Generalmente esto no es un problema ya que la mayoría de los navegadores web no se cerrarán de inmediato una
conexión y el estado existe el tiempo suficiente para no convertirlo en un problema, pero si usted es estrictamente dependiente

en un cliente específico nunca conseguir un servidor diferente en la piscina sin importar cuánto tiempo se encuentra el navegador
hay inactiva, debe buscar una solución de equilibrio de carga diferente.

La carga del servidor Web Equilibrio Ejemplo Configuración

Esta sección le muestra cómo configurar el equilibrador de carga de principio a fin por un servidor web en dos cargar entorno equilibrado.

Entorno de red Ejemplo

Figura 21.1. Carga del servidor de equilibrio de red de ejemplo

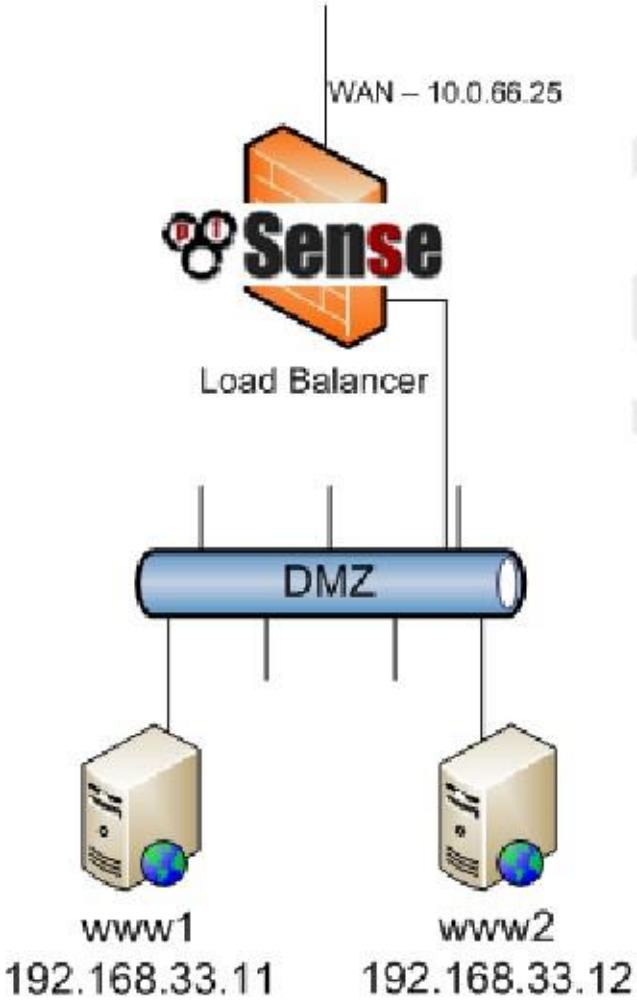


Figura 21.1, "Carga del servidor de equilibrio Ejemplo de red" muestra el entorno de ejemplo configurado
en esta sección. Se compone de un único servidor de seguridad, utilizando su IP WAN para la piscina, con dos servidores web
en un segmento de DMZ.

Configuración de la piscina

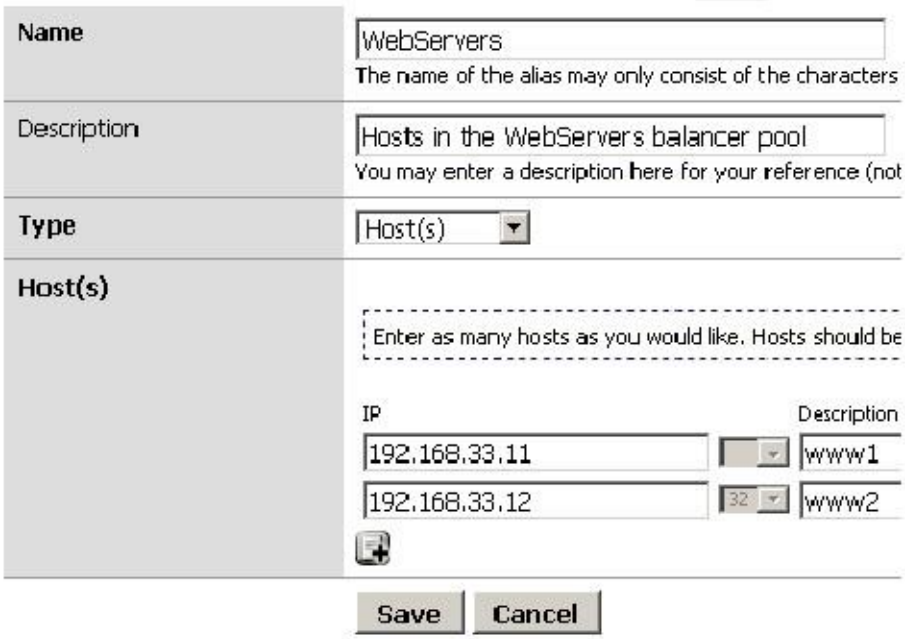
Para configurar el grupo, vaya a Servicios Equilibrador de carga y haga clic. Figura 21.2, "Pool configuración "muestra la configuración del grupo de equilibrio de carga para los dos servidores web, utilizando una red TCP
supervisar. Después de rellenar todos los campos correctamente, haga clic en Guardar.

Configuración de servidor virtual

Volver a la pantalla de la piscina de equilibrador de carga, haga clic en la ficha Servidores Virtuales y haga clic para añadir una nueva virtuales
servidor. Figura 21.3, "Configuración del servidor virtual" muestra la configuración de servidor virtual para escuchar en la IP WAN (10.0.66.25) en el puerto 80 y enviar el tráfico en esa IP y puerto para los servidores definidos
en el Servidores web piscina. Para el grupo de servidores de Down, esta configuración utiliza una de las IPs de la los servidores de la Servidores web piscina por falta de otra opción. En este caso, si ambos de la piscina
servidores están inactivos, el servidor virtual es inaccesible. Después de rellenar los campos aquí, haga clic en Enviar, entonces
Aplicar cambios.

Configuración de reglas de firewall

Figura 21.4. Alias para servidores web



Ahora las reglas del cortafuegos deben estar configurados para permitir el acceso a los servidores del grupo. Las reglas deben permitir
el tráfico a las direcciones IP internas y el puerto que se utiliza, y no hay reglas son necesarias para el exterior Dirección IP y el puerto utilizado en la configuración del servidor virtual. Es preferible utilizar un alias que contiene todos los servidores del grupo, por lo que el acceso se puede permitir que con una sola regla de firewall. Vaya a Cortafuego □
Alias y haga clic en añadir un alias. Figura 21.4, "Alias" para servidores web muestra los alias utilizados para este Ejemplo de configuración, que contiene los dos servidores web.

Haga clic en Guardar después de introducir el alias, y aplicar los cambios. Luego vaya a Firewall □ Reglas y en el

ficha de la interfaz donde el tráfico de los clientes se pondrá en marcha (WAN en este caso), haga clic en. Figura 21.5, "Adición de reglas de firewall para los servidores web" muestra un fragmento de la regla de firewall añadido para esta configuración.
Las opciones que no se muestran se dejaron a sus valores por defecto, a un lado de la descripción.

Figura 21.5. Adición de reglas de firewall para servidores web

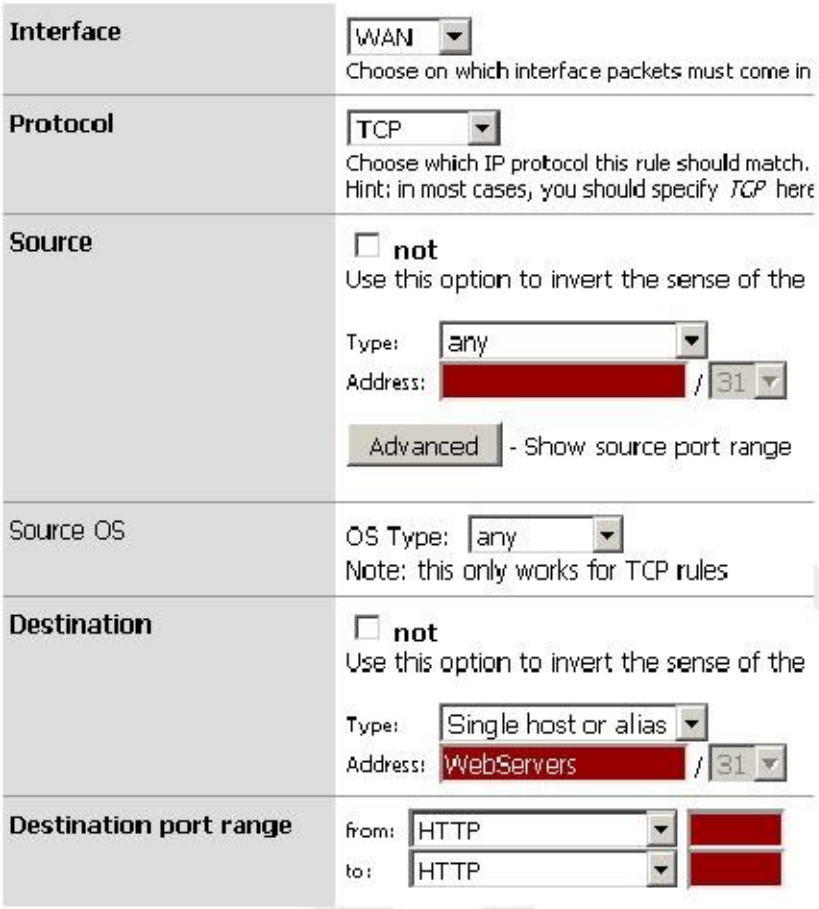


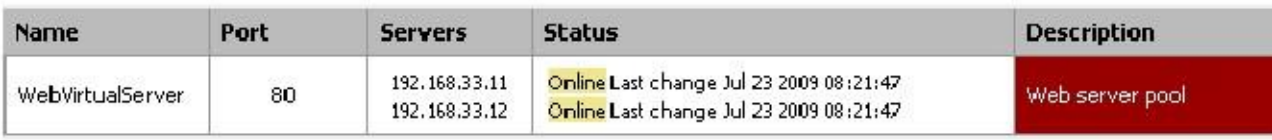
Figura 21.6, "regla de firewall para servidores web" muestra el estado después de que se añadió.

Figura 21.6. Regla de firewall para servidores web

Visualización del estado del equilibrador de carga

Ahora que el equilibrador de carga está configurado, al ver su estado, vaya a Estado Equilibrador de carga y haga clic en la ficha Servidores Virtuales. Aquí podrás ver el estado de cada servidor del grupo (como se muestra en Figura 21.7, "Estado del servidor virtual"). Si el estado ha cambiado a la línea en los últimos cinco minutos, ya que después de empezar a configurar el equilibrador de carga, verá "Online" está resaltado en un color amarillento de color. Después de cinco minutos han pasado, el estado cambiará a verde.

Figura 21.7. Estado del servidor virtual



Si detiene el servicio de servidor web en uno de los servidores o toma el servidor fuera de la red por completo si utilizando monitores ICMP, verá la actualización de estado de conexión y el servidor se eliminará de la piscina.

Balanceo de carga Verificación

Para comprobar el equilibrio de carga, rizarse es la mejor opción para garantizar la caché del navegador web y persistente conexiones no afectan a los resultados de sus exámenes. rizarse está disponible para todos los sistemas operativos imaginable y posible
puede descargar desde el sitio web de rizo [http://curl.haxx.se]. Para usarlo, simplemente ejecute rizo http://mysite sustitución misitio ya sea con la dirección IP o nombre de host de su sitio. Debe hacerlo desde fuera
su red. A continuación se ilustra un ejemplo de la prueba con rizarse desde el lado WAN.

#rizo http://10.0.66.25
```
<html>


<head>
<title> 0.12 </ title>
</ Head>


<body>

<p> 192.168.33.12 - Server 2 </ p>


</ Body>
</ Html>
```

Al probar inicialmente el equilibrio de carga, tendrá que configurar cada servidor para devolver una página especificando su nombre de host, dirección IP, o ambos, para que sepa qué servidor usted está golpeando. Si lo hace no han permitido que las conexiones adhesivas, obtendrá un servidor diferente cada vez que solicita una página con rizarse (Con la excepción de el escenario descrito en la sección denominada "equilibrio desigual").

Equilibrio de carga de solución de problemas del servidor

En esta sección se describen los problemas más comunes que encuentran los usuarios con el equilibrio de carga del servidor, y cómo
solucionarlos.

Las conexiones no están equilibradas

Las conexiones no están equilibrados es casi siempre un fracaso de la metodología de prueba que se utiliza, y es por lo general específico a HTTP. Navegadores Web comúnmente mantendrán las conexiones a un servidor web abiertas,
y golpeando refresco solo re-utiliza la conexión existente. Una única conexión nunca se cambiará a otro servidor equilibrada. Otro problema común es el caché de su navegador web, en el que el navegador nunca pide en realidad la página de nuevo. Es preferible utilizar una herramienta de línea de comandos como rizarse para las pruebas de esta naturaleza, ya que asegura que nunca se ve afectada por los problemas inherentes a la prueba con los navegadores web - no tiene caché, y se abre una nueva conexión al servidor cada vez que se ejecuta. Más información sobre rizarse se pueden encontrar en la sección llamada "Verificación de equilibrio de carga."

Si está utilizando las conexiones adhesivas, asegúrese que está probando desde múltiples direcciones IP de origen. Las pruebas de un
IP única fuente siempre irá a un único servidor a menos que esperar largos tiempos entre conexiones.

Equilibrio desigual

Debido a la forma en que las funciones de software subyacentes, en ambientes de poca carga, el equilibrio será desigual. El subyacente SLBD servicio de monitoreo restablece su anclaje pf en cada intervalo de supervisión, que es cada 5 segundos. Esto significa que cada 5 segundos, la próxima conexión irá al primer servidor de la piscina. Con los servicios de muy baja carga en la que con frecuencia tiene una conexión o menos cada 5 segundos, verá muy poco balanceo de carga. Usted todavía tiene capacidades de failover completo si uno de los servidores fallar. Este problema realmente resuelve en sí, aunque, como cuando la carga aumenta hasta el punto en el equilibrio la carga es importante, será equilibrado por igual. En entornos de producción que emplean a miles de paquetes por segundo, el equilibrio es igual en todos los servidores.

Servidor de Down no marcados como fuera de línea

Si un servidor se cae, pero no está marcado como sin conexión, es porque desde la perspectiva de la supervisión que pfSense está haciendo, no es realmente abajo. Si utiliza un monitor de TCP, que el puerto TCP está aceptando conexiones. El servicio en ese puerto podría romperse de muchas maneras y aún responder TCP conexiones. Para los monitores de ICMP, este problema se agrava, ya que los servidores se pueden colgar sin escuchar servicios a todos y todavía responden a los pings.

Servidor Live no marcado como línea

Si el servidor está en línea, pero no marcado como en línea, es porque no está en línea desde el punto de vista de la firewall. El servidor debe responder en el puerto TCP utilizado o responder a los pings provenientes de la interfaz IP de la interfaz de servidor de seguridad más cercano al servidor. Por ejemplo, si el servidor se encuentra en la LAN, el servidor
debe responder a las peticiones iniciadas desde LAN IP del servidor de seguridad. Para verificar esto para monitores ICMP, vaya Diagnósticos Ping y ping a la IP del servidor mediante la interfaz donde se encuentra el servidor. Para TCP monitores, inicie sesión en el servidor de seguridad a través de SSH, o en la consola, y escoge la opción de menú de la consola 8. Al
símbolo del sistema, intente telnet al puerto que el servidor debe estar escuchando en. Por ejemplo, para probar una red servidor en el ejemplo anterior de este capítulo, debe ejecutar telnet 192.168.33.11 80.

Una conexión fallida se sentará allí por un tiempo tratando de conectar, mientras que una conexión con éxito se conectar inmediatamente. El siguiente es un ejemplo de una conexión fallida.

```
#telnet 192.168.33.12 80
Tratando 192.168.33.12 ...
telnet: connect para abordar 192.168.33.12: Operation timed out
telnet: No se puede conectar al host remoto
```

Y he aquí un ejemplo de una conexión exitosa.

```
#telnet 192.168.33.12 80
Tratando 192.168.33.12 ...
Conectado a 192.168.33.12.
Carácter de escape es '^]'.
```

Usted encontrará probablemente que la conexión falla, y tendrá que resolver otros problemas en el servidor.

Capítulo 22. Inalámbrico

pfSense incluye construido en capacidades inalámbricas que le permiten convertir su pfSense instalar en un punto de acceso inalámbrico, utilice una conexión inalámbrica 802.11 como una conexión WAN o ambos. En este capítulo se incluye también los medios sugeridos de forma segura con capacidad inalámbrica externa puntos de acceso, y de cómo implementar con seguridad un punto de acceso inalámbrico. Cobertura en profundidad de 802.11 es fuera del alcance de este libro. Para aquellos que buscan esa información, le recomiendo el libro 802.11 Wireless Networks: The Definitive Guide [Http://www.amazon.com/gp/product/0596100523?ie = UTF8 & tag = pfSense-20 y linkCode = as2 y campo = 1,789 y = 9,325 y creativa creativeASIN = 0596100523].

Hardware inalámbrico recomendados

Hay una variedad de tarjetas inalámbricas soportadas en FreeBSD 7.2, y pfSense incluye soporte para todos los tarjeta compatible con FreeBSD. Algunos se apoyan mejor que otros. La mayoría de los desarrolladores de pfSense trabajan con el hardware de Atheros, por lo que tiende a ser el hardware más recomendado. Muchos tienen éxito con otras cartas, así, y Ralink es otra opción popular. Otras tarjetas pueden ser compatibles, pero no apoyar todas las funciones disponibles. En particular, algunas tarjetas de Intel se pueden utilizar en el modo de infraestructura, pero no se puede ejecutar en el modo de punto de acceso debido a las limitaciones del hardware en sí.

Las tarjetas inalámbricas de grandes proveedores de nombres

Linksys, D-Link, Netgear y otros grandes fabricantes comúnmente cambian los chipsets utilizados en su tarjetas inalámbricas sin necesidad de cambiar el número de modelo. No hay manera de asegurar un modelo de tarjeta específica a partir de estos vendedores serán compatibles porque no tienes forma de saber qué tarjeta de "menor" revisión que va a terminar con. Mientras una revisión de un modelo en particular puede ser compatible y el trabajo así, otra carta del mismo modelo puede ser incompatible. Por esta razón, se recomienda evitar cartas de los principales fabricantes. Si ya tienes uno, vale la pena intentarlo para ver si es compatible, pero ten cuidado si usted compra uno, porque el modelo de "igual" trabajó para otra persona, usted puede terminar con una pieza completamente diferente de hardware que no es compatible.

Controladores inalámbricos incluidos en 1.2.3

En esta sección se enumeran los controladores inalámbricos incluidas en pfSense 1.2.3, y los chipsets que son compatibles con los conductores (tirando de las páginas del manual de FreeBSD para los controladores). Los conductores en FreeBSD son referidos por su nombre conductor, seguido de (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 frecuencia de uso con pfSense, sobre la base de la lista de correo y el foro de anuncios desde el inicio del proyecto.

Para obtener información más detallada sobre las tarjetas admitidas, y la información más actualizada, consulte la pfSense wiki [http://doc.pfsense.org/index.php/Supported_Wireless_Cards].

ath (4)

Soporta tarjetas basadas en el Atheros AR5210, AR5211 y AR5212 chipsets.

ral (4)

Ralink Technology IEEE 802.11 controlador de red inalámbrica - soporta tarjetas basadas en el Ralink Tecnología RT2500, RT2501 y RT2600 chipsets.

wi (4)

Lucent Hermes, Intersil PRISM y Spectrum24 IEEE 802.11 conductor - soporta tarjetas basadas en Lucent Hermes, Intersil PRISM-II, Intersil PRISM-2.5, Intersil Prism-3, y Symbol Spectrum24 chipsets. Estas tarjetas sólo soportan 802.11b.

awi (4)

AMD PCnetMobile IEEE 802.11 PCMCIA controlador de red inalámbrica - soporta tarjetas basadas en el Controlador AMD 79c930 con Intersil (anteriormente Harris) PRISM chipset de radio.

una (4)

Aironet Comunicaciones 4500/4800 controlador de adaptador de red inalámbrica - apoya Aironet Comunicaciones 4500 y 4800 adaptadores de red inalámbrica y variantes.

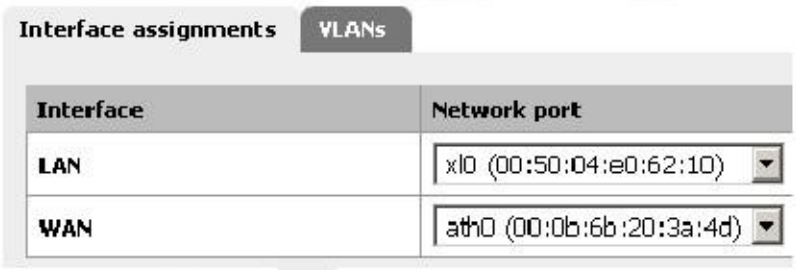
WAN inalámbrica

Puede asignar la tarjeta inalámbrica como su interfaz WAN, o un WAN OPT en un multi-WAN despliegue. Esta sección trata de asignar y configurar una interfaz inalámbrica como una interfaz WAN.

Asignación de interfaz

Si aún no lo ha asignado a su interfaz inalámbrica, vaya a Interfaces Asignar. Haga clic en Agregar añadir una interfaz OPT para su red inalámbrica, o seleccionarlo como WAN, si se desea. Figura 22.1, "Interface asignación - WAN inalámbrica "muestra una tarjeta Atheros asignado como WAN.

Figura 22.1. Asignación Interface - WAN inalámbrica



Configuración de la red inalámbrica

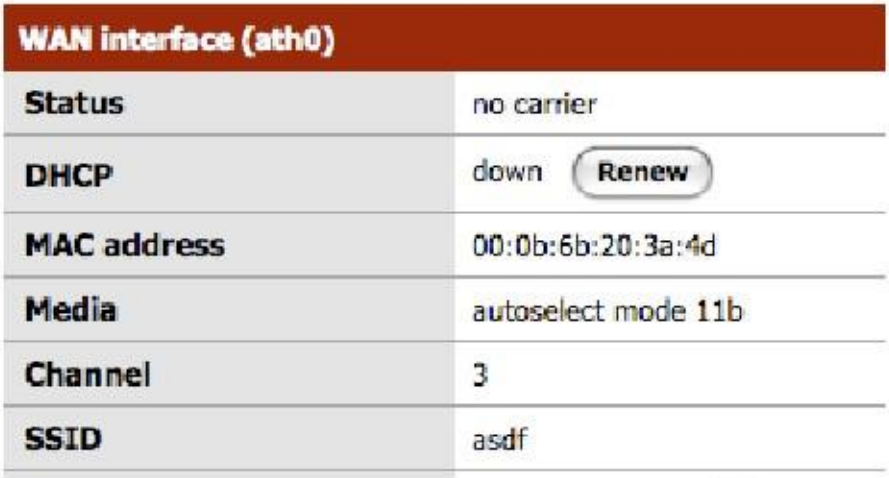
Navegue hasta el menú Interfaces para su interfaz inalámbrica WAN. En este ejemplo se utiliza WAN, así que voy a busque Interfaces WAN. Seleccione el tipo de configuración (DHCP, IP estática, etc) y de desplazamiento abajo bajo Configuración inalámbrica. Elija el modo Infraestructura (BSS), rellenar el SSID y configurar encriptación como WEP (Wired Equivalent Privacy) y WPA (Wi-Fi Protected Access) si se utiliza. Más redes inalámbricas no necesitan ninguna configuración adicional, pero si el suyo lo hace, asegúrese de que está configurado
Asignar para el punto de acceso que se va a utilizar. Luego haga clic en Guardar.

Comprobar el estado inalámbrico

Vaya a Estado Interfaces para ver el estado de la interfaz inalámbrica se acaba de configurar. Usted puede saber si la interfaz ha asociado con éxito con el punto de acceso elegido por mirando a la estado de la interfaz. Estado asociado significa que está conectado con éxito, como se muestra en la Figura 22.2, "Wireless WAN Asociado".

Si aparece No hay portadora, no estaba en condiciones de asociarse. Figura 22.3, "No portadora de WAN inalámbrica" espectáculos
un ejemplo de ello, donde configurado SSID asdf, una red inalámbrica que no existe.

Figura 22.3. No portadora de WAN inalámbrica



Mostrando las redes y de la señal inalámbrica disponible fuerza

Al navegar a Estado Wireless, se puede ver las redes inalámbricas visibles para el servidor de seguridad, como se muestra
En la Figura 22.4, "Estado inalámbrico". Su interfaz inalámbrica debe configurarse antes de este elemento de menú aparecerá.

Figura 22.4. Estado inalámbrico

Bridging e inalámbrico

Sólo las interfaces inalámbricas en una de las modalidades (hostap) acceso funcionarán en una configuración de puente. Usted
puede tender un puente sobre una interfaz inalámbrica en hostap a cualquier otra interfaz para combinar las dos interfaces en los
mismo dominio de difusión. Es posible que desee hacer esto si tiene dispositivos o aplicaciones que deben residir en el mismo dominio de difusión para funcionar correctamente. Esto se discute con más detalle en la sección "Escogiendo bridging o routing".

BSS y IBSS inalámbrico y puenteo

Debido a la forma en que funciona inalámbricos en BSS (Basic Service Set) y IBSS (Independent Basic Service Establezca) modo y la forma en la reducción de las obras, no se puede superar una interfaz inalámbrica en BSS o IBSS modo. Cada dispositivo conectado a una tarjeta de red inalámbrica en modo BSS o IBSS debe presentar la misma Dirección MAC. Con puente, la dirección MAC se pasa es la MAC real del dispositivo conectado.
Esto es normalmente deseable - es sólo la forma en la reducción de las obras. Con la tecnología inalámbrica, la única forma en que este

función se puede si todos los dispositivos detrás de esa tarjeta inalámbrica presentan la misma dirección MAC en la red inalámbrica. Esto se explica en profundidad por expertos inalámbrico señalado Jim Thompson en una lista de correo mensaje [http://lists.freebsd.org/pipermail/freebsd-current/2005-October/056977.html] 0.1 Como un ejemplo, cuando VMware Player, Workstation, o el servidor está configurado para salvar a una interfaz inalámbrica, traduce automáticamente la dirección MAC a la de la tarjeta inalámbrica. Debido a que no hay manera de simplemente traducir una dirección MAC en FreeBSD, y debido a la forma de puente en FreeBSD funciona, es difícil proporcionar soluciones provisionales similares a las que ofrece VMware. En algún punto puede pfSense apoyar esto, pero no está en la hoja de ruta para la 2.0.

El uso de un punto de acceso externo

Si usted tiene un punto de acceso inalámbrico existente, o un enrutador inalámbrico que desea utilizar sólo como un acceso
señalan ahora que pfSense está actuando como el servidor de seguridad, hay varias maneras de acomodar inalámbrico en su red. Esta sección cubre los escenarios más comúnmente utilizados.

En cuanto a su router inalámbrico en un punto de acceso

Al sustituir un router inalámbrico simple, como un Linksys o D-Link u otro dispositivo de casa de grado con pfSense como un servidor de seguridad perimetral, la funcionalidad inalámbrica puede ser retenido girando el inalámbrica
router en un punto de acceso inalámbrico, siguiendo los pasos descritos en esta sección. Estos son genéricos pasos que deben seguirse para cualquier dispositivo. Para conocer detalles de su router inalámbrico, consulte a su documentación.

Deshabilitar el servidor DHCP

En primer lugar tendrá que desactivar el servidor DHCP si estaba previamente en uso. Usted tendrá que pfSense para manejar esta función para la red, y que tiene dos servidores DHCP de la red hará que problemas.

Cambie la IP LAN

A continuación, tendrá que cambiar la IP LAN a una dirección IP no utilizada en la subred donde su punto de acceso residirá (comúnmente LAN). Probablemente está utilizando la misma IP que asignará a la LAN pfSense interfaz, por lo que requerirá una dirección diferente. Usted tendrá que mantener un IP funcional en el acceso señale a efectos de gestión.

Conecte la interfaz LAN

La mayoría de los routers inalámbricos cerrar la inalámbrica en el puerto LAN interno o puertos. Esto significa que el inalámbrica
estará en el mismo dominio de broadcast y la subred IP que los puertos alámbricos. Para los routers con un sistema integrado de
cambiar, cualquiera de los puertos del switch se suele trabajar. Usted no quiere que conecte el puerto WAN o Internet en el router! Esto pondrá a su red inalámbrica en un dominio de difusión diferente del resto de su red, y dará lugar a tráfico NATing entre su red inalámbrica y LAN y doble NATing el tráfico entre su red inalámbrica e Internet. Este es un diseño feo, y dará lugar a problemas en algunas circunstancias, especialmente si necesitan comunicarse entre los clientes inalámbricos y su LAN cableada.

Cuando se conecte a la interfaz LAN dependerá de su diseño de red elegida. El próximo secciones cubren sus opciones y sus consideraciones en los que elegir.

Bridging inalámbrico a su LAN

Uno de los medios comunes de despliegue inalámbrico es conectar el punto de acceso directamente en el mismo interruptor que
sus equipos de una LAN, donde la AP Puentes de los clientes inalámbricos a la red por cable. Esto funciona muy bien, pero ofrece un control limitado sobre la capacidad de los clientes inalámbricos para comunicarse con sus sistemas internos.

[1] http://lists.freebsd.org/pipermail/freebsd-current/2005-October/0 56977.html

Tender un puente inalámbrico para una interfaz OPT

Si desea más control sobre sus clientes inalámbricos, añadiendo una interfaz OPT para pfSense para su punto de acceso es la solución preferida. Si desea mantener sus redes inalámbricas y por cable en el misma subred IP y dominio de difusión, se puede cerrar la interfaz OPT a la interfaz LAN. Este escenario es funcionalmente equivalente a enchufar el punto de acceso directamente en su switch LAN, excepto desde pfSense está en el medio, puede filtrar el tráfico de la red inalámbrica para proporcionar una protección a sus equipos de una LAN.

También puede poner su red inalámbrica en una subred IP dedicada, si lo desea, al no superar la OPT interfaz en pfSense y asignándole a una subred IP fuera de la subred LAN. Esto permite enrutamiento entre sus redes internas e inalámbricas, según lo permitido por su conjunto de reglas de firewall. Es comúnmente se hace en las redes más grandes, donde los puntos de acceso múltiple son conectados a una central que sea a continuación, se conecta a la interfaz OPT en pfSense. También es preferible cuando se le obligue a su wireless clientes para conectarse a una VPN antes de permitir conexiones a los recursos de la red interna.

La elección de puente o encaminamiento

La elección entre el puente (utilizando la misma subred IP que la red LAN) o encaminamiento (usando una IP dedicada subred inalámbrica) para sus clientes inalámbricos dependerá de qué servicios requieren los clientes inalámbricos. Ciertas aplicaciones y dispositivos se basan en las emisiones para funcionar. AirTunes de Apple, como un ejemplo, no funcionará a través de dos dominios de difusión, por lo que si usted tiene AirTunes en su red inalámbrica y quieren usarlo desde un sistema en su red cableada, debe superar sus redes cableadas e inalámbricas.
Otro ejemplo es los servidores de medios utilizados por dispositivos como Xbox 360 y Playstation 3. Estos se basan en difusión o multidifusión de tráfico que sólo puede funcionar si se puentean sus redes cableadas e inalámbricas.
En muchos entornos de red doméstica que tendrá aplicaciones o dispositivos que requieren su cable y redes inalámbricas para puentear. En la mayoría de las redes corporativas, no hay aplicaciones que requerirá reducir. Cuál elegir depende de los requisitos de las aplicaciones de red que utiliza, como así como sus preferencias personales.

Hay algunos compromisos a esto, un ejemplo es el paquete de Avahi. Se puede escuchar en dos diferentes dominios de difusión y los mensajes de retransmisión de una a la otra con el fin de permitir multidifusión DNS para trabajar (también conocido como Rendezvous o Bonjour) para el descubrimiento y los servicios de red. Tener un WINS
Servidor (Windows Internet Name Service) es otro ejemplo, ya que le permitirá navegar por redes de / máquinas de SMB de Windows, incluso cuando usted no está en el mismo dominio de difusión.

pfSense como punto de acceso

Con una tarjeta inalámbrica que soporte el modo hostap (ath (4), `ral (4)` y `wi (4))`, pfSense puede ser se configura como un punto de acceso inalámbrico.

¿Debo usar un punto de acceso externo o pfSense como mi acceso apuntar?

Históricamente, la funcionalidad de punto de acceso en FreeBSD ha sufrido de compatibilidad grave problemas con algunos clientes inalámbricos. Con FreeBSD 7.x esto ha mejorado de manera significativa, sin embargo, hay
todavía puede haber algunos dispositivos incompatibles. Estos problemas con la compatibilidad del cliente no son siempre
limitado a FreeBSD, pero es posible que la calificación de los consumidores router inalámbrico barato volvió acceso puntos proporciona una mejor compatibilidad de capacidades de punto de acceso de FreeBSD en algunos casos. Yo uso puntos de acceso pfSense en casa sin ningún problema, con mi MacBook Pro, AirTunes de Apple, Mac mini G4, iPod Touch, Palm Treo, varios ordenadores portátiles de Windows, Xbox 360, y los clientes de FreeBSD y funciona muy fiable a través de todos estos dispositivos. Existe la posibilidad de encontrar dispositivos incompatibles con cualquier punto de acceso. FreeBSD no es una excepción y es posible que esto es más común en FreeBSD que otros puntos de acceso. En versiones anteriores de FreeBSD, especialmente con m0n0wall en FreeBSD 4.x, Me recomendó no utilizar la funcionalidad de punto de acceso de FreeBSD. Hoy funciona bien con casi todos los dispositivo y es probablemente adecuado para su red.

Esto está sujeto a cambios significativos con cada versión de FreeBSD. Una lista actualizada de los conocidos dispositivos incompatibles y la información más reciente sobre compatibilidad inalámbrica se puede encontrar en http:// www.pfsense.org / apcompat.

Configuración de pfSense 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 algunas opciones puede ser nuevo a menos que haya utilizado algún equipo inalámbrico de calidad comercial. Hay docenas de formas de configurar los puntos de acceso, y todos ellos dependen de su entorno. Aquí, cubrimos ajuste pfSense como un AP básico que utiliza el cifrado WPA2 con AES. En este ejemplo, ExampleCo necesita acceso inalámbrico para algunas computadoras portátiles en la sala de conferencias.

Preparación de la Interfaz inalámbrica

Antes de hacer cualquier otra cosa, asegúrese de que la tarjeta inalámbrica está en el router y la antena está firmemente adjunta. Como se ha descrito anteriormente en este capítulo, la tarjeta inalámbrica se debe asignar como una interfaz OPT y habilitado antes de la configuración restante se puede completar.

Interfaz Descripción

Cuando está en uso como punto de acceso, el nombre "WLAN" (Wireless LAN) o "Wireless" hará que sea fácil identificar en la lista de interfaces. Si usted tiene un SSID único, puede que le resulte más conveniente utilizar que en la descripción lugar. Si pfSense va a manejar múltiples puntos de acceso, que debería haber alguna manera de distinguir ellos, tales como "WLANadmin" y "WLANsales". Llamaremos a éste ConfRoom por ahora.

Tipo de interfaz / Dirección IP

Dado que este será un punto de acceso en una subred IP dedicada, se debe ajustar el tipo de Estático y especificar una dirección IP y la máscara de subred. Como se trata de una subred separada de las otras interfaces, puede ser 192.168.201.0/24, una subred que es de otra manera sin utilizar en la red ExampleCo.

Estándar inalámbrico

Dependiendo de soporte de hardware, hay varias opciones disponibles para la configuración estándar inalámbrico, incluyendo 802.11b, 802.11g, turbo 802.11g, 802.11a, y turbo 802.11a, y posiblemente otros. Por esta ejemplo, vamos a elegir 802.11g.

Modo inalámbrico

Establezca el campo Modo a Punto de Acceso, y pfSense utilizará hostapd para actuar como un AP.

Service Set Identifier (SSID)

Este será el "nombre" de la AP, como se ve por los clientes. Usted debe configurar el SSID a algo fácilmente identificable, pero único a su configuración. Siguiendo con el ejemplo, este puede ser nombrado ConfRoom.

Limitar el acceso a 802.11g Only

El 802.11g sólo controla si o no clientes 802.11b mayores son capaces de asociar a este
punto de acceso. Permitiendo a los clientes de edad avanzada pueden ser necesarios en algunos entornos de si los dispositivos son todavía alrededor
que así lo requieran. Algunos dispositivos móviles como el Nintendo DS y el Palm Tungsten C sólo son compatible con 802.11b y requieren una red mixta con el fin de trabajar. La otra cara de esto es que
podrás ver las velocidades más lentas, como resultado de permitir que tales dispositivos de la red, ya que el punto de acceso
se verá obligado a atender a un mínimo común denominador cuando un dispositivo 802.11b está presente. En nuestra sala de conferencia ejemplo, la gente sólo va a utilizar ordenadores portátiles propiedad de la compañía recientemente adquiridos que
Todos somos capaces de 802.11g, por lo que vamos a comprobar esta opción.

Comunicación Intra-BSS

Si marca Permitir la comunicación intra-BSS, los clientes inalámbricos puedan verse entre sí directamente, en lugar de enrutar todo el tráfico a través de la AP. Si los clientes sólo tendrán acceso a la Internet, es típicamente más seguro para desactivar esto. En nuestro escenario, la gente en la sala de conferencias pueden necesitar compartir archivos de ida y
establece directamente entre los ordenadores portátiles, por lo que este se quedará marcada.

SSID Ocultación (Disable SSID Broadcasting)

Normalmente, la AP transmitirá su SSID para que los clientes pueden localizar y asociarse con él fácilmente. Es considerado por algunos como un riesgo de seguridad, anunciando a todos los que están escuchando que usted tiene una conexión inalámbrica
red disponible, pero en la mayoría de los casos la comodidad es mayor que el riesgo de seguridad. Los beneficios de deshabilitar la difusión del SSID son exagerados por algunos, ya que en realidad no oculta la red de
alguien capaz de utilizar muchas herramientas de seguridad inalámbrica de libre acceso que fácilmente encontrar tales inalámbrica
redes. Para nuestra sala de conferencias AP, dejaremos esta opción sin marcar para que sea más fácil para la reunión los asistentes a encontrar y utilizar el servicio.

Selección Wireless Channel

Al seleccionar un canal, tendrá que ser consciente de los transmisores de radio en las proximidades de similares bandas de frecuencia. Además de los puntos de acceso inalámbrico, también hay teléfonos inalámbricos, Bluetooth, monitores de bebés, transmisores de video, microondas y muchos otros dispositivos que utilizan los mismos 2,4 GHz espectro que pueden causar interferencia. A menudo, usted puede conseguir lejos con el uso de cualquier canal que desee, siempre
como sus clientes de AP son cerca de la antena. Los canales más seguros para usar son 1, 6, y 11, ya que su frecuencia bandas no se solapan entre sí. Puede especificar Auto a contar la tarjeta para recoger un canal apropiado, sin embargo, esta funcionalidad no funciona con algunas tarjetas de red inalámbricas. Si usted elige Auto y las cosas no funciona, seleccione un canal específico en su lugar. Para esta red, ya que no hay otros a su alrededor, vamos a elegir el canal 1.

Cifrado inalámbrico

Hay tres tipos de cifrado son compatibles con las redes 802.11: WEP, WPA, y WPA2. WPA2 con AES es el más seguro. Incluso si usted no está preocupado acerca de la encriptación del tráfico de over-the-air (que usted debería ser), que proporciona un medio adicional de control de acceso. Una frase de contraseña WPA/WPA2 es también
más fácil trabajar con el entonces una clave WEP en la mayoría de los dispositivos; actúa más como una contraseña de un muy largo
cadena de caracteres hexadecimales. Al igual que con la elección entre 802.11by 802.11g, algunos dispositivos más antiguos
Para adentro WEP o WPA, pero, utilizaría WPA2, WEP y controladores. Para ello, desactivar los apoyar WPA2 y WEP, y seleccione Habilitar WPA. Para garantizar que sólo WPA2 estará en uso, ajuste el modo WPA para WPA2. Para nuestro
WPA Pre-Shared Key, utilizaremos excoconf213, y también configurar WPA en modo de administración de claves para Pre-
Shared Key.
Para utilizar WPA2 + AES, según se desee para la conexión inalámbrica de sesión, establezca WPA por parejas a AES.

Nota

Para utilizar WPA2 con un cliente inalámbrico de Windows XP, debe tener un controlador inalámbrico que soporta WPA2. Si está utilizando la interfaz de configuración inalámbrica de Windows XP, con el fin asociarse con un punto de acceso WPA2 funcionamiento tendrá que actualizar el PC a
Windows XP SP3 o instalar el parche de artículo de Microsoft Knowledge Base 917021 [http://support.microsoft.com/kb/917021].

Debilidades de cifrado inalámbrico

WEP ha tenido graves problemas de seguridad conocidos desde hace años, y nunca debe ser usado a menos que sea el única opción para los dispositivos inalámbricos se debe apoyar. Es posible obtener la clave WEP en cuestión de minutos

a lo sumo, y nunca se debe confiar en la seguridad. WEP no se puede confiar en nada más de mantener alejados a los solicitantes de Internet sin necesidad de conocimientos técnicos.

TKIP (Temporal Key Integrity Protocol), parte de AES, se convirtió en un sustituto de WEP después de que fuera roto. Se utiliza el mismo mecanismo subyacente como WEP, y por lo tanto es vulnerable a algunos similares ataques. Recientemente, estos ataques son cada vez más prácticos. En el momento de escribir estas líneas no es tan fácil de romper como WEP, pero todavía se debe nunca utilizar a menos que tenga los dispositivos que no son compatibles
con WPA o WPA2 con AES. WPA y WPA2 en combinación con AES no están sujetos a estas fallas en TKIP.

Ajustes de AP de acabado

Los ajustes anteriores deben ser suficientes para conseguir un punto de acceso inalámbrico 802.11g con funcionamiento con
WPA2 + AES. Hay otras opciones que se pueden utilizar para ajustar el comportamiento de la AP, pero no son necesarios para el funcionamiento normal en la mayoría de los entornos. Cuando haya terminado de cambiar la configuración, haga clic en Guardar y después en Aplicar cambios.

Configuración de DHCP

Ahora que hemos creado una red totalmente independiente, querremos que debe habilitar DHCP para que asociando los clientes inalámbricos puede obtener automáticamente una dirección IP. Vaya a Servicios DHCP Server, haga clic en la ficha para su interfaz inalámbrica (ConfRoom para nuestro ejemplo de configuración). Compruebe el
casilla para activar, configurar cualquier tamaño de rango que se necesita, y las opciones adicionales que se necesitan, y luego haga clic en
Guardar y Aplicar cambios. Para más detalles sobre cómo configurar el servicio de DHCP, consulte la sección llamada "DHCP Server".

Adición de reglas de firewall

Desde esta interfaz inalámbrica es una interfaz OPT, tendrá ninguna regla de firewall por defecto. Por lo menos usted tendrá que tener una regla para permitir el tráfico de esta subred a cualquier destino que se necesitará. Ya que nuestros usuarios de las salas de conferencia tendrán acceso a Internet y el acceso a otros recursos de la red,

un defecto permiten la regla va a estar bien en este caso. Para crear la regla, vaya a Firewall Reglas y clic en la pestaña de la interfaz inalámbrica (ConfRoom para este ejemplo). Agregue una regla para pasar el tráfico de cualquier
protocolo, con una dirección de origen de la subred ConfRoom, y cualquier destino. Para obtener más información sobre la creación de reglas de firewall, consulte el Capítulo 10, Firewall.

Asociar Clientes

El recién configurado pfSense AP debería aparecer en la lista de puntos de acceso disponibles en su dispositivo inalámbrico, asumiendo que no desactive la difusión del SSID. Usted debe ser capaz de clientes asociados con ella como lo haría con cualquier otro punto de acceso. El procedimiento exacto puede variar entre sistemas operativos, dispositivos y controladores, pero la mayoría de los fabricantes han simplificado el proceso para hacer
que sea sencillo para todos.

Ver el estado del cliente inalámbrico

Cuando usted tiene una interfaz inalámbrica configurada para el modo de punto de acceso, los clientes asociados serán que aparece en Estado Wireless.

Protección adicional para su red inalámbrica red

Además de una fuerte encriptación de WPA o WPA2 con AES, algunos usuarios les gusta emplear un capa adicional de encriptación y autenticación para permitir el acceso a los recursos de red. La

dos soluciones más comúnmente desplegados son Portal Cautivo y VPN. Estos métodos pueden ser empleados si se utiliza un punto de acceso externo en una interfaz OPT o una tarjeta inalámbrica interna como su punto de acceso.

Protección inalámbrica adicional con Portal Cautivo

Habilitando Portal Cautivo en la interfaz en la que reside su red inalámbrica, puede requerir la autenticación que los usuarios puedan acceder a los recursos de red. En las redes corporativas, esto se implementa comúnmente con Autenticación RADIUS de Microsoft Active Directory para que los usuarios puedan utilizar su Active Directory credenciales para autenticar mientras que en la red inalámbrica. Configuración de Portal Cautivo se cubre en Capítulo 23, Portal Cautivo.

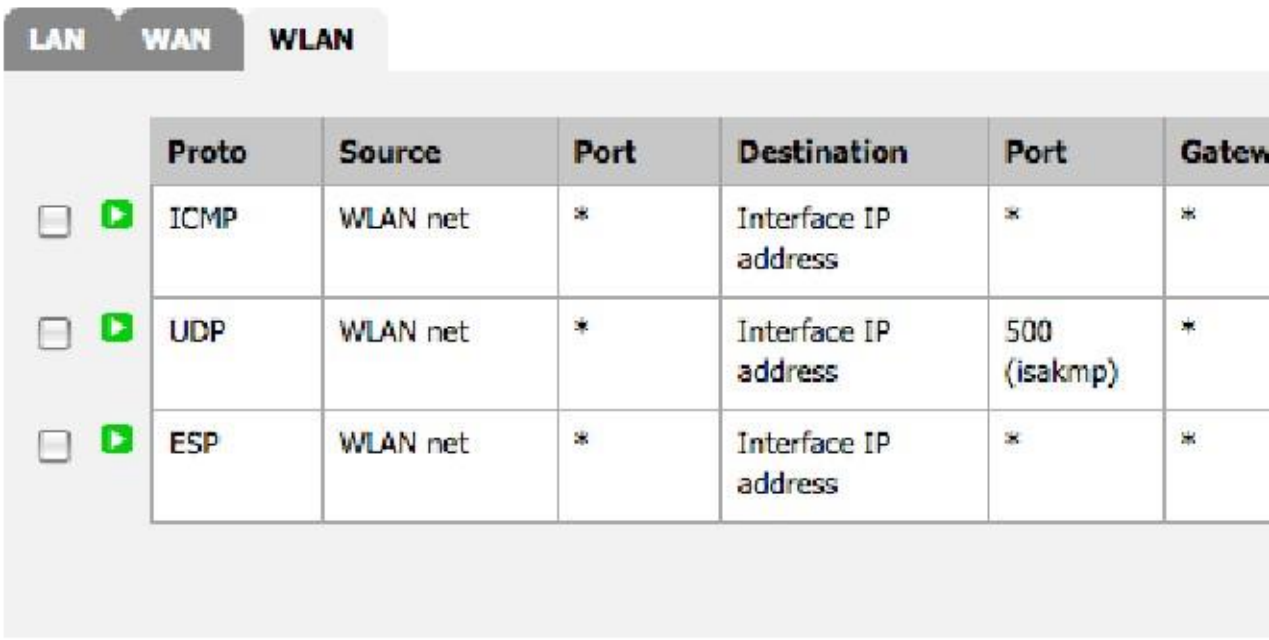
Protección adicional con VPN

Adición de Portal Cautivo ofrece otro nivel de autenticación, pero no ofrece ninguna adicional Protección contra escuchas de su tráfico inalámbrico. Exigir VPN antes de permitir el acceso a la red interna e Internet añade otra capa de autenticación, así como una capa adicional de cifrado para el tráfico inalámbrico. La configuración para el tipo elegido de VPN no será diferente desde una configuración de acceso remoto, pero usted tendrá que configurar las reglas de firewall en el pfSense interfaz sólo para permitir el tráfico VPN de los clientes inalámbricos.

Configuración de reglas de firewall para IPsec

Figura 22.5, "Reglas para permitir sólo IPsec desde inalámbrico" muestra las normas mínimas requeridas para permitir único acceso a IPsec en el IP de la interfaz WLAN. Pings a la IP de la interfaz WLAN también pueden ayudar en la solución de problemas.

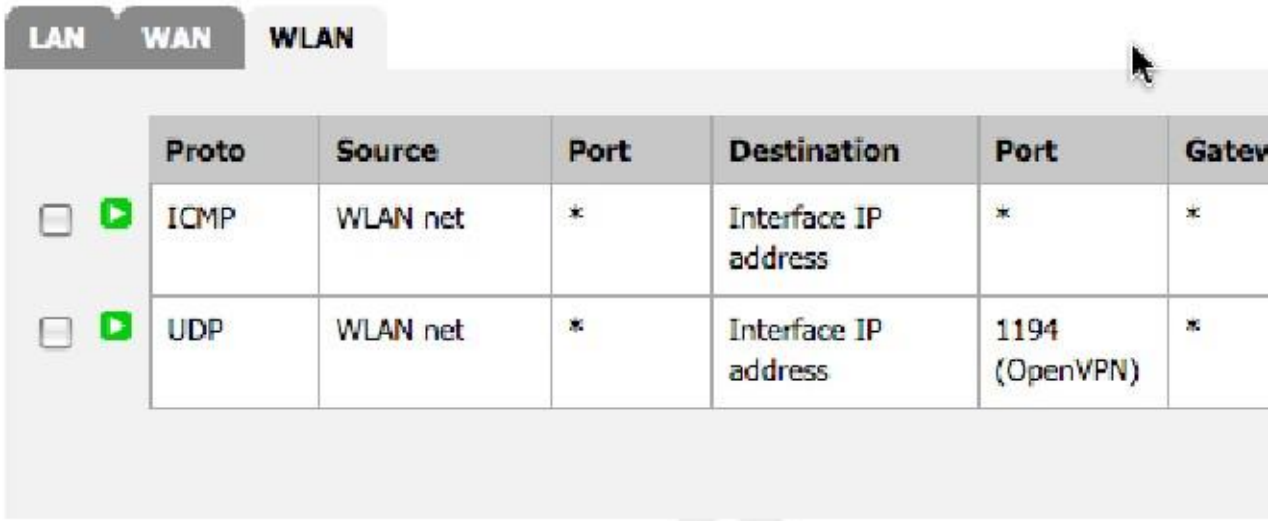
Figura 22.5. Reglas para permitir sólo IPsec desde inalámbrico



Configuración de reglas de firewall para OpenVPN

Figura 22.6, "Reglas para permitir sólo OpenVPN desde inalámbrico" muestra las normas mínimas requeridas para permitir
acceso sólo a OpenVPN en la IP de la interfaz WLAN. También se permiten pings a la IP de la interfaz WLAN para ayudar en la solución de problemas. Esto supone que está utilizando el puerto UDP predeterminado 1194. Si decide otro protocolo o puerto, ajustar la regla en consecuencia.

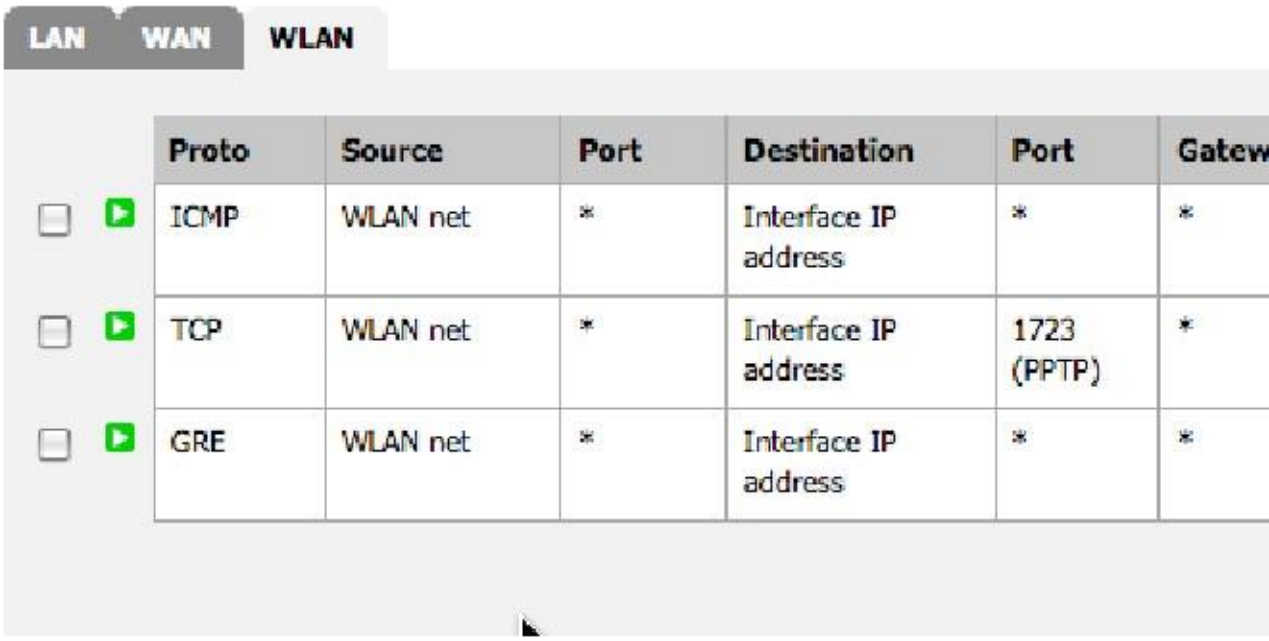
Figura 22.6. Reglas para permitir sólo OpenVPN desde inalámbrico



Configuración de reglas de firewall para PPTP

Figura 22.7, "Reglas para permitir sólo PPTP desde inalámbrico" muestra las normas mínimas requeridas para permitir acceso sólo a PPTP en la IP de la interfaz WLAN. Pings a la IP de la interfaz WLAN también pueden ayudar en la solución de problemas.

Figura 22.7. Reglas para permitir sólo PPTP desde inalámbrico



Configuración de un punto de acceso inalámbrico seguro

Su empresa u organización puede desear proporcionar acceso a Internet para los clientes o huéspedes que utilicen la conexión a Internet existente. Esto puede ser una bendición para sus clientes y los negocios, sino que también puede exponer su red privada para atacar si no se hace correctamente. Esta sección trata de los medios comunes de proporcionar acceso a Internet a los huéspedes y clientes, al tiempo que protege su red interna.

Enfoque firewall Múltiple

Para la mejor protección entre la red privada y la red pública, obtener al menos dos públicas
IPs de su proveedor de Internet, y el uso de un segundo servidor de seguridad para la red pública. Para solucionar esto, se pone
un cambio entre la conexión a Internet y la WAN de dos cortafuegos. Esto también tiene la ventaja
de poner su red pública en una IP pública diferente de su red privada, por lo que si usted debe
recibir un informe de abuso, usted será capaz de distinguir si se originó a partir de su público
o una red privada. El firewall protege la red privada verá su red pública sin
de manera diferente a cualquier host de Internet.

Enfoque único firewall

En entornos en los que el enfoque de firewall múltiple es un costo prohibitivo o no deseado,
todavía se puede proteger la red interna mediante la conexión de la red pública a una interfaz OPT en
pfSense. Debe asignar una subred IP privada dedicada a esta interfaz OPT, y configurar el
reglas de firewall para permitir el acceso a la Internet, pero no la red interna.

Control de accesos y consideraciones filtrado de salida

Aparte de no permitir que el tráfico procedente de la red de acceso público a la red privada, hay
cosas adicionales que usted debe tener en cuenta en la configuración de su punto de acceso.

Restringir el acceso a la red

Mientras que muchos puntos de acceso utilizan las redes inalámbricas abiertas sin ningún otro tipo de autenticación, se debe considerar
protecciones adicionales para prevenir el abuso de la red. En su red inalámbrica, puede utilizar WPA o WPA2 y
proporcionar la frase de contraseña para sus invitados o clientes. Algunos tendrán la frase de contraseña en un cartel en el
vestíbulo o sala de espera, publicado en una habitación de invitados, o proporcionar a quienes la soliciten. También considere la implementación de
Portal Cautivo en pfSense (cubierto en el Capítulo 23, Portal Cautivo). Esto ayuda a evitar que la gente en otros
oficinas y fuera del edificio de la utilización de su red inalámbrica.

Desactivar la comunicación Intra-BSS

Si su punto de acceso permite, no debe permitir la comunicación intra-BSS. Esto evita inalámbrica
clientes de comunicarse con otros clientes inalámbricos, que protege a los usuarios contra intencional
ataques de otros usuarios inalámbricos, así como los no intencionales, como los gusanos.

Filtrado de salida

Considere qué tipo de política egreso configurar. El permitir el acceso más básico, a la Internet
sin permitir el acceso a la red privada, es, probablemente, el más comúnmente desplegados pero
deberían considerar restricciones adicionales. Para evitar que su negro dirección IP pública que cotiza por
infectado los sistemas que actúan como robots de spam visitar, usted debe considerar el bloqueo de SMTP. Una alternativa que
todavía permite a las personas utilizar su correo electrónico SMTP, pero limita el efecto de los robots de spam es la de crear una regla de permiso para
SMTP y especificar las entradas estatales Máximo por host en Opciones avanzadas del Firewall: Reglas:
Editar página. Asegúrese de que la norma está por encima de cualquier otra norma que se correspondería con el tráfico SMTP y especifique un bajo
limitar. Puesto que las conexiones no siempre se cierran correctamente por el cliente de correo o el servidor, no podrá
quieren establecer este demasiado bajo para evitar el bloqueo de usuarios legítimos, pero un límite de cinco conexiones debe ser
razonable. Es posible que desee especificar entradas Máximo estatales por host en todas las reglas del cortafuegos, pero
tenga en cuenta que algunos protocolos requieren decenas o cientos de conexiones a la función. HTTP
y HTTPS pueden requerir numerosas conexiones que cargue una página web según el contenido
de la página y el comportamiento del navegador, por lo que no establezca sus límites demasiado bajos.
Usted tendrá que equilibrar los deseos de sus usuarios contra los riesgos inherentes a la concesión de Internet
acceso para los sistemas que no controla, y definir una política que se adapte a su entorno.

Solución de problemas de conexiones inalámbricas

Cuando se trata de radio, hay un montón de cosas que pueden salir mal. De hardware defectuoso
conexiones a interferencias de radio en software incompatible / drivers o configuraciones simples desajustes,
cualquier cosa es posible, y puede ser un desafío para hacer que todo funcione en el primer intento. Esta sección cubrirá
algunos de los problemas más comunes que han sido encontrados por los usuarios y desarrolladores de pfSense.

Compruebe la antena

Antes de gastar cualquier momento el diagnóstico de un problema, dobles y triples comprobar la conexión de la antena. Si
es un tipo de rosca, asegúrese que quede bien apretado. Para las tarjetas mini-PCI, asegúrese de que los conectores de cable flexible son
correctamente conectado y quebró en su lugar. Coletas en las tarjetas mini-PCI son frágiles y fáciles de romper.
Después de desconectar y volver a conectar un par de veces, puede que tenga que reemplazarlos.

Pruebe con varios clientes o tarjetas inalámbricas

Para eliminar una posible incompatibilidad entre las funciones inalámbricas del pfSense y su cliente inalámbrico,
no deje de probar con varios dispositivos o tarjetas de primera. Si el mismo problema es repetible con varios
diferentes marcas y modelos, es más probable que sea un problema con la configuración o hardware relacionado
que el dispositivo cliente.

Intensidad de la señal es baja

Si usted tiene una señal débil, incluso si estás cerca de la antena del punto de acceso, compruebe la antena
de nuevo. Para las tarjetas mini-PCI, si sólo tienes una coleta en uso y hay dos conectores internos,
intentar conectar a otro conector interno de la tarjeta. También puede intentar cambiar el canal o
el ajuste de la potencia de transmisión en la configuración de la interfaz inalámbrica. Para las tarjetas mini-PCI, compruebe si hay
extremos rotos en los conectores pigtail frágiles donde se conectan a la tarjeta mini-PCI.

Capítulo 23. Portal Cautivo

La función de Portal Cautivo de pfSense le permite dirigir a los usuarios a una página web antes de acceso a Internet es permitida. Desde esa página, puede permitir a los usuarios acceder a Internet después de hacer clic a través de, o requerir la autenticación. Los usos más comunes de Portal Cautivo son los puntos calientes inalámbricos, o adicional autenticación antes de permitir el acceso a las redes internas de los clientes inalámbricos. También se puede utilizar con clientes por cable si se desea.

Limitaciones

La aplicación de portal cautivo en pfSense tiene algunas limitaciones. Esta sección cubre los, y las formas más comunes de trabajo alrededor de ellos siempre que sea posible.

Sólo se puede ejecutar en una sola interfaz

Sólo se puede utilizar el portal cautivo en una interfaz de servidor de seguridad. Para redes donde múltiples IP subredes requieren funcionalidad Portal Cautivo, usted tendrá que utilizar un router dentro de su portal cautivo instalar, como se ilustra en la Figura 23.1, "Captive Portal en varias subredes".

Que no sean capaces de portal inverso

Un portal inversa, que requiere autenticación para el tráfico que llega a su red desde Internet, es no es posible.

Configuración del portal sin autenticación

Para un simple portal sin autenticación, todo lo que tiene que hacer es marcar la casilla Habilitar portal cautivo, seleccionar una interfaz, y cargar una página HTML con el contenido de su portal, como se describe en la sección llamado "contenido de la página del Portal". Es posible que desee para especificar las opciones de configuración adicionales que se detallan
en la sección llamada "Opciones de configuración".

Configuración de portal Usando Local Autenticación

Para configurar un portal con autenticación local, active la casilla Habilitar portal cautivo, selecciona una interfaz, elegir la autenticación local, y cargar una página HTML con el contenido de su portal, como se describe en el sección llamada "contenido de la página del Portal". Es posible que desee para especificar las opciones de configuración adicionales como
se detalla en la sección titulada "Opciones de configuración". A continuación, configure los usuarios locales de los usuarios
tab de los Servicios Página de portal cautivo.

Portal de configuración mediante RADIUS Autenticación

Para configurar un portal mediante la autenticación RADIUS, primero configurar el servidor RADIUS, a continuación, siga el
mismos procedimientos que la creación de un portal con autenticación local, llenando la información apropiada para el servidor RADIUS. Lea la siguiente sección para obtener información sobre las opciones de configuración específicas que
tal vez desee utilizar.

Opciones de configuración

En esta sección se describe cada una de las opciones de configuración de Portal Cautivo.

Interfaz

Aquí se selecciona el portal cautivo interfaz se ejecutará en. Esto no puede ser una interfaz de puente, y no puede ser cualquier interfaz de WAN WAN o OPT.

Número máximo de conexiones concurrentes

Este campo especifica el número máximo de conexiones simultáneas por dirección IP. El valor por defecto es 4, que debería ser suficiente para la mayoría de entornos. Este límite existe para evitar que un único host desde agotar todos los recursos en el servidor de seguridad, ya sea accidental o intencional. Un ejemplo donde este de otro modo sería un problema es un huésped infectado con un gusano. Los miles de conexiones emitidas hará que la página del portal cautivo que se genere en varias ocasiones si el anfitrión no está autenticado, que de otro modo generar tanta carga que dejaría su sistema deje de responder.

Intervalo de espera inactivo

Si quiere desconectar a los usuarios inactivos, rellenar un valor aquí. Los usuarios serán capaces de entrar de nuevo inmediatamente.

Timeout duro

Para iniciar la sesión con fuerza fuera de los usuarios después de un período determinado, introduzca un valor de tiempo de espera dura. Usted debe registrarse en un
tiempo de espera de disco, tiempo de inactividad o ambos para garantizar que las sesiones se eliminan si los usuarios no cierran la sesión, ya que lo más probable
No lo haré. Los usuarios serán capaces de entrar de nuevo inmediatamente después de que el tiempo de espera de disco, si sus credenciales son
siendo válido (para las cuentas locales, no caducado, y para la autenticación RADIUS, el usuario todavía puede con éxito autenticarse en RADIUS).

Ventana emergente Salir

Marque esta casilla para activar una ventana de cierre de sesión de pop up. Por desgracia, ya que la mayoría de los navegadores han abrirá
bloqueadores habilitados, esta ventana puede no funcionar para la mayoría de sus usuarios a menos que controles los ordenadores
y puede excluir a su portal en su bloqueador de elementos emergentes.

URL de redirección

Si introduce una URL aquí, después de la autenticación o hacer clic a través del portal, los usuarios serán redirigidos a esta URL en lugar de la que originalmente intentaron acceder. Si este campo se deja en blanco, el usuario ser redirigido a la URL inicialmente el usuario ha intentado acceder.

Los inicios de sesión de usuarios concurrentes

Si se marca esta casilla, sólo se permite un inicio de sesión por cada cuenta de usuario. Se permite el inicio de sesión más reciente
y los inicios de sesión previos en virtud de ese nombre de usuario se desconectarán.

Filtrado MAC

Esta opción le permite desactivar el filtrado de MAC por defecto. Esto es necesario en el caso de múltiples subredes detrás de un router a través del portal, como se ilustra en la Figura 23.1, "portal cautivo en múltiples subredes ", ya que todos los usuarios detrás de un router aparecerán en el portal como la dirección MAC del router.

Autenticación

Esta sección le permite configurar la autenticación si se desea. Si se deja sin autenticación seleccionado, los usuarios sólo tendrán que hacer clic a través de la pantalla de su portal de acceso. Si usted requiere autenticación, puede utilizar el gestor de usuario local o la autenticación RADIUS. Los usuarios del gestor de usuario local

se configuran en la ficha Usuarios de los Servicios Página de portal cautivo. Los usuarios de RADIUS se definen en el servidor RADIUS. Para aquellos con una infraestructura de red de Microsoft Active Directory, RADIUS puede utilizarse para autenticar a los usuarios de portal cautivo de su Active Directory con Microsoft IAS. Esto se describe en la sección "Autenticación RADIUS con Windows Server". Hay numerosos otros servidores RADIUS que también se pueden utilizar. Contabilidad RADIUS se puede habilitar para enviar información de uso de cada usuario al servidor RADIUS. Consulte la documentación de su RADIUS servidor para obtener más información.

HTTPS de inicio de sesión

Marque esta casilla para utilizar HTTPS para la página del portal. Si marca esta debe introducir un certificado y clave privada.

HTTPS nombre del servidor

Este campo es donde se especifica el FQDN (nombre de host + dominio) que se utilizará para HTTPS. Este necesidades para que coincida con el nombre común (CN) del certificado para evitar que sus usuarios reciban certificado errores en sus navegadores.

Contenido de la página del Portal

Aquí usted carga una página HTML que contiene la página del portal los usuarios verán cuando se trata de acceso Internet antes de autenticar o accediendo al portal.

Página Portal sin autenticación

Esto muestra el código HTML de una página de portal que se puede utilizar sin 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 name="accept" type="submit" value="Continue">
</ Form>
</ Body>
</ Html>
```

Página Portal con autenticación

He aquí un ejemplo de página de portal que requiere 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 haga clic en Login para acceder a Int
</ 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 name="accept" type="submit" value="Login">
</ Form>
</ Body>
</ Html>
```

Contenido de la página de error de autenticación

Aquí puede cargar una página HTML que se mostrará en los errores de autenticación. Un error de autenticación se produce cuando un usuario entra en un mal nombre de usuario o contraseña, o en el caso de la autenticación RADIUS, potencialmente un servidor RADIUS inalcanzable.

Solución de problemas de Portal Cautivo

Esta sección contiene sugerencias para la solución para el problema más común con el portal cautivo.

Los errores de autenticación

Los errores de autenticación son normalmente el resultado de los usuarios que entran en un nombre de usuario o contraseña incorrecta.
En el caso de la autenticación RADIUS, estos pueden ocurrir debido a problemas de conectividad a su Servidor RADIUS, o problemas en el servidor RADIUS en sí. Compruebe los registros de su servidor RADIUS para la indicios de por qué se le negó el acceso, y asegurar el firewall puede comunicarse con el RADIUS servidor.

Página de Portal nunca carga (tiempo de espera) ni ningún otro carga de la página

Esto ha sido reportado a suceder al utilizar 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 etiqueta VLAN 10 en `fxp1`, no se puede tener `fxp1` asignado como cualquier otra interfaz, debe dejarse sin utilizar. Este es el recomienda la configuración de todos modos, y este problema es una razón más para seguir ese consejo.

Capítulo 24. Servidor de seguridad de redundancia / Alta disponibilidad

pfSense es una de las pocas soluciones de código abierto de clase empresarial que ofrecen alta disponibilidad capacidades con reconexión dinámica, lo que permite la eliminación del firewall como un único punto de fallo. Esto está previsto por la combinación de CARP, pfsync, y la configuración de XML-RPC de pfSense de sincronización, cada uno de los cuales se explicará en este capítulo. A menudo esto se refiere simplemente como CARP, aunque técnicamente CARP es sólo parte de la solución completa.

Comenzando con pfSense 2.1, la configuración de sincronización de alta disponibilidad se han movido a Sistema Alta Disponibilidad. Sync. Esto se hizo para desacoplar la asociación lógica de los ajustes de sincronización de la configuración de IP virtual porque mientras ellos están algo relacionados, son funciones independientes. VIPs CARP se pueden utilizar sin hacer de conmutación por error, y la sincronización se pueden utilizar para otros fines además CARP. En referencia a los ajustes de sincronización como la configuración de la "carpa" era un nombre poco apropiado
que llevó a la gente a hacer falsas suposiciones sobre el comportamiento y la interacción entre estas funciones.

Es importante distinguir entre las dos funciones porque ocurren en diferentes lugares. La XML-RPC y pfsync tráfico que sucede en su interfaz de sincronización, comunicación directa entre la dos unidades de firewall. Latidos CARP se envían en cada interfaz con un VIP CARP, una vez por segundo o así que dependiendo de la publicidad de inclinación y la base. Si una unidad secundaria no logra ver un latido del corazón de la
dominar en cualquier interfaz, se tratará de ocupar el cargo de maestro. En otras palabras, la señalización de conmutación por error
no ocurre en la interfaz de sincronización como se podría creer, sino más bien esto ocurre en cada CARP-interfaz habilitada.

CARP general

Dirección general del protocolo de redundancia (CARP) fue creado por los desarrolladores de OpenBSD como un país libre, abierto
solución de redundancia para el intercambio de direcciones IP entre un grupo de dispositivos de red. Soluciones similares ya existía, principalmente el estándar IETF para el protocolo de redundancia de enrutador virtual (VRRP). Sin embargo Cisco afirma VRRP está cubierto por su patente en su Protocolo Hot Standby Router (HSRP), y le dijo a los desarrolladores de OpenBSD que haría cumplir su patente. Por lo tanto, los desarrolladores de OpenBSD creado un nuevo protocolo abierto, libre para llevar a cabo esencialmente el mismo resultado sin infringir Patentes de Cisco. CARP llegó a estar disponible en octubre de 2003 en OpenBSD, y más tarde se añadió a FreeBSD así.

Cada firewall pfSense en un grupo CARP tiene su propia dirección IP única asignada a cada interfaz, y tiene los VIPs CARP compartidos asignado también. Estas IPs CARP sólo están activos si el servidor de seguridad es Actualmente el maestro.

CARP echará sus propios paquetes de otros nodos para ver, uno por cada VIP en cada interfaz, una vez por segundos más o menos, dependiendo de los valores de la publicidad de base y el sesgado (más sobre esto más adelante). Estos
latidos se envían a través de multidifusión y el interruptor llevarán las de los demás miembros. CARP también supervisa todas las interfaces que tiene un VIP CARP permitido ver a estos paquetes CARP. En caso de que un paquetes no llegan tan rápido como se esperaba, se tomará el fracaso ha tenido lugar, y un nodo de menor prioridad asumirá el cargo de maestro. Configuramos el sistema CARP tal que si una falla de cualquier interfaz de red se detecta, el próximo firewall designado pasa a dominar en todas las interfaces.

O bien una pérdida de la señal del maestro en una interfaz (no hay latidos llegan) o si llegan demasiado lentamente (más lenta que la velocidad propia del nodo secundario), se asumirá un fracaso. Esta propiedad de la CARP del
La comunicación puede ser la causa de algún problema en la capa 2, porque hay interruptores que ya sea en bloque multicast, manejarlo mal, o de otra manera no pueden entregar correctamente los paquetes de latido entre los nodos, dando lugar a una situación en la que todos los nodos se creen maestro para ciertas personalidades. Hay más detalle en la depuración de problemas del interruptor con CARP en la sección llamada "CARP Solución de problemas". Un común
concepto erróneo es que la conmutación por error se indica de alguna manera a través del interfaz de sincronización, pero eso no es correcto.

CARP ocurre en todas partes se definen VIPs carpa, ya que es la única manera de determinar con fiabilidad si un determinado enlace ha fallado.

Nota

Debido a que cada miembro del grupo CARP debe tener una dirección IP en una subred, además de la Dirección IP CARP, se requieren al menos tres direcciones IP disponibles para cada interfaz, y más direcciones IP para los miembros de grupo adicionales. Esto también se aplica a la interfaz WAN, así que asegúrese de tener al menos tres direcciones IP disponibles disponibles de su ISP. El más pequeño bloque enrutable que incluye 3 direcciones IP es un / 29, que tiene 8 direcciones (6) utilizable.

pfsync Información general

pfsync permite la sincronización de la tabla de estado de servidor de seguridad desde el servidor de seguridad maestro para secundaria
firewalls. Cambios en la tabla de estados de las primarias se envían en la red para el servidor de seguridad secundario (s), y viceversa. Esto utiliza multicast por defecto, aunque la dirección IP se puede definir en el pfSense
interfaz para forzar actualizaciones unicast para entornos con sólo dos servidores de seguridad, donde el tráfico multicast no funcionará correctamente (algunos interruptores bloquean o ruptura de multidifusión). Se puede utilizar cualquier interfaz activa
para el envío de actualizaciones pfsync, sin embargo le recomendamos que utilice una interfaz dedicada para la seguridad y
razones de rendimiento. pfsync no admite ningún tipo de autenticación, por lo que si usted usa otra cosa de una interfaz dedicada, es posible para cualquier usuario con acceso a la red local para insertar en estados el servidor de seguridad secundario. En entornos de bajo rendimiento que no son de seguridad paranoide, el uso de la LAN
interfaz para este propósito es aceptable. Ancho de banda necesario para la sincronización del estado variará significativamente de un entorno a otro, pero podría ser tan alto como 10% del rendimiento de desplazamiento
El servidor de seguridad en función de la carga por errores y pérdida de la tabla de estado, lo que permite una perfecta conmutación por error. En algunos entornos, no se dará cuenta de la diferencia entre la conmutación por error y statefully perdiendo estado durante la conmutación por error. En otras redes, puede causar una significativa pero breve interrupción de la red.

Los ajustes pfsync debe estar habilitado en todos los nodos que participan en la sincronización de estado, los nodos esclavos
incluido.

pfsync y actualizaciones

Normalmente pfSense permitiría mejoras de firewall sin ninguna interrupción de la red. Desafortunadamente, este no es siempre el caso con las actualizaciones como el protocolo pfsync cambia, para adaptarse adicional funcionalidad. Si va a actualizar desde pfSense 1.2.x para 2.x o superior, el sistema operativo subyacente cambió de FreeBSD 6.x o 7.x para FreeBSD 8.x e incluye un pfsync más reciente. Siempre revise la guía de actualización vinculado en todos los anuncios de publicación antes de actualizar a ver si hay alguna consideración especial para los usuarios de CARP.

pfSense XML-RPC Sync Información general

sincronización de la configuración de pfSense le permite realizar la mayoría de los cambios de configuración en sólo el servidor de seguridad primaria, que a continuación se replica esos cambios a la secundaria automáticamente. Las áreas con el apoyo de esto son los usuarios y los grupos, los certificados, las reglas del cortafuegos, programas de firewall, alias, NAT,
IPsec, OpenVPN, DHCP, Wake on LAN, rutas y puertas de enlace, equilibrador de carga, IPs virtuales, regulador de trafico
(colas, limitadores, y la capa 7), promotor de DNS y de portal cautivo. Otros ajustes deben estar individualmente configurada en el servidor de seguridad secundaria, según sea necesario, aunque la sincronización cubre la mayor parte, si no todos
lo que va a cambiar de forma rutinaria. La sincronización de configuración debe utilizar la misma interfaz que el tráfico pfsync.
La configuración de XML-RPC debe sólo estar habilitado en el nodo principal, el resto de nodos deben tener estos configuración discapacitados.

XML-RPC y actualizaciones

Al igual que con pfsync, puede ser necesario tener un poco de cuidado al actualizar un clúster de servidor de seguridad con XML-RPC
la sincronización está habilitada cuando se pasa de 1.2.x para 2.x. Vas a actualizar ya sea la primaria o la secundaria primero, dejando el otro en 1.2.3 hasta que finalice la prueba. Ya sea para elegir la primaria o la
depende secundaria de su preferencia, sin embargo, hay consideraciones adicionales. Históricamente hemos recomienda actualizar el secundario en primer lugar, la verificación de que funciona como se desea, y luego actualizar la primaria. Sin embargo, con 2,0 lo contrario puede ser preferible. 1.2.3 no comprueba la versión es
sincronizar su configuración para, por lo que se sobreponen a las piezas de un config 2.x con la antigua estructura de la configuración que no es
correcta para 2.x. Esto significa actualizando el primario puede ser preferible como 2.x no se sincronizará la configuración para
1.2.3 Para evitar los problemas que se producen al sincronizar la versión de configuración incorrecta.
Si actualiza el secundario en primer lugar, tomar la IP, nombre de usuario y la contraseña de Firewall IPs virtuales, Ficha Configuración de la carpa en la primaria hasta la primaria se actualiza a 2.1. Una vez que se ha actualizado el primaria a 2,1 puede rellenar las opciones de vuelta pulg Tenga en cuenta que el 2.1 tiene la ubicación de estos centros

cambiado al Sistema Alta Disponibilidad. Sync.

Configuración redundante Ejemplo

Esta sección describe los pasos en la planificación y configuración de una sencilla interfaz de tres CARP configuración. Las tres interfaces son LAN, WAN, y pfsync. Esto es funcionalmente equivalente a un dos interfaces LAN y WAN de despliegue, con la interfaz pfsync se utiliza únicamente para sincronizar configuración y estados de firewall entre los servidores de seguridad primaria y secundaria.

Determinar asignaciones de dirección IP

En primer lugar usted necesita para planificar sus asignaciones de direcciones IP. Una buena estrategia es utilizar el IP bajo utilizable en
la subred que la IP CARP, el siguiente IP posterior como interfaz IP del servidor de seguridad primaria, y el siguiente IP como interfaz IP del servidor de seguridad secundario. Puede asignar estos como se desee, por lo que la elección de un esquema que
que tiene más sentido para usted, se recomienda.

WAN Dirigiéndose

Las direcciones WAN serán seleccionados de los asignados por su ISP. Para el ejemplo de la tabla 24.1, "Asignaciones de direcciones WAN IP", la WAN de la pareja CARP está en una red privada, y la direcciones 10.0.66.10 10.0.66.12 través se utilizarán como la WAN IPs.

Tabla 24.1. Asignaciones de dirección IP WAN

Dirección IP	Uso
10.0.66.10	CARP compartió IP
10.0.66.11	Firewall primaria WAN IP
10.0.66.12	Firewall Secondary IP WAN

LAN Direccionamiento

La subred LAN es 192.168.1.0/24. Para este ejemplo, la LAN IPs se asignará como se muestra en Tabla 24.2, "Asignación de direcciones IP de la LAN".

Tabla 24.2. Asignaciones de direcciones IP de la LAN

Dirección IP	Uso

192.168.1.1	CARP compartió IP
192.168.1.2	Firewall Primaria LAN IP
192.168.1.3	Firewall Secondary LAN IP

pfsync Dirigiéndose

No habrá IP CARP compartida en esta interfaz porque no hay necesidad de uno. Estas direcciones IP están utilizado sólo para la comunicación entre los servidores de seguridad. Para este ejemplo, voy a utilizar 172.16.1.0/24 como la
subred pfsync. Se utilizarán sólo dos IPs, pero voy a utilizar un / 24 para ser coherente con la otra interna interfaz (LAN). Para el último octeto de la dirección IP, elegí el mismo último octeto como el firewall de IP LAN para mantener la coherencia.

Tabla 24.3. Asignaciones de direcciones IP pfsync

Dirección IP	Uso
172.16.1.2	Firewall Primaria LAN IP
172.16.1.3	Firewall Secondary LAN IP

En la Figura 24.1, "Ejemplo de diagrama de red CARP" 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 una cable cruzado entre ellos para conectar las interfaces pfsync. En este ejemplo básico, el conmutador WAN y el interruptor de LAN son todavía posibles puntos de fallo. Redundancia de conmutación se describe más adelante en este capítulo en la sección llamada "Capa 2 Redundancia".

Configure el firewall primario

En primer lugar vamos a tener todo funciona como se desea en el primario, el secundario se agregará. Deja el firewall secundario apagado hasta que se llega a ese punto.

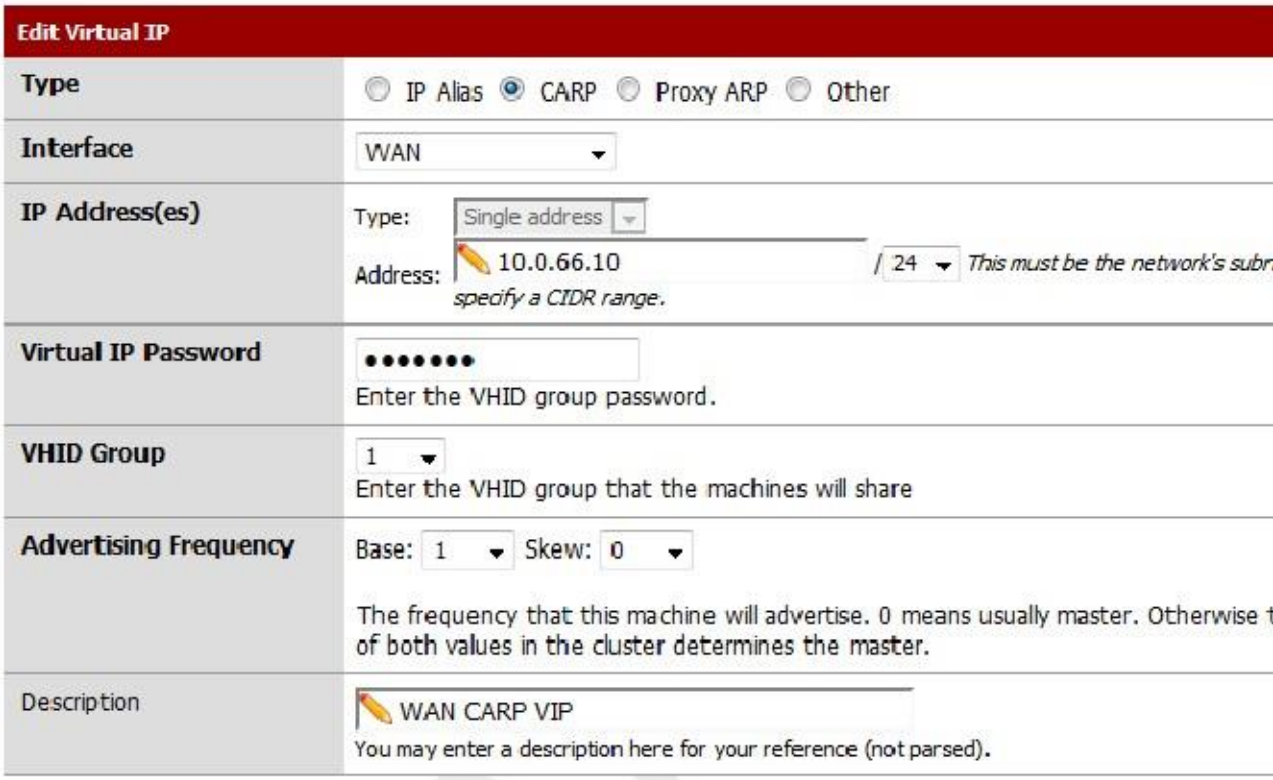
Instalación, misiones interfaz y configuración básica

Ir a través de la instalación y asignación de interfaces de manera diferente que si se tratara de una instalación única. Asigne la dirección IP designada previamente a la interfaz LAN, y acceder a la interfaz web para continuar. Ir a través del asistente de configuración, seleccionar la zona horaria, la configuración de la IP estática previamente
designado para el firewall primario en la WAN, y el establecimiento de la contraseña de administrador. Continuar a la siguiente paso después de completar el asistente de configuración (refiérase a la sección llamada "Asistente de configuración" en caso necesario).

Configuración de las direcciones IP virtuales CARPA

Vaya a Cortafuego IPs virtuales y clickto añadir la primera VIP CARP. La edición de IP virtual Aparecerá la pantalla, como se ve en la Figura 24.2, "WAN IP CARP"

Figura 24.2. WAN IP CARP



Para el tipo, seleccione CARP. La interfaz se debe establecer en WAN. Para la Dirección IP, introduzca en el compartido Dirección IP WAN elegido anteriormente. En este ejemplo, es 10.0.66.10. Asegúrese de que la máscara de subred para que la dirección coincide con la máscara de subred para la interfaz, 24. La IP Contraseña virtual puede ser lo te gusta, y siempre que todos sus sistemas utilizan pfSense con su sincronización de la configuración, usted nunca necesitará saber esta contraseña, ya que se sincronizará automáticamente con el servidor de seguridad secundario. Usted puede
generar una contraseña aleatoria utilizando una herramienta de generación de clave o explosión al azar en el teclado para crear una. Cada IP CARP en un par de servidores de seguridad debe utilizar un grupo VHID única (Host virtual Identificación), y también debe ser diferente de cualquier VHIDs en uso activo en cualquier red conectada directamente interfaz si CARP o VRRP también está presente en otros routers o cortafuegos de su red. Si usted tiene ningún otro CARP o VRRP tráfico presente en su red, puede comenzar a 1. De lo contrario, ponerlo en la próxima VHID disponible en su red. Se debe establecer el valor de frecuencia de Publicidad para Skew de acuerdo a la función de esta máquina en el grupo. Dado que ésta será maestro, se debe establecer en 0. En el sistema de copia de seguridad, este debe ser 1o superior. La Base normalmente se puede dejar en el valor predeterminado de 1, pero en
algunas redes, tales como aquellos con alta latencia entre nodos, una base más alta puede hacer que la conmutación por error
proceso más tolerante, aunque se necesitará más tiempo de conmutación por error que se produzca. Para la descripción, escriba algo
pertinente, como WAN IP CARP. Haga clic en Guardar cuando haya terminado.
Ahora clickto añadir otra IP virtual para la LAN (Figura 24.3, "LAN CARP IP"). Esta vez, establecer Escriba a CARP, Interfaz a LAN, y la dirección IP a la LAN IP compartida, 192.168.1.1 y el CIDR a 24. Esta Virtual IP contraseña es para un grupo de IP diferente, por lo que no tiene que coincidir con el de WAN, y otra vez que nunca necesitará saber esta contraseña. El VHID debe ser diferente de la que de la WAN CARP IP, normalmente se establece un número más alto, en este caso 2. Una vez más, ya que este sistema es dueño del Skew Frecuencia La publicidad debe ser 0. Para la descripción, escriba LAN CARP IP o algo similar descriptiva. Haga clic en Guardar cuando haya terminado.

Después de guardar el CARP LAN IP, verá ambas personalidades en la lista, como en la Figura 24.4, "lista de IP virtual". Haga clic en Aplicar cambios y luego ambos IPs carpa estarán activos.

Configure NAT saliente para CARP

El siguiente paso será configurar NAT para que los clientes de la LAN utilizarán la WAN IP compartida como Dirección. Vaya a Cortafuego NAT, y haga clic en la ficha de salida. Seleccione la opción de habilitar Manual NAT de salida (Outbound avanzada NAT), a continuación, haga clic en Guardar.

Una regla aparecerá que le NAT el tráfico de su LAN a la WAN IP. Puede ajustar esta norma a trabajar con la dirección IP CARP lugar. Haga clic theTo la derecha de la regla. En la sección de traducción, seleccione la dirección IP WAN del CARP Dirección desplegable. Cambie la descripción por mencionar que esta regla NAT LAN a la WAN CARP. Como referencia, puede comparar su salida Configuración de las reglas de NAT a los de la Figura 24.5, "Entrada NAT Saliente"

Después de hacer clic en Guardar en la regla de NAT, y luego haga clic en Aplicar cambios, nuevas conexiones de salir de la WAN ahora será traducido a la IP CARP. Puede confirmar esto con un sitio web que muestra el Desde el que se lo está accediendo la dirección IP, como http://www.pfsense.org/ip.php.

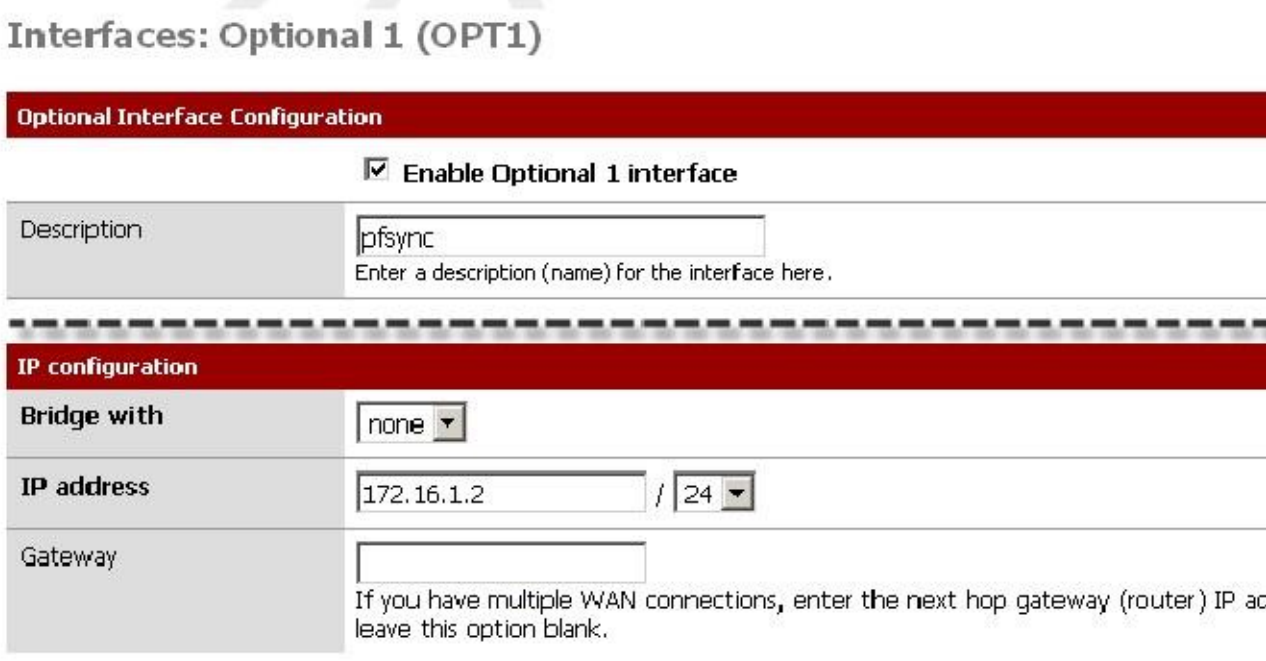
También debe ver la configuración de la regla de NAT saliente correctamente en la lista, como en la Figura 24.6, "Avanzada Configuración NAT saliente ".

Configure pfsync

La siguiente tarea es configurar la interfaz pfsync que será la línea de comunicación entre el firewall primario y de reserva. Navegue hasta Interfaces OPT1 instalar esto. Si usted no tiene una interfaz OPT1 embargo, tendrá que asignarle bajo Interfaces (Asignar) (véase la sección de nombre "Asignación de las interfaces").

Sólo unas pocas opciones se deben establecer, como se muestra en la Figura 24.7, "Configuración de la interfaz pfsync". La interfaz debe estar habilitado, y que ayudaría a utilizar pfsync por su nombre. Se debe ajustar para una estática IP, y se le dio la dirección decidida anteriormente para el lado primario del pfsync, 172.16.1.2/24.

Figura 24.7. Configuración de la interfaz pfsync



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 a Firewall Reglas y haga clic en la pestaña pfsync. Añadir una nueva regla de firewall que permitan el tráfico de cualquier protocolo de cualquier

origen a cualquier destino. Dado que esto sólo será una conexión privada directa con un cable cruzado, es seguro para permitir todo el tráfico desde el par pfsync.

Modificación del Servidor DHCP

Si pfSense está actuando como un servidor DHCP, es necesario instruir a asignar una IP CARP como la puerta de enlace IP.
De lo contrario pfSense hará uso de su comportamiento por defecto de la asignación de la IP configurada en la interfaz como la
puerta de enlace. Eso IP es específico para el firewall primario, por lo que necesita para cambiar a una IP CARP para conmutación por error
a trabajar para los sistemas cliente DHCP.

Vaya a Servicios DHCP Server. Cambie el campo Puerta de entrada a 192.168.1.1, CARP compartida IP LAN. Establezca la IP de pares de conmutación por error a la actual IP LAN del sistema de copia de seguridad, 192.168.1.3. Este
permitirá que el servicio DHCP en ambos sistemas para mantener un conjunto común de arrendamientos.

Guardar, y aplicar los cambios.

Configuración del servidor de seguridad secundaria

A continuación, las interfaces, las direcciones IP y las reglas de firewall en la necesidad secundaria a configurarse.

Asignación de interfaz y de direccionamiento IP

Antes de enchufar la WAN, LAN, o las interfaces pfsync, encienda el sistema y pasar por el instalación y asignación de interfaz como lo hizo para el firewall primario. Establezca la IP LAN de la consola para la copia de seguridad inalámbrica IP previamente designada de 192.168.1.3, establecer la configuración de DHCP del
igual que la primaria, y luego debe ser seguro para enchufar las conexiones de red.

A continuación, debe iniciar sesión en la interfaz web y pasar por el asistente de configuración, tal y como se hizo en el primaria. Configure la IP WAN, y establecer la contraseña de administrador para el mismo valor que en el primario.

También tendrá que configurar la interfaz de sincronización, como en la sección llamada "Configurar pfsync", pero con la dirección IP elegida para el sistema de copia de seguridad

Las reglas de firewall

Usted necesitará una regla de firewall temporalmente para permitir la sincronización de la configuración inicial ocurra. Ir a Firewall
 Reglas y haga clic en la pestaña pfsync. Añadir una nueva regla de firewall que permitan el tráfico de cualquier protocolo de
cualquier origen a cualquier destino. Ponga "temp" en la descripción de lo que puede estar seguro de que ha sido reemplazado
más tarde. La regla debe ser similar a la Figura 24.8, "regla del cortafuegos en la interfaz pfsync"

Figura 24.8. Regla de firewall en la interfaz pfsync

Configuración de la sincronización de configuración

En el servidor de seguridad de copia de seguridad, vaya a Firewall IPs virtuales y haga clic en la ficha Configuración del CARP. Comprobar
Sincronización activada, elija pfsync como la Interfaz Sincronizar, y para la sincronización de pares pfsync IP, escriba la dirección IP para la interfaz pfsync del sistema primario, 172.16.1.2. Haga clic en Guardar cuando terminado. No coloque ningún otro valor en esta página.

El último paso es configurar la sincronización de la configuración entre el primario y el de respaldo. En el maestro único firewall, vaya a Firewall IPs virtuales y haga clic en la ficha Configuración del CARP.

Compruebe Sincronizar Habilitado y encontrarás pfsync como la interfaz Sincronizar. Para la sincronización pfsync pares IP, escriba la dirección IP para la interfaz pfsync del sistema de copia de seguridad, 172.16.1.3. Revise toda la restante cajas en la pantalla, e introduzca pfsync IP del sistema de copia de seguridad de nuevo en Sincronizar para IP. Por último, introduzca la contraseña de administrador WebGUI en el cuadro Contraseña del sistema remoto. Haga clic en Guardar cuando terminado.

Cuando los ajustes de sincronización se guardan en el primario, se copiará automáticamente los ajustes de la primaria a la copia de seguridad para cada opción seleccionada en la página Configuración del CARP. Esto incluye la configuración de NAT salientes adecuados para CARP, las reglas de firewall para la interfaz pfsync, e incluso la VIPs CARP. Dentro de los 30 segundos, la sincronización de la configuración inicial debería haber terminado.

La configuración del servidor DHCP no están sincronizadas, lo que los cambios en el sistema de copia de seguridad será necesario para establecer la IP CARP como puerta de entrada, y para usar la dirección IP de LAN del principal como la conmutación por error de DHCP pares, como en la sección denominada "Modificación del servidor DHCP".

Si los ajustes sincronizados desde la primaria hasta la copia de seguridad, entonces usted sabe que la interfaz de sincronización es conectado y funciona correctamente. Si no, usted puede ir a Diagnósticos Ping, escoja la interfaz pfsync, y el intento de hacer ping a la dirección IP pfsync del sistema de oposición. Si eso no funciona, compruebe que usted está usando un cable cruzado y / o tiene una luz de enlace en la interfaz pfsync de ambos sistemas.

La pareja CARP ahora estará activo, pero todavía tendrá que comprobar el estado y comprobar que la conmutación por error es funciona correctamente. Salte a la sección "Verificación de conmutación por error de Funciones" para el resto.

> Nota
>
> Usted debe no sincronización de la configuración de instalación desde el servidor de seguridad de copia de seguridad al maestro firewall. Hay protecciones que deberían impedir este bucle de sincronización de causar daño, pero va a saturar sus registros con mensajes de error y nunca debe ser configurado este manera.

Multi-WAN con CARP

También puede desplegar CARP para redundancia de firewall en una configuración multi-WAN, siempre y cuando todos sus Interfaces WAN tienen al menos 3 IPs estáticas cada uno. En esta sección se detalla la configuración VIP y NAT necesaria para un despliegue CARP WAN dual. En este apartado sólo se tratan temas específicos de CARP y multi-WAN.

Determinar asignaciones de dirección IP

Para este ejemplo, cuatro direcciones IP se usarán en cada WAN. Cada servidor de seguridad necesita una IP, más uno CARP IP para NAT de salida, más uno para un NAT 01:01 que se utilizará para un servidor de correo interno en el Segmento de DMZ.

WAN y WAN2 direccionamiento IP

Tabla 24.4, "WAN IP Direccionamiento" y la Tabla 24.5, "WAN2 direccionamiento IP" mostrar frente a la IP para ambas redes WAN. En la mayoría de los entornos de estos serán IPs públicas.

Tabla 24.4. WAN direccionamiento IP

Dirección IP	Uso
10.0.66.10	IP CARP compartido para NAT de salida
10.0.66.11	Firewall primaria WAN IP

10.0.66.12	Firewall Secondary IP WAN
10.0.66.13	IP CARP compartido para NAT 01:01

Tabla 24.5. WAN2 direccionamiento IP

Dirección IP	Uso
10.0.64.90	IP CARP compartido para NAT de salida
10.0.64.91	Firewall Primaria WAN2 IP
10.0.64.92	Firewall Secondary WAN2 IP
10.0.64.93	IP CARP compartido para NAT 01:01

LAN Direccionamiento

La subred LAN es 192.168.1.0/24. Para este ejemplo, la LAN IP se asigna de la siguiente manera.

Tabla 24.6. Asignaciones de direcciones IP de la LAN

Dirección IP	Uso
192.168.1.1	CARP compartió IP
192.168.1.2	Firewall Primaria LAN IP
192.168.1.3	Firewall Secondary LAN IP

DMZ Dirigiéndose

La subred DMZ es 192.168.2.0/24. Para este ejemplo, la LAN IPs se asignará de la siguiente manera en Tabla 24.7, "Asignación de direcciones IP DMZ".

Tabla 24.7. Asignaciones de direcciones IP DMZ

Dirección IP	Uso
192.168.2.1	CARP compartió IP
192.168.2.2	Primaria firewall DMZ IP
192.168.2.3	Secundaria firewall DMZ IP

pfsync Dirigiéndose

No habrá IP CARP compartida en esta interfaz porque no hay necesidad de uno. Estas direcciones IP están utilizado sólo para la comunicación entre los servidores de seguridad. Para este ejemplo, 172.16.1.0/24 se utilizará como la subred pfsync. Se utilizarán sólo dos IPs, pero a / 24 se utiliza para ser coherente con la otra interna interfaces. Para el último octeto de las direcciones IP, se elige el mismo último octeto como LAN IP de dicho servidor de seguridad
para mantener la coherencia.

Tabla 24.8. Asignaciones de direcciones IP pfsync

Dirección IP	Uso
172.16.1.2	Firewall Primaria LAN IP
172.16.1.3	Firewall Secondary LAN IP

Configuración de NAT

La configuración de NAT al utilizar CARP es lo mismo que sin él, aunque es necesario utilizar sólo VIPs carpa, o IPs públicas en una subred enrutada a uno de sus IPs CARP para asegurar estas direcciones

son siempre accesibles. Consulte el Capítulo 11, Network Address Translation para más información sobre NAT configuración.

Configuración del cortafuegos

Con Multi-WAN necesita una política para la red local a la ruta a la puerta de enlace predeterminada de otro modo cuando intenta enviar tráfico a la dirección CARP será en lugar de salir de una WAN secundaria conexión.

Es necesario añadir una regla en la top de las reglas de firewall para todas las interfaces internas que dirigirán el tráfico para todas las redes locales a la puerta de enlace predeterminada. La parte importante es la puerta de entrada tiene que ser por defecto 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 LAN local, o un alias que contiene todas las redes localmente alcanzables.

Multi-WAN CARP con DMZ Diagrama

Debido a los elementos adicionales WAN y DMZ, un diagrama de este diseño es mucho más complejo como se puede ver en la Figura 24.9, "Diagrama de multi-WAN CARP con DMZ".

Comprobación de la funcionalidad de conmutación por error

Dado que el uso CARP es sobre la alta disponibilidad, debe ser probado a fondo antes de ponerse en producción. La parte más importante de esta prueba es asegurarse de que los compañeros CARP se failover con gracia durante las interrupciones del sistema.

Si las acciones de esta sección no funcionan como se esperaba, consulte la sección "Solución de problemas CARP".

Comprobar el estado de CARP

En ambos sistemas, vaya al Estado CARP (failover). El principal debe mostrar MAESTRO para el estado de todos los VIPs CARP. El sistema de copia de seguridad debe mostrar copia de seguridad como el estado. Si la copia de seguridad
sistema en lugar muestra MINUSVALIDOS, haga clic en el botón Activar CARP y, a continuación, actualice el Estatuto
CARP página (failover). Ahora debería aparecer correctamente.

Comprobación de la configuración de replicación

Vaya a lugares clave en el enrutador de respaldo, tales como Firewall Reglas y Firewall NAT y garantizar que las normas creadas sólo en el sistema principal se replican en las copias de seguridad.

Si ha seguido el ejemplo anterior de este capítulo, usted debe ver que su "temp" regla de firewall en la interfaz pfsync ha sido sustituido por el imperio de la primaria.

Compruebe DHCP Failover Estado

Si ha configurado con DHCP, su estado se puede comprobar visitando Estado Concesiones DHCP.
Una nueva sección aparecerá en la parte superior de la página que contiene el estado del conjunto DHCP de conmutación por error, como
En la Figura 24.10, "DHCP Failover piscina de estado".

Figura 24.10. DHCP Failover Piscina Estado

Failover Group	My State	Since	Peer State	Since
"dhcp0"	normal	2009/07/21 16:33:03	normal	2009/07/21 1

CARP prueba de conmutación por error

Ahora, para la prueba de conmutación por error real. Antes de empezar, asegúrese de que se puede navegar desde un cliente detrás de la
Par CARP con ambos firewalls pfSense en línea y funcionando. Una vez que se confirma al trabajo, lo haría ser un excelente momento para hacer una copia de seguridad.

Para la prueba en sí, desenchufe el principal de la red o apagarlo. Usted debe ser capaz de mantener navegar por Internet a través del router de respaldo. Comprobar estado CARP (failover) de nuevo en la copia de seguridad
y ahora debe informar de que es maestro 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 la copia de seguridad sistema debe degradarse a sí mismo una copia de seguridad una vez más, y la conectividad a Internet debería funcionar adecuadamente.

Se debe probar el par CARP en tantas situaciones de error posible. Algunas otras pruebas individuales puede incluir:

- Desconecte el cable WAN o LAN
- Saque el enchufe de alimentación de la primaria
- CARP Desactivar en la primaria
- Prueba con cada sistema individual (copia de seguridad de apagado, entonces el poder de nuevo y cerró la primaria)
- Descargar un archivo o probar el streaming de audio / vídeo durante la conmutación por error
- Pruebe con un ping continuo a un host de Internet durante la conmutación por error

Proporcionar redundancia Sin NAT

Como se mencionó anteriormente, sólo VIP CARP proporcionan redundancia y sólo pueden ser utilizados en conjunción con NAT. También puede proporcionar redundancia para las subredes IP públicas enrutados con CARP. En esta sección describe este tipo de configuración, que es común en redes grandes, ISP y ISP inalámbrico redes y entornos de co-localización.

Asignación IP públicas

Usted necesitará por lo menos un bloque de IP pública / 29 para el lado WAN de pfSense, que ofrece seis utilizable Direcciones IP. Sólo tres son necesarios para un despliegue de dos firewall, pero esta es la subred IP más pequeña que se acomoda a tres direcciones IP. Cada servidor de seguridad requiere de una dirección IP, y que necesita por lo menos un
VIP CARP en el lado WAN.

La segunda subred IP pública se dirigirá a uno de tus VIPs CARP por su ISP, co-location proveedor o el router de salida si controlas la parte de la red. Debido a que esta subred es siendo enrutada a un VIP CARP, el enrutamiento no será dependiente de un único servidor de seguridad. Para el representado
Ejemplo de configuración en este capítulo, una subred IP pública / 23 será utilizado y se divide en subredes en dos / 24 redes.

Descripción general de la red

La red de ejemplo representado aquí es un entorno de co-ubicación que consta de dos instalaciones pfSense con cuatro interfaces de cada uno - WAN, LAN, DBDMZ y pfsync. Esta red contiene un número de Web y los servidores de base de datos. No se basa en ninguna red real, pero hay un sinnúmero de producción despliegues similares a este.

WAN Red

La WAN es donde la red se conecta a la red aguas arriba, ya sea con su ISP, co-location proveedor o el router de salida.

LAN Red

LAN en pfSense es un nombre de interfaz fija, y es una interfaz requerida en el punto 1.2. LAN no es una nombre apropiadamente descriptivo para este segmento en esta implementación. El segmento de LAN en esta red contiene servidores web, y se describe más apropiadamente como una DMZ o segmento de servidores web, pero será LAN aquí debido a esta restricción. Es posible que desee añadir un quinto interfaz para los servidores de seguridad
en esta circunstancia, y dejar la interfaz asignada como LAN desenchufado por lo que sus interfaces tienen más nombres descriptivos. pfSense 2.0 permite cambiar el nombre de la interfaz LAN, así que esto no será una consideración en el futuro. Frecuentes VLAN se utilizan en este tipo de implementaciones, en cuyo caso se puede asignar una VLAN no utilizado a la LAN, y el uso de una interfaz OPT apropiado nombre para esta red interna, en lugar de LAN.

DBDMZ Red

Este segmento es una interfaz OPT y contiene los servidores de bases de datos. Es común para segregar la web y servidores de bases de datos en dos redes en entornos de alojamiento. Los servidores de bases de datos nunca debe requerir el acceso directo a través de Internet, y por lo tanto están menos sujetos a compromiso de sus servidores web.

pfsync Red

La red pfsync en este diagrama se utiliza para replicar los cambios de configuración pfSense vía XML RPC y para pfsync replicar cambios de la tabla de estado entre los dos servidores de seguridad. Como se ha descrito anteriormente en este
capítulo, se recomienda una interfaz dedicada para este fin.

Layout Red

Figura 24.11, "Diagrama de CARP con enrutado IPs" ilustra este diseño de la red, incluyendo todos los direcciones IP disponibles, una LAN y DMZ Database.

Nota

Los segmentos que contienen los servidores de base de datos típicamente no tienen que ser accesibles al público, y
por lo tanto, sería más común utilizar subredes IP privadas, pero el ejemplo que se ilustra aquí puede ser utilizado independientemente de la función de las dos subredes internas.

Capa 2 de redundancia

Los diagramas anteriores en este capítulo no describieron la capa 2 (interruptor) de redundancia, para evitar que se produzca
demasiados conceptos a los lectores de forma simultánea. Ahora que tiene una comprensión de hardware redundancia con pfSense, esta sección cubre la capa 2 elementos de diseño que debe considerar al la planificación de una red redundante. En este capítulo se asume un despliegue de dos sistemas, aunque esto se escala para
el mayor número de instalaciones en lo que usted requiere.
Si los dos sistemas redundantes pfSense estén enchufados en el mismo interruptor en cualquier interfaz, que el interruptor se convierte en un punto único de fallo. Para evitar este único punto de fallo, la mejor opción es el despliegue de dos interruptores para cada interfaz (que no sea la interfaz pfsync dedicado).

El diagrama de enrutado IP es centrada en la red, no se muestra la infraestructura de conmutación. La Figura 24.12, "Diagrama de CARP con conmutadores redundantes" ilustra cómo ese entorno se ve con una redundante cambiar la infraestructura.

Configuración de conmutación

Al utilizar múltiples conmutadores, debe interconectarlos. Siempre y cuando usted tiene una conexión única entre los dos interruptores, y no superar en cualquiera de los servidores de seguridad, esto es seguro con cualquier tipo de cambiar. Cuando el uso de puentes, o donde existen múltiples interconexiones entre los interruptores, la atención se debe tomar para evitar bucles de Capa 2. Usted necesitará un switch administrado que es capaz de utilizar Spanning Tree Protocol (STP) para detectar y bloquear puertos que de otro modo crear bucles de conmutación. Al utilizar STP, si un enlace activo muere, por ejemplo, cambiar el fracaso, a continuación, un enlace de respaldo puede automáticamente ser educado
en su lugar.

En pfSense 2.0, también se añadirá soporte para el `lagg (4)` agregación de enlaces y la interfaz de enlace de conmutación por error
que también le permiten tener varias interfaces de red conectadas a uno o más conmutadores para más tolerancia a fallos.

Anfitrión de redundancia

Es más difícil de obtener redundancia de acogida para sus sistemas críticos dentro del firewall. Cada sistema podría tener dos tarjetas de red y una conexión a cada grupo de interruptores utilizando agregación de enlaces Control Protocol (LACP) o la funcionalidad específica del proveedor similar. Los servidores también pueden tener múltiples
conexiones de red, y en función del sistema operativo que puede ser capaz de ejecutar CARP en un conjunto de servidores por lo que
que serían redundantes también. Proporcionar redundancia de acogida es más específica a las capacidades de los interruptores y el sistema operativo del servidor, que está fuera del alcance de este libro.

Otros puntos de fallo

Cuando se trata de diseñar una red totalmente redundante, hay muchos puntos de fallo que a veces conseguir perdido. Dependiendo del nivel de tiempo de actividad que se espera lograr, hay más y más cosas a considerar que un fracaso simple interruptor. Aquí hay algunos ejemplos más de la redundancia en un escala más amplia:

- Cada segmento redundante debe tener potencia aislada.
- Los sistemas redundantes deben estar en los interruptores separados.
- Los bancos utilizan múltiples UPS / generadores.
- Utilice varios proveedores de energía, entrando en lados opuestos del edificio siempre que sea posible.
- Incluso una configuración multi-WAN no es garantía de tiempo de actividad de Internet.
- Utilizar múltiples tecnologías de conexión a Internet (ADSL, Cable, T1, Fibra, Wireless).
- Si alguno de los dos transportistas utilizan la misma / túnel / path polo, ambos podrían ser eliminados al mismo tiempo.
- Tener enfriamiento de respaldo, enfriadores redundantes o un aire acondicionado portátil / emergencia.
- Considere la posibilidad de la colocación de la segunda serie de equipos redundantes en otra habitación, otro piso, u otra edificio.
- Tener una configuración duplicada en otra parte de la ciudad o en otra ciudad. ¿Por qué comprar uno cuando usted puede comprar dos por el doble del precio?
- Escucho alojamiento es barato en Marte, pero la latencia es asesino.

CARP con Bridging

CARP no es actualmente compatible con puente en una capacidad nativa. Se requiere una gran cantidad de manuales intervención. Los detalles del proceso se pueden encontrar en la sección llamada "CARP".

CARP Solución de problemas

CARPA es una tecnología muy compleja, y con tantas formas diferentes para configurar un clúster de conmutación por error,
puede ser difícil para que las cosas funcionen correctamente. En esta sección, algunas comunes (y no tan común) problemas serán discutidos y resueltos con suerte para la mayoría de los casos. Si sigue teniendo problemas después de leer esta sección, hay un tablero CARPA / VIPs dedicado en el pfSense Forum [http://forum.pfsense.org / index.php / tabla, 36.0.html].

Antes de ir mucho más lejos, tómese el tiempo para comprobar todos los miembros del clúster CARP para garantizar que se
tener configuraciones coherentes. A menudo, ayuda a caminar a través de la configuración de ejemplo, doble control de todos
de los ajustes adecuados. Repita el proceso en los miembros de copia de seguridad, y esté pendiente de los lugares donde la configuración debe ser diferente en las copias de seguridad. Asegúrese de comprobar el estado de la carpa (la sección llamado "Comprobar el estado CARP") y asegúrese de CARP está habilitado en todos los miembros del clúster.
Errores relacionados con CARP se registrarán en Estado Registros del sistema, en la ficha Sistema. Compruebe los registros en cada sistema involucrado para ver si hay algún mensaje relacionados con sincronización XMLRPC, estado CARP
transiciones, u otros errores relacionados.

Errores de configuración comunes

Hay tres configuraciones erróneas muy comunes que suceden que impiden CARP de trabajo adecuadamente.

Utilice un VHID diferente en cada VIP CARP

A VHID diferente se debe utilizar en cada VIP CARP que cree. Por desgracia, no siempre es tan sencilla. CARPA es una tecnología multicast, y como tal, cualquier cosa usando CARP en la misma red segmento debe utilizar un VHID único. VRRP también utiliza un protocolo similar al CARP, por lo que también debe garantizar que no existan conflictos con VRRP VHIDs, como si su proveedor u otro router en su red utiliza VRRP.

La mejor forma de evitar esto es utilizar un conjunto único de VHIDs. Si usted está en una red privada conocida seguro, iniciar la numeración en 1. Si usted está en una red donde VRRP o CARP son contradictorios, es posible que tenga que consultar con el administrador de la red para encontrar un bloque libre de VHIDs.

Horas incorrectas

Compruebe que todos los sistemas implicados se sincronizan correctamente sus relojes y tienen zonas horarias válidas, especialmente si se ejecuta en una máquina virtual. Si los relojes están demasiado separados, tareas poco de sincronización
como DHCP de conmutación por error no funcionará adecuadamente.

Máscara de subred incorrecta

Debe utilizar la máscara de subred real para un VIP CARP, no / 32. Debe coincidir con la máscara de subred la dirección IP de la interfaz a la que está asignada la IP CARP.

Dirección IP para CARP Interface

La interfaz en la que reside el IP CARP ya deben tener otra IP definida directamente en el interfaz (VLAN, LAN, WAN, OPT) antes de que pueda ser utilizado.

Hash incorrecta Error

Hay algunas razones por las que este error puede surgir en los registros del sistema, algunos más preocupante que otros.

Si CARP no funciona correctamente cuando vea este error, puede ser debido a una falta de coincidencia de configuración.
Asegúrese de que para un VIP dado, que el VHID, contraseña y dirección IP / máscara de subred, coincidan.
Si la configuración parece ser adecuada y CARP aún no funciona mientras se genera este mensaje de error, entonces puede haber varias instancias de la carpa en el mismo dominio de difusión. Puede que tenga que desactivar CARP y monitorear la red con tcpdump (Capítulo 29, Captura de paquetes) para comprobar si hay otros CARP o el tráfico-CARP similar, y ajustar sus VHIDs adecuadamente.

Si CARP funciona correctamente, y ves este mensaje cuando el sistema arranca, puede ser en cuenta. Es normal que este mensaje sea visto durante el arranque, siempre y cuando CARP sigue función correctamente (espectáculos primario maestro, copia de seguridad muestra de reserva para el estado).

Ambos sistemas aparecen como MAESTRO

Esto sucederá si la copia de seguridad no puede ver los anuncios de la carpa principal. Compruebe firewall reglas, problemas de conectividad, configuraciones del switch. También puedes ver los registros del sistema de los errores pertinentes
que podría conducir a una solución. Si usted está viendo esto en una máquina virtual (VM) de producto como ESX, consulte la sección titulada "Problemas en el interior de máquinas virtuales (ESX)".

Sistema principal se ha quedado atascado como ALTERNATIVA

En algunos casos, esto es que puede ocurrir normalmente durante unos 5 minutos después de que un sistema vuelve a la vida.
Sin embargo, ciertos errores de hardware o de otras condiciones de error pueden hacer que un servidor tome en silencio en un
alta advskew de 240 con el fin de señalar que todavía tiene un problema y no debe convertirse en maestro. Usted puede comprobar desde el shell o Diagnóstico , Comando.

```
#ifconfig carp0
carp0: flags = 49 <UP,LOOPBACK,RUNNING> mtu 1500
 inet 10.0.66.10 máscara de red 0xFFFFFF80
 carpas: RESPALDO vhid 1 advbase 1 advskew 240
```

En ese caso, usted debe aislar ese servidor de seguridad y llevar a cabo más pruebas de hardware.

Problemas dentro de máquinas virtuales (ESX)

Al utilizar CARP dentro de una máquina virtual, especialmente VMware ESX, algunas configuraciones especiales se necesitan para:

1. Activar el modo promiscuo en el conmutador virtual.

2. Habilitar "Los cambios de dirección MAC".

3. Activar "transmite forjados".

Además, hay un error en la funcionalidad de switch virtual de VMware, donde el tráfico de multidifusión se bucle volver al sistema de envío que múltiples tarjetas de red físicas están conectadas a un conmutador virtual. CARP hace No pase por alto este tipo de tráfico, ya que en una red que funciona normalmente, que nunca va a pasar, y lo ve como otro host que dice ser el maestro. De ahí que ambos cortafuegos siempre será atrapado en el modo de copia de seguridad.
Hay algunos parches que se están probando para proporcionar una solución alternativa para CARP en esta situación, y VMware
ha sido notificado del fallo vSwitch, por lo que puede no ser un problema en el futuro.

Configuración Problemas de sincronización

Verifique los siguientes puntos cuando se encuentran problemas con la sincronización de configuración:

• 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 de la copia de seguridad.

• La WebGUI debe estar en el mismo puerto en todos los nodos.

• La WebGUI debe estar usando el mismo protocolo (HTTP o HTTPS) en todos los nodos.

• Debe permitir el tráfico al puerto WebGUI en la interfaz que estás sincronizando a.

• La interfaz pfsync debe estar habilitado y configurado en todos los nodos.

• Retire todo caracteres especiales de todo tipo que estás sincronizando: reglas NAT, Firewall reglas, IPs virtuales, etc Esto ya no deberían ser un problema, pero en caso de tener dificultades, es una buena cosa para probar.

• Compruebe que sólo el nodo de sincronización principal tiene las opciones de sincronización habilitados.
• Asegúrese de ninguna dirección IP se especifica en el Sincronizar A IP en el nodo de copia de seguridad.

CARP y Multi-WAN Solución de problemas

Si tiene problemas para llegar a VIPs CARP desde cuando se trata de múltiples WAN, vuelva a comprobar que usted tener una norma como la que se menciona en la sección "Configuración del Firewall"

Extracción de un VIP CARP

Si necesita una IP CARP que ser eliminado por cualquier razón, el sistema host se debe reiniciar. Extracción una IP CARP desde un sistema en vivo puede dar lugar a una situación de pánico del kernel u otra inestabilidad del sistema. Más reciente
versiones de pfSense advertirán acerca de este hecho, y le pedirá que reinicie el sistema cuando una eliminación VIP CARP
se intenta.

Capítulo 25. Servicios

La base instalada de pfSense viene junto con un conjunto de servicios que tengan un poco de fundamental funcionalidad y flexibilidad para el sistema de servidor de seguridad. Como su nombre lo indica, las opciones que se encuentran dentro de
servicios de control de que el router proporcionará a los clientes, o en el caso de los servicios de enrutamiento, otros routers como
así. Estos servicios incluyen proporcionar DHCP direccionamiento, resolución de DNS y DNS dinámico, SNMP, UPnP y mucho más. Este capítulo cubre los servicios disponibles en el sistema base. Hay muchos
más servicios que se pueden agregar a los paquetes, los cuales serán cubiertos más adelante en el libro.

Servidor DHCP

El servidor DHCP asigna direcciones IP y las opciones de configuración relacionados a los PC cliente de la red. Está habilitado de forma predeterminada en la interfaz LAN, y con el default LAN IP 192.168.1.1, el valor predeterminado
rango de alcance sería 192.168.1.10 través 192.168.1.199. En su configuración por defecto, pfSense
asigna la IP LAN que la puerta de enlace y servidor DNS si el reenviador DNS está habilitada. Hay muchos opciones disponibles para ajustar en el WebGUI.

Configuración

Para modificar el comportamiento del servidor DHCP, vaya a Servicios DHCP Server. Desde allí se puede alterar la comportamiento del servidor DHCP, junto con las asignaciones de IP estáticas y algunas opciones relacionadas, como la estática ARP.

Elección de una interfaz

En la página de configuración de DHCP hay una ficha para cada interfaz no WAN. Cada interfaz tiene su propia configuración del servidor DHCP independiente, y pueden ser activados o desactivados independientemente uno otra. Antes de realizar cambios, asegúrese de que usted está buscando en la ficha de la interfaz de la derecha.

Opciones de servicio

La primera configuración en cada ficha dice pfSense si o no para manejar peticiones DHCP en la interfaz. Para habilitar DHCP en la interfaz, compruebe que el servidor DHCP Activar en [nombre] caja de interfaz. Para desactivar
el servicio, desmarque la misma caja.

Normalmente, el servidor DHCP responderá a las peticiones de cualquier cliente que solicite un contrato de arrendamiento. En la mayoría
entornos de este comportamiento es normal y aceptable, pero en ambientes más restringidos o seguras este comportamiento es indeseable. Con el Denegar desconocido conjunto de opciones de clientes, sólo los clientes con asignaciones estáticas
definida recibirán contratos de arrendamiento, lo cual es una práctica más segura, pero es mucho menos conveniente.

> **Nota**
>
> Esto protegerá contra los usuarios bajo el conocimiento y las personas que casualmente se enchufan en los dispositivos. Ser
> consciente, sin embargo, que un usuario con conocimiento de su red puede codificar una dirección IP, máscara de subred, puerta de enlace y DNS que todavía les dará acceso. También podrían alterar / suplantar la dirección MAC para que coincida con un cliente válido y todavía obtener una concesión. Siempre que sea posible,
> pareja esta configuración con las entradas ARP estáticas, control de acceso en un interruptor que limitará MAC direcciones a ciertos puertos de conmutación para una mayor seguridad y desactivar o deshabilitar los puertos de conmutación
> que se sabe que no debe estar en uso.

También se muestra la dirección IP de la interfaz que se está configurando, junto con su máscara de subred. Debajo esa línea del rango disponible de direcciones IP para que la máscara de subred se imprime, lo que puede ayudar a determinar
lo direcciones inicial y final a utilizar para la gama de pool de DHCP.

Rango de direcciones (DHCP Pool)

Las dos cajas para Range dicen pfSense lo que será la primera y la última dirección para su uso como un conjunto DHCP. La gama se debe ingresar con el número más bajo en primer lugar, seguido por el número más alto. Por ejemplo,

la gama de LAN DHCP por omisión se basa en la subred para la dirección IP de la LAN por defecto. Sería ser 192.168.1.10 a 192.168.1.199. Este rango puede ser tan grande o tan pequeño como su red necesita, pero debe ser completamente contenida dentro de la subred para la interfaz que se está configurando.

Servidores WINS

Dos servidores WINS (Windows Internet Name Service) pueden ser definidos que se transmite a los clientes. Si usted tiene uno o más servidores WINS disponibles, introduzca su dirección IP aquí. Los servidores reales hacen no tiene que ser en esta subred, pero asegúrese de que las reglas de enrutamiento y cortafuegos adecuados estén en su lugar para permitir que ellos puede llegar en los PC cliente. Si se deja en blanco, no hay servidores WINS se enviarán al cliente.

Servidores DNS

Los servidores DNS pueden o no necesitar rellenado, dependiendo de su configuración. Si está utilizando el DNS Forwarder integrado en pfSense para manejar DNS, deje estos campos en blanco y pfSense serán automáticamente asignará a sí mismo como servidor DNS para PC clientes. Si el reenviador DNS está desactivada y estos campos son deja en blanco, pfSense pasará en el que los servidores DNS se asignan en virtud del Sistema General Configuración. Si desea utilizar los servidores DNS personalizado en lugar de las opciones automáticas, rellene las direcciones IP para un máximo de dos servidores DNS aquí. (Consulte la sección "Contenido Abierto Filtrado con OpenDNS" para un ejemplo.) En redes con servidores Windows, especialmente los que utilizan Active Directory, es recomienda el uso de los servidores de DNS de cliente. Cuando se utiliza el reenviador DNS en combinación con CARP, especifique la IP en esta interfaz CARP aquí.

Entrada

La opción de puerta de enlace también se puede dejar en blanco si pfSense es la puerta de entrada para la red. En caso de que no ser el caso, escriba la dirección IP de la puerta de entrada a ser utilizado por los clientes en esta interfaz. ¿Cuándo utilizando CARP, rellene el IP CARP en esta interfaz aquí.

DHCP Lease tiempos

El tiempo predeterminado de arrendamiento y el control máximo tiempo de concesión de la duración de un contrato de arrendamiento de DHCP va a durar. El valor por defecto se utiliza el tiempo de concesión, cuando un cliente no solicita el tiempo de vencimiento específica. Si el cliente no especifica el tiempo que quiere un contrato de arrendamiento a la última, el ajuste máximo de tiempo de concesión le permitirá limitar eso a un razonable cantidad 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) durante el tiempo máximo.

Failover

Si este sistema es parte de una configuración de conmutación por error, como un racimo CARP, escriba la dirección IP del par de conmutación por error siguiente. Esta debe ser la dirección IP real del otro sistema en esta subred, no una dirección CARP compartida.

ARP estática

La Habilitar estática ARP entradas casilla funciona de manera similar a la negación de direcciones MAC desconocidas de obtención de contratos de arrendamiento, pero se lo lleva un paso más allá, ya que también limitaría cualquier máquina desconocido comunicándose con el enrutador pfSense. Esto dejaría de aspirantes a los que abusan de codificar alguna toma de salida abordar en esta subred, eludir restricciones de DHCP.

Nota

Al utilizar ARP estática, tenga cuidado para asegurarse de 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 la sistema que se utiliza para conectarse a la pfSense WebGUI.

DNS dinámico

Para la configuración de DNS dinámico, haga clic en el botón Opciones avanzadas a la derecha de ese campo. Para activar esta función, marque la casilla y luego rellenar un nombre de dominio para los nombres de host DHCP. Si está utilizando de pfSense

Reenviador DNS, es posible que en lugar de dejar esta opción en blanco y configurar la configuración interior del DNS configuración promotor.

Servidores NTP

Para especificar servidores NTP (Network Time Protocol Servidores), haga clic en el botón Opciones avanzadas a la derecha del
ese campo, e introduzca las direcciones IP de hasta dos servidores NTP.

De inicio de redes

Para ver la configuración de activar el arranque de red, haga clic en el botón Opciones avanzadas a la derecha de ese campo. Usted
puede comprobar a continuación, la casilla para activar la función, y luego ingrese una dirección IP desde la que arranca imágenes
están disponibles, y un nombre de archivo para la imagen de arranque. Ambos campos se deben configurar para la red arranque funcione correctamente.

Guardar configuración

Después de realizar estos cambios, asegúrese de hacer clic en Guardar antes de intentar crear asignaciones estáticas. La ajustes se perderán si se desplaza fuera de esta página sin guardar primero.

Asignaciones estáticas

Asignaciones DHCP estáticas permiten expresar una preferencia por la que se asigna la dirección IP a un
PC dado, basado en su dirección MAC. En la red, donde se les niega clientes desconocidos, esto también sirve como una lista de clientes "conocidos" que están autorizados para recibir contratos de arrendamiento o tiene entradas ARP estáticas. Estático
asignaciones se pueden añadir en una de dos maneras. En primer lugar, desde esta pantalla, haga clic y se le presentará con un formulario para agregar una asignación estática. El otro método consiste en añadir desde el punto de vista de arriendos DHCP,
que se describen más adelante en este capítulo.

De los cuatro campos de esta pantalla, sólo la dirección MAC es necesaria. Al participar sólo el MAC
dirección, ésta se añadirá a la lista de clientes conocidos para su uso cuando la opción Denegar clientes desconocidos es establecer. Hay un enlace al lado del campo de dirección MAC que copiar la dirección MAC del ser PC
utilizado para acceder a la WebGUI. Esto se proporciona para su conveniencia, en comparación con la obtención de la dirección MAC
en otras, más complejas, formas.

Nota

La dirección MAC se puede obtener a partir de un símbolo del sistema en la mayoría de las plataformas. En UNIX-
o basado en sistemas operativos UNIX-trabajo-por igual, incluyendo Mac OS X, si escribes "ifconfig -Un " mostrará la dirección MAC de cada interfaz. En las plataformas basadas en Windows, "ipconfig /
todos " mostrará la dirección MAC. La dirección MAC puede también a veces se encuentra en una pegatina en la tarjeta de red, o cerca de la tarjeta de red para los adaptadores integrados. Para los hosts de la misma subred, el MAC se puede determinar haciendo ping a la dirección IP de la máquina y luego funcionamiento "Arp-a".

El campo de dirección de IP es necesario si esta será una asignación de IP estática en lugar de sólo informar a la DHCP servidor que el cliente es válida. Esta dirección IP es realmente un preferencia, y no una reserva. Asignación de una Dirección IP aquí no va a evitar que alguien más utilizando la misma dirección IP. Si esta dirección IP se encuentra en utilizar cuando este cliente solicita un contrato de arrendamiento, será en cambio recibir una de la piscina general. Por esta razón,
el pfSense WebGUI no permite asignar asignaciones IP estáticas dentro de la agrupación de DHCP.

Un nombre de host también puede ser establecido, y no tiene que coincidir con el conjunto nombre real en el cliente. La nombre de host configurado aquí se puede utilizar al registrar direcciones DHCP en el reenviador DNS.

La descripción es cosmético, y disponible para su uso para ayudar a rastrear cualquier información adicional sobre esta entrada. Podría ser el nombre de la persona que utiliza el PC, su función, la razón por la que necesitaba una dirección estática o el administrador que añadió la entrada. También se puede dejar en blanco.

Haga clic en Guardar para terminar de editar la asignación estática y volver a la página de configuración del servidor DHCP.

Estado

Encontrará el estado del servicio de servidor DHCP en Estado Servicios. Si está habilitado, su el estado debe aparecer como correr, como en la Figura 25.1, "DHCP Servicio Daemon Estado". Los botones en el lado derecho le permiten reiniciar o detener el servicio del servidor DHCP. Reinicio Nunca debe haber necesaria como pfSense se reiniciará automáticamente el servicio cuando se realizan cambios de configuración que requerir un reinicio. Detener el servicio también es probable que nunca sea necesario, ya que el servicio se interrumpirá al desactivar todas las instancias del servidor de DHCP.

Figura 25.1. DHCP Servicio Daemon Estado

Service	Description	Status
dnsmasq	DNS Forwarder	Running
dhcpd	DHCP Service	Running

Arrendamientos

Puede ver los actuales contratos asignados a Diagnóstico Arriendos DHCP. Esta pantalla muestra el Dirección IP asignada, la dirección MAC se asigna a, el nombre de host (si lo hay) que el cliente envía como parte de la solicitud de DHCP, los tiempos de inicio y finalización del contrato de arrendamiento, si el equipo se encuentra actualmente en línea, y si el contrato de arrendamiento es activa, ha caducado, o de un registro estático.

Ver concesiones inactivas

Por defecto, sólo concesiones activas y estáticas se muestran, pero usted puede ver todo, incluyendo la vencida arrendamientos, haciendo clic en el botón Mostrar todos los arrendamientos configurado. Para reducir la vista de nuevo a normal, haga clic en el Salón concesiones activas y estática sólo botón.

Wake on LAN Integración

Si hace clic en la dirección MAC o la función Wake on LAN botón a la derecha del contrato de arrendamiento, pfSense se enviar un paquete Wake On LAN a ese host. Para más detalles acerca de Wake on LAN, consulte la sección llamada "Wake on LAN".

Añadir asignación estática

Para hacer un permiso dinámico en una asignación estática, haga clic en theTo el derecho del contrato de arrendamiento. Esto pre-fill la dirección MAC de ese host en la pantalla "Editar asignación estática". Usted tendrá que añadir la IP deseada dirección, nombre de host y la descripción y haga clic en Guardar. Cualquier arrendamientos existentes para esta dirección MAC será limpiado de los contratos de arrendamiento de archivo al guardar la nueva entrada.

Eliminar un contrato de arrendamiento

Mientras ve los contratos de arrendamiento, puede eliminar un arrendamiento inactiva o caducados manualmente haciendo clic en el botón en el extremo de una línea. Esta opción no está disponible para las concesiones activas o estáticas, sólo para fuera de línea o concesiones vencidas.

Bitácoras de Servicio DHCP

El demonio DHCP registrará su actividad al Estado Registros del sistema, en la ficha DHCP. Cada DHCP Se mostrarán solicitud y la respuesta, junto con otros mensajes de estado y de error.

DHCP Relay

Solicitudes DHCP se transmiten tráfico. El tráfico de difusión se limita a la dominio de difusión donde está iniciados. Si necesita proveer un servicio DHCP en un segmento de red sin un servidor DHCP, utilizar DHCP Relay para reenviar las solicitudes a un servidor definido en otro segmento. No es posible para ejecutar tanto un servidor DHCP y un relé DHCP en el mismo tiempo. Para activar el relé DHCP deberá desactivar primero el servidor DHCP en cada interfaz.

Una vez que el servidor DHCP está desactivado, visite Servicios DHCP Relay. Como con el servidor DHCP, hay es una ficha para cada interfaz. Haga clic en la interfaz en la que desea ejecutar el relé DHCP, marque la casilla junto a Activar relé DHCP en [nombre] de la interfaz, lo que también permitirá establecer otro opciones disponibles.

Si marca Append ID de circuito y el agente de ID a las solicitudes, el relé DHCP añadirá la identificación de circuito (Número de interfaz pfSense) y el ID de agente para la solicitud DHCP. Esto puede ser necesario por el DHCP servidor en el otro lado, o puede ayudar a distinguir dónde se originaron las solicitudes.

La opción para Proxy solicita al servidor DHCP en WAN subred hace exactamente lo que dice. Si se activa, pasará las peticiones DHCP de los clientes en esta interfaz para el servidor DHCP que asigna el IP frente a la interfaz WAN. Alternativamente, usted puede llenar en la dirección IP del servidor DHCP para que las solicitudes deberán proxy.

DNS Forwarder

El reenviador DNS en pfSense es un caché de resolución de DNS. Está habilitada de forma predeterminada y utiliza el DNS servidores configurados en el sistema Configuración general, o los obtenidos de su ISP para obtener dinámicamente interfaces WAN configurados (DHCP, PPPoE, PPTP y). Para conexiones IP WAN estática, debe

introducir los servidores DNS en el Sistema Configuración general o durante el asistente de configuración para el reenviador DNS
a funcionar. También puede utilizar los servidores DNS configurados estáticamente con configurada dinámicamente WAN
en el Sistema La página de configuración
interfaces desmarcando la casilla "Permitir que la lista de servidores DNS para ser anulado por DHCP / PPP en WAN" general.

En versiones anteriores, pfSense intentó inicialmente el primer servidor DNS configurado cuando se trata de resolver un Nombre DNS, y se trasladó a configurarse posteriormente servidores DNS si el primero no pudieron resolver. Este podría causar grandes retrasos si uno o más de los servidores DNS disponibles era inalcanzable. En pfSense 1.2.3 y más tarde este comportamiento se ha cambiado para consultar todos los servidores DNS de una sola vez, y el único de la primera
respuesta recibida se utiliza y se almacena en caché. Esto se traduce en un servicio DNS más rápido, y puede ayudar a suavizar
sobre los problemas que se derivan de los servidores DNS que son de forma intermitente lenta o que tienen una alta latencia.

Configuración DNS Forwarder

La configuración de reenviador DNS se encuentra en Servicios Forwarder DNS.

Habilitar reenviador DNS

Al marcar esta casilla se activa el reenviador DNS o desmarque si desea desactivar esta funcionalidad.

Registrarse arriendos DHCP en DNS forwarder

Si desea que sus nombres internos de la máquina para los clientes DHCP para resolver en DNS, marque esta casilla. Este sólo funciona en máquinas que especifican un nombre de host en sus peticiones DHCP.

Regístrese DHCP asignaciones estáticas en DNS forwarder

Esto funciona igual que el Registro de arriendos DHCP en la opción reenviador DNS, excepto que se registra las direcciones de asignación estática de DHCP.

Anfitrión anulaciones

La primera sección en la parte inferior de la pantalla reenviador DNS es el que puede especificar valores de reemplazo de DNS del servidor de resolución de nombres. Aquí usted puede configurar un nombre de host específico para resolver de manera diferente que
de otra manera sería a través de los servidores DNS utilizados por el reenviador DNS. Esto es útil para la división de DNS
configuraciones (véase la sección "DNS Split"), y como un medio semi-efectivas de bloqueo del acceso
a ciertos sitios web específicos.
Figura 25.2, "Ejemplo de anulación DNS" ilustra una anulación de DNS para un servidor web interno (Example.com y www.example.com), así como un ejemplo de bloquear el acceso a myspace.com y www.myspace.com.

Figura 25.2. Ejemplo Override DNS

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

Nota

No se recomienda utilizar estrictamente la funcionalidad de anulación de DNS como un medio de bloquear el acceso a ciertos sitios. Hay innumerables maneras de conseguir alrededor de esto. Dejará de carácter no técnico
usuarios, pero es muy fácil de recorrer para aquellos con aptitudes más técnico.

Anulaciones de dominio

Anulaciones de dominio se encuentran en la parte inferior de la pantalla de DNS reenviador. Esto le permite especificar un servidor DNS diferente a utilizar para la resolución de un dominio específico.

Un ejemplo de que esto es comúnmente desplegado en redes de pequeñas empresas con una sola interna servidor con Active Directory, por lo general de Microsoft Small Business Server. Las peticiones DNS para el Nombre de dominio de Active Directory debe ser resuelta por el Windows Server interno para Active Directory para funcionar correctamente. Adición de un reemplazo para el dominio de Active Directory que señala al interior La dirección IP del servidor de Windows asegura que estos expedientes se resuelven correctamente si los clientes están utilizando
pfSense como un servidor DNS o el propio Windows Server.

En un entorno de Active Directory, los sistemas siempre deben utilizar el servidor DNS de Windows como sus servidores DNS funciones de registro de nombres tan dinámicos primarios adecuadamente. En ambientes con sólo un servidor DNS de Windows, se debería permitir que el reenviador DNS con un reemplazo para su activo Del dominio del directorio y el uso pfSense como el servidor DNS secundario para sus máquinas internas. Este garantiza la resolución de DNS (a excepción de Active Directory) no tiene un único punto de fallo, y la pérdida del servidor único no significará un corte completo de Internet. La pérdida de un solo servidor en tal medio ambiente por lo general tiene consecuencias significativas, pero los usuarios se sentirá más inclinado a dejar en paz
para solucionar el problema si es que todavía pueden retirar sus lolcats, MySpace, Facebook, y otros en la media hora.

Otro uso común de las anulaciones de DNS es resolver dominios DNS internos en sitios remotos utilizando un Servidor DNS en el sitio principal, accesible a través de VPN. En estos entornos normalmente se quiere resolver todas las consultas DNS en el sitio central para el control centralizado sobre DNS, sin embargo, algunas organizaciones prefieren dejar resolución DNS de Internet con pfSense en cada sitio, y sólo reenviar consultas para interior dominios en el servidor DNS central. Tenga en cuenta que usted necesitará una ruta estática para que esto funcione a través de IPsec.
Vea la sección llamada "El tráfico iniciado por pfSense y IPsec" para obtener más información.

DNS dinámico

El cliente de DNS dinámico en pfSense le permite registrar la dirección IP de la interfaz WAN con una variedad de proveedores de servicios de DNS dinámico. Esto es útil cuando se quiere acceder de forma remota dinámica
Conexiones IP, más utilizadas para conectarse a una VPN, servidor web o servidor de correo.

> Nota
>
> Esto sólo funciona en la interfaz WAN primaria. Cualquier interfaz OPT no pueden utilizar el construido en el cliente de DNS dinámico. También sólo se puede registrar un nombre de DNS dinámico. pfSense 2.0 soporta la mayor cantidad de servicios de DNS dinámico diferentes como desee, permite el registro de OPT WAN IP, y permite el registro de su dirección IP pública real en entornos en los que pfSense recibe una IP privada para WAN y está nado contra la corriente.

El uso de DNS dinámico

pfSense permite el registro con nueve proveedores de DNS dinámicas diferentes a partir de la versión 1.2.3. Usted puede ver los proveedores disponibles haciendo clic en el desplegable Tipo de servicio desplegable. Puede encontrar más información sobre
los proveedores mediante la búsqueda de su nombre para encontrar su sitio web. La mayoría ofrece un servicio de nivel básico en
sin costo alguno, y algunas ofrecen servicios de primera calidad a un costo adicional.
Una vez que usted decida sobre un proveedor, visite su sitio web, se registra para una cuenta y configurar un nombre de host.
Los procedimientos de este variar para cada proveedor, pero tienen instrucciones en sus sitios web. Después configurar el nombre de host con el proveedor, a continuación, configura pfSense con esos ajustes.

Tipo de Servicio

Seleccione su proveedor de DNS dinámico aquí.

Hostname

Introduzca el nombre de host que ha creado con su proveedor de DNS dinámico.

MX

Un MX (Mail Exchanger) Registro es cómo los servidores de correo de Internet saben dónde entregar el correo para su dominio. Algunos proveedores de DNS dinámico le permitirá configurar esto a través de su cliente de DNS dinámico. Si el suyo no, escriba el nombre de host del servidor de correo que recibir el correo electrónico de Internet para su dinámica Dominio DNS.

Los comodines

Habilitación de DNS comodín en el nombre de DNS dinámico significa todas las consultas de nombres de host se resolverán en el
Dirección IP del nombre de host DNS dinámico. Por ejemplo, si el nombre de host es example.dyndns.org, permitiendo comodín hará que *. example.dyndns.org (a.example.dyndns.org, b.example.dyndns.org, etc) resolver el mismo que example.dyndns.org.

Nombre de usuario y Contraseña

Aquí es donde se introduce el nombre de usuario y la contraseña de su proveedor de DNS dinámico.

RFC 2136 actualizaciones de DNS dinámico

El RFC 2136 funcionalidad actualizaciones de DNS dinámico le permite registrar un nombre de host en cualquier DNS servidor que soporte RFC 2136 actualizaciones. Esto puede ser usado para actualizar los nombres de host en BIND y Windows
Los servidores DNS del servidor, entre otros.

Esto puede funcionar simultáneamente con uno de los proveedores de servicios de DNS dinámicos discutidos previamente,
Sin embargo, también se limita a una única configuración y sólo registrará el IP WAN, no las de cualquier Interfaces de OPT WAN.

SNMP

El Network Management Protocol [http://en.wikipedia.org/wiki/Snmp] (SNMP) daemon simple le permitirá controlar remotamente algunos parámetros del sistema pfSense. Dependiendo de las opciones elegido, puede supervisar el tráfico de red, los flujos de red, colas pf, y la información general del sistema tales como la CPU, la memoria y el uso del disco. La implementación SNMP utilizado por pfSense es bsnmpd, que por defecto sólo tiene las bases de información de gestión más básicos (MIB) disponibles, y se extiende por modules.1 cargable Además del daemon SNMP, también puede enviar capturas a un servidor SNMP para ciertos eventos. Estos varían en base a los módulos cargados. Por ejemplo, los cambios de estado de enlace de red generará una trampa si tiene el módulo MIB II cargado. El servicio SNMP se puede configurar por

navegación a Servicios SNMP.

La forma más fácil de ver lo que se dispone de datos sería correr snmpwalk contra el sistema pfSense desde otro host con net-snmp o un equivalente instalado. El contenido íntegro de las MIB disponibles son más allá del alcance de este libro, pero hay un montón de recursos impresos y en línea para SNMP, y algunos de los árboles están cubiertos de MIB RFC. Por ejemplo, el MIB recursos de acogida se define en el RFC 2790.

SNMP Daemon

Estas opciones determinan si, y cómo, el demonio SNMP se ejecutará. Para desactivar el daemon SNMP, compruebe Habilitar. Una vez Enable se haya comprobado, las otras opciones pueden entonces ser cambiados.

Sondeo Puerto

Conexiones SNMP son todos UDP, y los clientes SNMP predeterminado para usar el puerto UDP 161. Este ajuste se hacer que el daemon para que escuche en un puerto diferente, y su cliente o el agente SNMP de votación deben ser cambiado para que coincida.

Ubicación del sistema

Este campo de texto especifica qué cadena se devuelve cuando la ubicación del sistema se realiza una consulta a través de SNMP.
Usted puede seguir cualquier convención es necesaria para su organización. Para algunos dispositivos una ciudad o estado
puede ser lo suficientemente cerca, mientras que otros pueden necesitar más detalles específicos, tales como qué bastidor y posición en
que el sistema reside.

Sistema de contacto

El contacto del sistema es también un campo de texto que se puede establecer sin embargo sus necesidades requieren. Podría ser un nombre,
una dirección de correo electrónico, se necesita un número de teléfono, o lo que sea.

Leer Community String

Con SNMP, la cadena de comunidad actúa como una especie de nombre de usuario y contraseña en una. Clientes SNMP tendrá que utilizar esta cadena de comunidad cuando el sondeo. El valor por defecto de "público" es común, por lo que debería pensar en cambiar a otra cosa además de restringir el acceso al servicio SNMP
con reglas de firewall.

SNMP Traps

Encomendar al daemon SNMP para enviar capturas SNMP, marque Activar. Una vez Habilitar haya sido chequeada, las otras opciones pueden entonces ser cambiados.

[1] http://people.freebsd.org/ ~ harti / BSNMP /

Servidor de Trampa

El servidor trampa es el nombre de host o la dirección IP a la que las capturas SNMP deberán ser remitidas.

Puerto del servidor trampa

Por defecto, las capturas SNMP se configuran en el puerto UDP 162. Si el receptor de capturas SNMP se establece para un diferente
puerto, ajuste este valor a la par.

SNMP trap cadena

Esta cadena será enviado junto con cualquier trampa SNMP que se genera.

Módulos

Los módulos cargables disponibles aquí permiten que el daemon SNMP para entender y responder a las consultas para más información del sistema. Cada módulo cargado consumirá recursos adicionales. Como tal, garantizar que sólo los módulos que realmente se utilizan se cargan.

MIBII

Este módulo proporciona información especificada en el árbol MIB II estándar, que abarca la creación de redes información y las interfaces. Tras este módulo cargado voluntad, entre otras cosas, deje que se consulta la red interconectar la información, incluyendo direcciones de estatus, de hardware y de propiedad intelectual, la cantidad de datos transmitidos y
recibido, y mucho más.

Netgraph

El módulo netgraph proporciona alguna información relacionada netgraph-tales como los nombres de nodo y netgraph estados, los pares de ganchos y errores.

PF

El módulo pf da acceso a una gran cantidad de información acerca de pf. El árbol MIB cubre aspectos de la conjunto de reglas, los estados, las interfaces, tablas y colas altq.

Los recursos de acogida

Este módulo cubre información sobre el propio anfitrión, incluyendo el tiempo de actividad, la media y los procesos de carga,
tipos de almacenamiento y uso, los dispositivos del sistema conectados, e incluso software instalado.

Enlazar a la interfaz LAN sólo

Esta opción hará que el daemon SNMP escucha en la interfaz LAN solamente. Esto facilita las comunicaciones sobre túneles IPSec VPN, ya que elimina la necesidad de que la ruta estática mencionado anteriormente, pero también ayuda a proporcionar una seguridad adicional mediante la reducción de la exposición del servicio en otras interfaces.

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 para configurar el uno al otro cuando se conecta a una red. Esto incluye la creación de sus propias puerto remite NAT y las reglas del cortafuegos asociados. El servicio UPnP en pfSense,

encontrar en Servicios UPnP, permitirá a los PC clientes y otros dispositivos como consolas de videojuegos a permitir automáticamente el tráfico requerido para llegar a ellos. Hay muchos programas y sistemas populares que soportan UPnP, como Skype, uTorrent, mIRC, clientes de mensajería instantánea, PlayStation 3 y XBox 360.

UPnP utiliza el Protocolo simple de descubrimiento de servicios (SSDP) para la detección de redes, que utiliza Puerto UDP 1900. El demonio UPnP utilizado por pfSense, miniupnpd, también utiliza el puerto TCP 2189. Usted puede

debe permitir el acceso a estos servicios con reglas de firewall, especialmente si usted ha eliminado el defecto LAN-a-cualquier regla, o en configuraciones de puente.

Las preocupaciones de seguridad

El servicio 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 y reenviar todo el tráfico - una potencial pesadilla de seguridad. Por otro lado, puede ser una tarea para entrar y mantener el puerto NAT forwards y sus normas correspondientes, especialmente cuando se trata de consolas de juego. Hay una gran cantidad de conjeturas y la investigación involucrados para encontrar los puertos y los ajustes adecuados, pero UPnP simplemente funciona y requiere
poco esfuerzo administrativo. Puerto remite Manual para acomodar estos escenarios tienden a ser excesivamente permisiva, lo que podría exponer servicios que no deberían estar abiertas desde Internet. Los delanteros del puerto son también siempre encendido, donde UPnP puede ser temporal.

Hay controles de acceso presentes en la configuración del servicio UPnP, lo que ayudará a bloquear que y lo que se le permite hacer modificaciones. Más allá de la incorporada en los controles de acceso, se puede ampliar controlar el acceso con reglas de firewall. Cuando se controla adecuadamente, UPnP también puede ser un poco más seguro
permitiendo que los programas para recoger y escuchar en puertos aleatorios, en lugar de tener siempre el mismo puerto abierto
y reenviado.

Configuración

El servicio UPnP está configurado por la navegación a los Servicios UPnP. Active el servicio marcando el cuadro Habilitar UPnP. Cuando haya terminado de realizar los cambios necesarios, que se describen en el resto de la sección, haga clic en Guardar. El servicio UPnP A continuación, se inicia automáticamente.

Interfaces

Esta configuración permite que usted escoja las interfaces en las que se permite UPnP para escuchar. Más de uno interfaz puede ser elegido, mantenga pulsada Ctrl mientras hace clic en las interfaces adicionales. Anulación de la selección
una interfaz funciona de la misma manera, mantenga Ctrl mientras hace clic para eliminar la selección. Si una interfaz se puentea a otro, UPnP sólo se debe seleccionar en la interfaz de "padre", no la que es
puenteado. Por ejemplo, si usted tiene OPT1 puenteada a una red LAN, sólo habilitar UPnP en la red LAN.

Velocidades Máximas

A partir de la versión 1.2.3 pfSense, ahora puede configurar la velocidad máxima de carga y descarga en los puertos abierto por el UPnP. Estas velocidades se establecen en kilobits por segundo, por lo que para limitar una descarga a 1,5 Mbit / s, se
entraría 1536 en el campo de descarga máxima velocidad.

Reemplazar dirección WAN

Por defecto, el servicio UPnP configurará forwards portuarias y reglas de firewall para la dirección WAN.
Este ajuste le permitirá introducir una dirección IP alternativa, tal como una dirección WAN secundaria o una compartida Dirección CARP.

Traffic Shaping Queue

Por defecto, las normas creadas por UPnP no asignar el tráfico en una cola shaper. Al ingresar el nombre de una cola en este campo, el tráfico que pasa por una norma UPnP creados caerá en esta cola. Elegir
la cola con prudencia, ya que cualquier dispositivo o programa compatible con UPnP utilizará esta cola. Podría ser Bittorrent,
o podría ser una consola de juegos, así que elige una cola que tiene una prioridad que se ajuste mejor con el tráfico que espere ser más común.

Los paquetes de registro

Cuando se marca esta casilla, los delanteros portuarios generados por UPnP se ajustarán al registro, de manera que cada conexión realizada tendrá una entrada en los registros del firewall, que se encuentra en el Estado Registros del sistema, en la
Ficha Firewall.

Use System Uptime

Por defecto, el daemon UPnP informa el tiempo de servicio cuando se les pregunta y no la disponibilidad del sistema. Al seleccionar esta opción hará que se reporte el tiempo de actividad del sistema real en lugar.

Denegar por defecto

Si la forma predeterminada denegar el acceso a la opción UPnP está habilitada, entonces UPnP únicamente permitirá el acceso a los clientes
coincidir las reglas de acceso. Este es un método más seguro de controlar el servicio, pero como se ha discutido más arriba, también es menos conveniente.

UPnP permisos de usuario

Hay cuatro campos para especificar reglas de acceso definidas por el usuario. Si se elige la opción de denegación por omisión, que
debe establecer las reglas para permitir el acceso. Las reglas se formulan con el siguiente formato:

<[Permitir | deny]> <[puerto externo | rango de puertos]> <[IP interna | IP / CIDR]>
<[Puerto interno | rango de puertos]>

Ejemplo Permiso UPnP usuario 1

Denegar el acceso al puerto 80 de reenvío de todo en la LAN, 192.168.1.1, con una subred / 24.

negar 192.168.1.1/24 80 80

Ejemplo Permiso UPnP Usuario 2

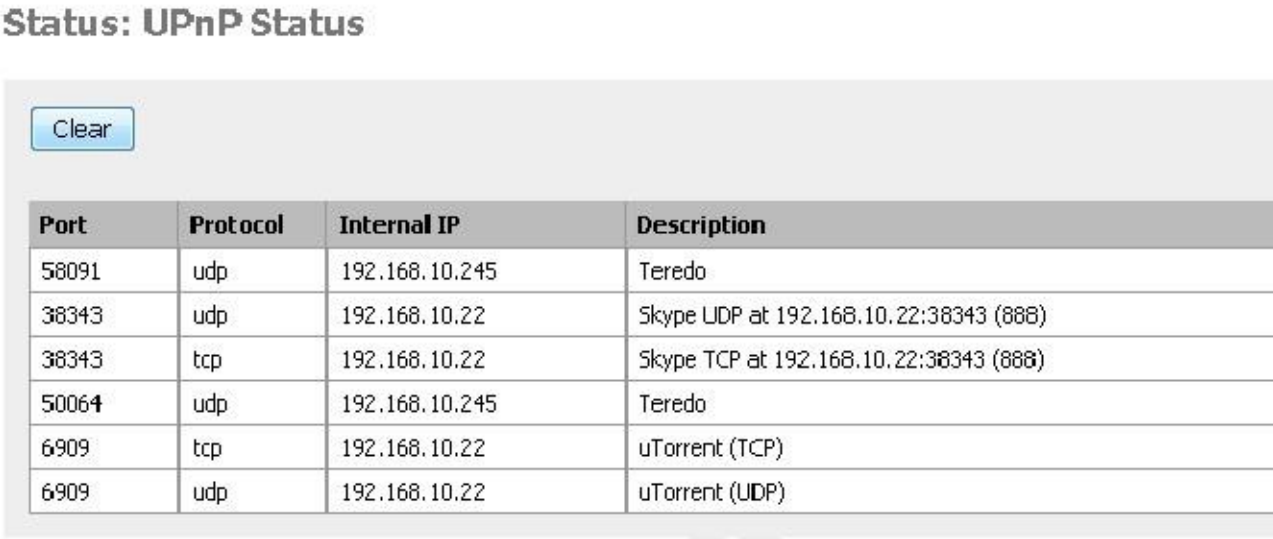
Permita 192.168.1.10 que transmita cualquier puerto sin privilegios.

permitir 1024-65535 1024-65535 192.168.1.10

Estado

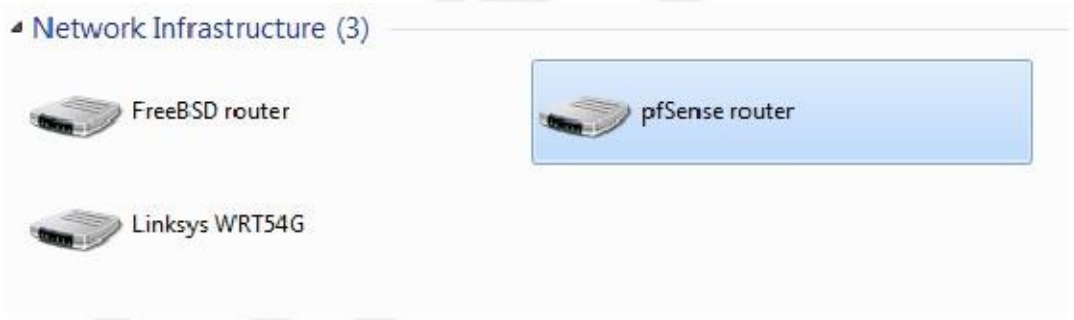
El estado del servicio UPnP sí mismo puede ser visto en Estado Servicios. Esto demostrará si el servicio está en marcha o parado, y le permitirá detener, iniciar o reiniciar el servicio. Todo esto debe ser manejado de forma automática, pero puede ser controlada manualmente, si es necesario. Una lista de los puertos y los clientes actualmente reenviados
como la de la Figura 25.3, "pantalla de estado de UPnP mostrando PC clientes con puertos reenviados" puede ser visto en Estado UPnP.

Figura 25.3. Pantalla de estado de UPnP mostrando PC clientes con puertos reenviados



Cuando el servicio se está ejecutando, también debe aparecer al navegar por la red utilizando un UPnP-aware Sistema operativo como Windows 7 o Windows Vista, como se muestra en la Figura 25.4, "sistema de pfSense como visto por Windows 7 cuando se navega por la red ". Puede hacer clic derecho sobre el icono del router y luego haga clic en Ver página Web del dispositivo para abrir el WebGUI en el navegador predeterminado. Si hace clic derecho sobre el
router y haga clic en Propiedades, también se mostrará la versión pfSense y la dirección IP del router.

Figura 25.4. sistema pfSense como se ha visto por Windows 7 en su navegación por la red



Solución de problemas

La mayoría de los problemas con UPnP tienden a involucrar puente. En este caso, es importante que usted hace que el específico
reglas de firewall para permitir UPnP en el puerto UDP 1900. Puesto que es el tráfico de multidifusión, el destino debe ser la dirección de broadcast para la subred, o en algunos casos por lo que es cualquier será necesario. Consultar el firewall registra en Estado □ Registros del sistema, en la pestaña de firewall, para ver si el tráfico está bloqueado. Pagar
especial atención a la dirección de destino, ya que puede ser diferente de lo esperado.

Más problemas con las consolas de juegos también puede ser aliviada por el cambio a NAT saliente manual y permitiendo de puerto estático. Vea la sección llamada "puerto estático" para más detalles.

NTPD

El servicio OpenNTPD [http://www.openntpd.org/] es un protocolo de tiempo de red [http:// en.wikipedia.org / wiki / Network_Time_Protocol] (NTP) daemon que escuche las solicitudes de clientes y les permite sincronizar su reloj con la del sistema de pfSense. Mediante la ejecución de un local de Servidor NTP y usarlo para sus clientes, se reduce la carga en los servidores del estrato bajo y puede asegurarse de que sus sistemas siempre se puede llegar a un servidor de hora. Antes de delegar esta tarea a su pfSense sistema, es una buena práctica para asegurarse de que tiene un reloj de precisión y mantiene la hora razonable.

No hay mucho para configurar el servidor OpenNTPD, disponible en Servicios OpenNTPD. Comprobar la casilla Activar, elija qué interfaces debe escuchar a, y haga clic en Guardar. Más de una interfaz pueden elegirse manteniendo pulsada Ctrl mientras hace clic en las interfaces adicionales. Al anular la selección de una interfaz funciona de la misma manera, mantenga Ctrl mientras hace clic para eliminar la selección. Se iniciará el servicio inmediatamente, sin embargo, habrá un retraso de varios minutos antes de que dará servicio a las solicitudes de NTP, como la servicio asegura su tiempo es exacto antes de responder a las solicitudes.

Registros OpenNTPD se mantienen en Estado Registros del sistema, en la ficha OpenNTPD. OpenNTPD tiene muy poco registro, a menos que exista un problema, el servicio nunca generará ninguna entrada de registro.

Wake on LAN

El 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 ordenadores desde un estado de apagado enviando especiales "paquetes mágicos". La NIC en el equipo que se va a despertar debe ser compatible con WOL y tiene que ser configurado correctamente. Por lo general hay una configuración del BIOS para activar WOL y adaptadores no integrados probablemente necesita un WOL cable conectado entre la NIC y un encabezado WOL en la placa base.

WOL tiene muchos usos potenciales. Por lo general, las estaciones de trabajo y servidores se mantienen en funcionamiento debido a servicios que prestan, archivos o impresoras que comparten, o por conveniencia. Usando WOL permitiría estos permanecer apagado, y conservar la energía. Si se necesita un servicio, el sistema se puede activar cuando sea necesario. Otro ejemplo sería si alguien necesita acceso remoto a un sistema, pero el usuario apagarlo. Usando WOL la máquina puede ser despertado, y puede entonces tener acceso una vez iniciado.

WOL no ofrece seguridad inherente. Cualquier sistema en la misma red de capa 2 puede transmitir una WOL paquete, y el paquete serán aceptadas y obedecidas. Lo mejor es sólo para configurar WOL en la BIOS para las máquinas que lo necesitan, y desactivarlo en todos los demás. Hay un par de WOL específica del proveedor extensiones que proporcionan una seguridad adicional, pero nada universalmente compatibles.

Wake Up una sola máquina

Para despertar una sola máquina, seleccione la interfaz a través del cual se puede llegar, y entrar en el la dirección MAC del sistema en el formato de xx: xx: xx: xx: xx: xx. Al hacer clic en Enviar, pfSense se transmitir un Magic Packet WOL fuera de la interfaz elegida, y si todo ha ido según lo previsto, el sistema debe despertar. Tenga en cuenta que los sistemas tendrán un tiempo para arrancar. Pueden pasar varios minutos antes de que el sistema de destino está disponible.

Almacenar direcciones MAC

Para almacenar una dirección MAC para mayor comodidad después, haga clic en Theby la lista de direcciones MAC almacenados y usted verá una pantalla de edición en blanco. Elija la interfaz a través del cual se puede llegar, y entrar en el la dirección MAC del sistema en el formato de xx: xx: xx: xx: xx: xx. Una descripción también se puede introducir para su posterior consulta, por ejemplo "PC de Pat" o "Servidor de Sue". Haga clic en Guardar cuando haya terminado y usted 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 en para eliminar una entrada.

Despierta una sola máquina almacenado

Para enviar un Magic Packet WOL a un sistema que ha sido ingresado previamente, haga clic en su dirección MAC en la lista de sistemas almacenados. La dirección MAC debe destacarse como un enlace. Usted será llevado de nuevo a la vista de WOL, con la interfaz del sistema y la dirección MAC de pre-llenado en el formulario. Haga clic en Enviar y el Magic Packet será enviado.

Despierta todas las máquinas almacenados

En la página WOL, hay aButton que puede ser utilizado para enviar un paquete mágico WOL a todos los almacenados sistemas. Haga clic en el botón y se enviarán las solicitudes, sin otra intervención necesaria.

Reactivación desde concesiones DHCP Vista

Para enviar un Magic Packet WOL de los arrendamientos DHCP ver en Diagnóstico Concesiones DHCP, haga clic en su dirección MAC en la lista de contratos de arrendamiento, que debe ser destacado como un enlace. El enlace WOL sólo se
estar activo para los sistemas cuyo estado se representa como "fuera de línea". Usted será llevado a la página de WOL, con la interfaz del sistema y la dirección MAC de pre-llenado en el formulario. Haga clic en Enviar y el Magic Packet será enviado.

Sálvame de arriendos DHCP Vista

Puede copiar una dirección MAC a una nueva entrada de asignación WOL mientras ve el arrendamiento DHCP en Diagnóstico Arriendos DHCP. Haga clic en el botón al final de la línea, y usted será llevado a la WOL
pantalla de edición de entrada con la información de que el sistema de pre-llenado en el formulario. Añadir una descripción, y luego
haga clic en Guardar.

PPPoE servidor

pfSense puede actuar como un servidor PPPoE y aceptar / autenticar conexiones de clientes PPPoE en un
interfaz local, que actúa como un concentrador de acceso. Esto puede ser utilizado para obligar a los usuarios para autenticar
antes de obtener acceso a la red, o para controlar su comportamiento de inicio de sesión. Esto se encuentra en Servicios PPPoE Server. Usted encontrará que esta configuración es muy similar a la del servidor PPTP VPN (Capítulo 18, PPTP VPN).

Para activar esta función, primero debe seleccionar Habilitar servidor PPPoE. A continuación, elija el que la interfaz de para ofrecer este servicio. Configure la máscara de subred que se debe asignar a los clientes PPPoE y el
Número de usuarios PPPoE para permitir. A continuación, introduzca la dirección del servidor que es la dirección IP que el
sistema pfSense enviará a los clientes PPPoE de usar como su puerta de enlace. Introduzca una dirección IP en el Cuadro Intervalo de direcciones remotas y que se utilizará junto con la máscara de subred establecen principios para definir
la red utilizada por los clientes PPPoE.
Las opciones restantes son para la autenticación mediante RADIUS. Si desea pasar la autenticación
peticiones en un servidor RADIUS, complete la información en la mitad inferior de la pantalla. Si lo haría
en vez prefiera utilizar la autenticación local, a continuación, Guardar los ajustes y haga clic en la ficha Usuarios para agregar locales
los usuarios. Clic para agregar un usuario y luego rellenar el nombre de usuario, contraseña y una dirección IP opcional.
Vea la sección "Autenticación RADIUS con Windows Server" para obtener información sobre la configuración de RADIUS en un servidor Windows, pero puede utilizar cualquier servidor RADIUS que prefiera.

Capítulo 26. Supervisión del sistema

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 cualquiera podría desear (Y algo más).

Registros del sistema

pfSense registra una buena cantidad de datos por defecto, pero lo hace de una manera que no se desborde el almacenamiento en el router. Los registros se encuentran en Estado Registros del sistema en el WebGUI, y bajo `/ Var / log /` en el sistema de archivos. Algunos componentes, tales como DHCP e IPsec, entre otros, generan suficientes registros que ellos tienen sus propias fichas de registro para reducir el desorden en el registro principal del sistema y facilitar la solución de problemas para estos servicios individuales. Para ver estos otros registros, haga clic en la ficha correspondiente al subsistema que desea ver.

registros pfSense están contenidos en un fichero cíclico binario o zueco formato. Estos archivos son de un tamaño fijo, y nunca crecer. Como consecuencia de esto, el registro sólo se llevará a cabo una cierta cantidad de entradas, y el viejo entradas son empujados continuamente fuera del registro a medida que se agregan otras nuevas. Si esto es un problema para usted o su organización, puede ajustar la configuración de registro para copiar estas entradas a otro servidor con syslog donde que se pueden conservar o rotados con menos frecuencia de forma permanente. Vea la sección llamada "Remote Anotaciones con Syslog "más adelante en esta sección para obtener información acerca de syslog.

Visualización de los registros del Sistema

Los registros del sistema se pueden encontrar en Estado Registros del sistema, en la ficha Sistema. Esto incluirá registro entradas generadas por el propio huésped, además de los creados por algunos servicios y paquetes que no tienen sus registros redireccionados a otras fichas / archivos de registro.

Como se puede ver por las entradas de ejemplo en la Figura 26.1, "Entradas del registro de sistema de ejemplo", hay registro entradas del demonio SSH, el paquete avahi, y el cliente de DNS dinámico. Muchos otros subsistemas registrará aquí, pero la mayoría no sobrecargar los registros en cualquier momento. Normalmente, si un servicio tiene muchas log entradas que se moverán a su propio archivo de pestaña / log. También tenga en cuenta en este ejemplo que los registros están configurados a aparecer en orden inverso, y las entradas más recientes aparecen en la parte superior de la lista. Consulte la siguiente sección para saber cómo configurar los registros de orden inverso.

Figura 26.1. Entradas del registro de sistema de ejemplo

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 Entr
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()

Cambiar Configuración del registro

Configuración de registro pueden ser ajustados por ir a Estado Registros del sistema y el uso de la ficha Configuración. Aquí
encontrará varias opciones para elegir que el control de cómo se muestran los registros.

La primera opción, Mostrar entradas de registro en orden inverso, controla el orden en el que aparecen en los registros las fichas de registro. Con esta opción activada, las entradas más recientes estarán en la parte superior del registro de salida. Cuando esta opción no está seleccionada, las entradas más antiguas estarán en la parte superior. Algunas personas encuentran tanto
de estos métodos útiles y fáciles de seguir, así que usted puede elegir cualquier configuración que prefiera.

El siguiente ajuste, Número de entradas de registro para mostrar, sólo controla cuántos se muestran en líneas de registro cada ficha. Los registros reales pueden contener más datos, por lo que este puede ser ajustado hacia arriba o hacia abajo un poco si es necesario.

Normalmente, cada paquete bloqueado por defecto del firewall regla de rechazo se registra. Si no quieres ver estas entradas de registro, desactive los paquetes de registro bloqueados por la opción de reglas predeterminadas.

La opción Mostrar registros de filtro prima controla la salida del Firewall registra pestaña. Cuando se activa, la salida no será interpretado por el analizador de registro, y en su lugar se mostrará en su formato raw. A veces esto puede ayudar en la solución de problemas o si necesita apoyar el registro de crudo dará un técnico más información que se ve normalmente en la salida del registro de firewall predeterminada. Los registros crudos son más difíciles de leer e interpretar
que los registros analizados, por lo que este se deja típicamente más desenfrenado de la época.

Haga clic en Guardar cuando haya terminado de hacer cambios. Se discuten las opciones restantes de esta pantalla en la siguiente sección.

Registro remoto con Syslog

Las otras opciones en Estado Registros del sistema de la ficha Configuración son para el uso de syslog para copiar registro
entradas a un servidor remoto. Debido a que los registros mantenidos por pfSense en el propio router son de un tamaño finito,
copiar estas entradas a un servidor syslog puede ayudar con la solución de problemas y el seguimiento a largo plazo. La registros en el router se borran al reiniciar, así que tener una copia remota también pueden ayudar a diagnosticar eventos que
ocurrir justo antes de que un router se reinicia.
Algunas políticas corporativas o legales dictan cómo troncos largos se deben mantener por los cortafuegos y similares dispositivos. Si su organización requiere de retención del registro a largo plazo, tendrá que configurar un syslog servidor para recibir y retener estos registros.

Para iniciar el registro de forma remota, marque Activar syslog'ing al servidor syslog remoto, y rellenar una dirección IP para su servidor syslog lado remoto Syslog Server. Si usted también desea deshabilitar el registro local
usted puede comprobar los archivos de registro de escritura Desactivar el disco ram local, pero esto no se recomienda generalmente.

El servidor syslog es típicamente un servidor que es directamente accesible desde su sistema pfSense a nivel local interfaz. Explotación también se puede enviar a un servidor a través de una VPN, pero puede ser necesario algún tipo de configuración adicional
(Ver la sección llamada "Traffic iniciado por pfSense y IPsec") Usted no debe enviar directamente los datos de registro del sistema
a través de su conexión WAN, ya que es texto plano y puede contener información confidencial.
Marque las casillas para las entradas del registro que le gustaría copiado al servidor syslog. Usted puede elegir para iniciar la sesión de forma remota los eventos del sistema, eventos de firewall, eventos del servicio DHCP, Portal auth, eventos y VPN
Todo.

Asegúrese de hacer clic en Guardar cuando haya terminado de realizar los
cambios.

Si no tiene un servidor syslog, es bastante fácil de configurar una. Vea la sección llamada "Servidor Syslog en Windows con Kiwi Syslog "para obtener información sobre la configuración de Kiwi Syslog en Windows. Casi cualquier
UNIX o un sistema de tipo UNIX se pueden utilizar como un servidor syslog. FreeBSD se describe en el siguiente sección, pero otros pueden ser similares.

Configuración de un servidor Syslog en FreeBSD

Configuración de un servidor syslog en FreeBSD sólo requiere un par de pasos. En estos ejemplos, reemplazar 192.168.1.1 con la dirección IP de su servidor de seguridad, reemplace EXCO-rtr con el nombre de host el servidor de seguridad, y vuelva a colocar EXCO-rtr.example.com con el nombre de host completo y el dominio de su firewall. Yo uso 192.168.1.1 en estos ejemplos, ya que se recomienda hacer esto con la interno dirección de su router, no es 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 firewall, así:

192.168.1.1 EXCO-rtr EXCO-rtr.example.com

Luego hay que ajustar de syslogd banderas de inicio para aceptar los mensajes de syslog desde el servidor de seguridad. Editar `/ etc / rc.conf` y agregar esta línea si no existe, o añadir esta opción a la línea existente para el ajuste:

```
syslogd_flags = "-a 192.168.1.1 "
```

Por último, tendrá que añadir algunas líneas a `/ Etc / syslog.conf` que va a coger las entradas del registro de esta anfitrión. Debajo de las otras entradas existentes, agregue las siguientes líneas:

```
! *
+ *
+ EXCO-rtr
*. *                                                    / Var / log / EXCO-rtr.log
```

Esas líneas se restablecerá el programa y filtros de host, a continuación, establecer un filtro de host para el servidor de seguridad (uso su nombre corto como entró en `/ Etc / hosts)`. Si está familiarizado con el syslog, se puede ver en `/ Etc / syslog.conf` en el router pfSense y filtrar los registros de diversos servicios en registro independiente archivos en el servidor syslog.

Después de estos cambios tendrá que reiniciar syslogd. En FreeBSD esto es sólo un simple comando:

#/ / Rc.d / syslogd restart etc

Ahora debería ser capaz de mirar el archivo de registro en el servidor syslog y ver que llenar con el registro entradas como la actividad que ocurre en el firewall.

Salpicadero

Después de terminar el Asistente de configuración, el resultado final será en la página principal del servidor de seguridad, que es el Dashboard. La página Panel, introducido en pfSense 2.0, mejora en gran medida la cantidad y calidad de información que se puede ver de un vistazo en la página principal del servidor de seguridad. La misma información del sistema se muestra como en las versiones anteriores de pfSense, además de mucho más. Muchos otros tipos de información están disponibles en los widgets separados. Estos widgets pueden ser añadidos o eliminados, y arrastrados en torno a la posiciones deseadas por el usuario.

Gestión Reproductores

Cada widget sigue algunas normas básicas para el control de su posición, tamaño, configuración, etc. La mecánica de estas operaciones están cubiertas aquí, antes de pasar a los widgets individuales y sus capacidades.

Añadir y quitar widgets

Para empezar a añadir widgets, haga clic en el botón situado en la parte superior del tablero de instrumentos y la lista de widgets será se muestra. Haga clic en el nombre de un widget para añadirlo al cuadro de instrumentos, y luego aparecerá en uno de los columnas. Una vez que el widget se ha añadido, haga clic en Guardar configuración.

Figura 26.2. Widget Barra de título

Para cerrar y eliminar un widget de Dashboard, haga clic en el botón en la barra de título, como se ve en Figura 26.2, "Widget barra de título", a continuación, haga clic en Guardar configuración.

Reorganización de widgets

Los widgets pueden ser reorganizados y se movían entre las columnas. Para mover un widget, haga clic y arrastre la barra de título
(Figura 26.2, "Widget barra de título"), mueva el ratón a la posición deseada y luego suelte. A medida que el Widget se mueve será "complemento" en su nueva posición, para que pueda ver su nueva ubicación antes de soltar el botón del ratón. Después de colocar un widget, haga clic en Guardar configuración.

Minimizando Reproductores

Para minimizar un widget por lo que sólo se muestra como su barra de título, ocultando el contenido, haga clic en el botón en su
barra de título, como se ve en la Figura 26.2, "Widget barra de título". Para restaurar el widget a su pantalla normal, haga clic en
el botón. Después de cambiar la opinión del widget, haga clic en Guardar configuración.

Cambio de la configuración de widgets

Algunos widgets tienen ajustes personalizables que controlan cómo se muestra o actualiza sus datos. Si un widget tiene la configuración, el botón se mostrará en la barra de título, como se ve en la Figura 26.2, "Título Widget Bar ". Haga clic en ese botón y aparecerá la configuración del widget. Una vez que haya ajustado la configuración, haga clic en
Ahorra en el interior del widget.

Disponible Reproductores

Cada widget contiene un conjunto específico de datos, el tipo de información, gráfica, etc. Cada uno de los actualmente widgets disponibles serán cubiertos en esta sección, junto con sus valores (si los hay). Éstos se enumeran en orden alfabético.

Portal Cautivo Estado

Este widget muestra la lista actual de usuarios del portal cautivo en línea, incluyendo su dirección de IP, MAC la dirección y el nombre de usuario.

Estado CARP

El widget de Estado en CARP muestra una lista de todas las direcciones IP virtuales tipo CARP, junto con su estado como maestro o BACKUP.

Gateways

Los Gateways flash enumera todas las puertas de enlace del sistema, junto con su estado actual. El estado información consiste en la dirección IP de la puerta de entrada, Round Trip Time (RTT), también conocido como retraso o
latencia, la cantidad de pérdida de paquetes, y el estado (en línea, Advertencia, hacia abajo, o Recolección de datos). La los widgets se actualiza cada pocos segundos a través de AJAX.

Estado gmirror

Este widget se mostrará el estado de una matriz gmirror RAID en el sistema, si hay uno configurado. La widget se mostrará si la matriz está en línea / OK (completo), la reconstrucción o degradada.

Paquetes instalados

Los paquetes instalados flash se enumeran todos los paquetes instalados en el sistema, junto con algunos información básica sobre ellos, tales como la versión instalada y si hay una actualización disponible.

Los paquetes pueden ser actualizados desde este widget haciendo clic en  botón al final de la fila de un paquete. el

Estadísticas de la interfaz

Este Elemento muestra una cuadrícula, con cada interfaz en el sistema mostrado en su propia columna. Varios interfaz las estadísticas se muestran en cada fila, incluyendo paquetes, bytes y recuentos de errores.

Interfaces

El widget de Interfaces difiere de las estadísticas de la interfaz del widget que muestra información general acerca de la interfaz en lugar de los contadores. El widget de Interfaces muestra el nombre de cada interfaz, IPv4 dirección, dirección de IPv6, el estado del enlace de la interfaz (arriba o abajo), así como la velocidad de enlace.

IPsec

El widget de IPsec tiene dos fichas para sus dos puntos de vista distintos. La primera pestaña, general, es una cuenta de activo
y túneles inactivos. La segunda pestaña, estado del túnel, enumera cada túnel IPsec configurados y si ese túnel es arriba o abajo.

Equilibrador de carga de estado

Este widget muestra una vista compacta de la configuración de equilibrio de carga del servidor. Cada fila muestra el estado
para un servidor virtual. La columna muestra el nombre del servidor virtual del servidor, el estado, y la dirección IP con puerto donde el servidor virtual acepta conexiones. La columna muestra la piscina de la piscina individuo servidores y su estado, con un porcentaje de tiempo de actividad. La columna Descripción muestra la descripción del texto
desde el servidor virtual.

Registros del cortafuegos

El widget de Registros de firewall proporciona una vista AJAX-udpating del registro del cortafuegos. El número de filas mostrado por el widget es configurable. Al igual que con la vista del registro de firewall normal, haga clic en el icono de acción
al lado de la entrada de registro se mostrará una ventana con la regla que causó la entrada de registro.

OpenVPN

El widget de OpenVPN muestra el estado de cada instancia de OpenVPN configurado, tanto para servidores y los clientes. El estado de cada instancia se muestra, pero el estilo y el tipo de información que se muestra varía dependiendo del tipo de conexión de OpenVPN. Por ejemplo, para los servidores basados en SSL / TLS se mostrará una lista de todos los clientes conectados. Para los clientes y servidores de claves estáticas, se mostrará un estatus arriba / abajo. En cada uno
caso se muestra la dirección IP del cliente que se conecta con el nombre y la hora de la conexión.

Imagen

El asistente de la imagen muestra una imagen de su elección dentro de un widget. Esto se puede utilizar funcionalmente, de un diagrama de red o similar, o puede ser por el estilo, que muestra un logotipo de la empresa o otra imagen. Para agregar una imagen, haga clic en la barra de herramientas del widget de imagen, haga clic en Examinar para buscar la imagen
en el equipo, y haga clic en Cargar para cargar la imagen. Como se menciona en la nota sobre el widget, el mejores fotos están dentro de las dimensiones de 350 píxeles de ancho por 350 píxeles de alto.

RSS

El RSS (RDF Site Summary, o como se le llama a menudo, Really Simple Syndication) widget se mostrará un canal RSS de su elección. Por defecto, se muestra la pfSense bitácora RSS feed. Algunas personas optan por para mostrar interno de la compañía RSS alimenta o se alimenta sitio de seguridad RSS, pero puede cargar cualquier fuente RSS.

Servicios Estado

Un widget ofrece la misma vista y control de los servicios que aparece en Estado Servicios. Cada servicio está en la lista junto con su descripción, el estado (EN EJECUCIÓN, DETENIDO) y de inicio / reinicio / parada controles.

Información del sistema

Este widget es el widget principal, que muestra una gran cantidad de información sobre el sistema en funcionamiento. La información que se muestra incluye:

Nombre	El nombre de host configurado del servidor de seguridad.
Versión	La versión actual en ejecución de pfSense en el firewall. La versión, tiempo de la arquitectura y la construcción se muestran en la parte superior. En virtud de la acumulación tiempo, se muestra la versión subyacente de FreeBSD. Al hacer clic en el Versión de FreeBSD le mostrará los detalles completos del núcleo en ejecución versión. Bajo esos artículos es el resultado de una comprobación de actualización automática para un mayor versión reciente de pfSense.
Plataforma	La plataforma indica que la variación de pfSense se está ejecutando. Un completo instalar mostrará pfSense, instalación incorporada shows nanobsd, y si que va desde el LiveCD o memory stick se mostrará cdrom.
NanoBSD rebanada de arranque	Si se trata de una instalación incorporada, también se muestra la rebanada corriendo (Pfsense0 o `pfsense1)`, junto con la rebanada que se utilizará para el siguiente arranque.
Tipo de CPU	El tipo de CPU que se muestra aquí es la cadena de la versión para el procesador, tales como "Intel (R) Core (TM) i5 CPU 750@2.67GHz". Si powerd está activo y la frecuencia de la CPU ha bajado ben, a continuación, se muestra la frecuencia actual a lo largo de tamaño de la frecuencia máxima.
Cripto Hardware	Si un conocido hardware acelerador criptográfico que se ha detectado, lo hará se mostrará aquí. Puede haber otras tarjetas soportadas por FreeBSD que funcionar correctamente, pero no son detectados por este widget porque no lo hicimos tener acceso a las cadenas específicas necesarias para detectarlas. Si usted tiene tal una tarjeta, ponerse en contacto con nosotros con la información al respecto se agradecería.
Uptime	Este es el tiempo desde que el firewall se reinicia pasado.
Fecha / hora actual	La fecha y la hora actuales del servidor de seguridad, incluyendo la zona horaria. Este es útil para comparar las entradas del registro, en caso de la zona horaria donde se ver el firewall de ser diferente de donde reside, se puede decir la hora local del servidor de seguridad de esta línea.
DNS Server (s)	Enumera todos los servidores DNS configurados en el firewall.
Último cambio config	La fecha del último cambio de configuración en el servidor de seguridad.
Tamaño de la tabla Estado	Muestra el número de estados activos y los estados máximos posibles como configurada en el servidor de seguridad. Debajo de los conteos estatales es un enlace para ver el contenido de la tabla de estado.
El uso de la MBUF	Muestra el número de buffers de memoria en uso, y el máximo de la sistema tiene disponible. Estos buffers de memoria se utilizan para la red operaciones, entre otras tareas.

Uso de la CPU	Un gráfico de barras y el porcentaje de tiempo de CPU en uso por el firewall. Tenga en cuenta que viendo el tablero de instrumentos se incrementará el uso de la CPU un poco, dependiendo de su plataforma. Así que en las plataformas más lentas, como ALIX esto es probable que lea un poco más alto de lo que sería de otra manera.
Uso de memoria	La cantidad actual de RAM en uso por el sistema. Tenga en cuenta que no utilizada RAM a menudo se utiliza para cachear y otras tareas por lo que no se desperdicia o inactivo, por lo que este número puede mostrar mayor de lo esperado, incluso si está funcionando normalmente.
El uso del intercambio	La cantidad de espacio de intercambio en uso por el sistema. Si el sistema se queda sin de RAM física, y no hay espacio de intercambio disponible, las páginas menos utilizadas de memoria se localicen en la el archivo de intercambio en el disco duro. Este indicador sólo muestra cuando el sistema haya configurado el espacio de intercambio, que sólo estará en las instalaciones nuevas.
Uso del disco	La cantidad de espacio utilizado en el disco duro o medios de almacenamiento.

Tráfico Gráficos

El widget de Tráfico Gráficos proporciona un gráfico SVG en directo para el tráfico en cada interfaz. Cada gráfico puede ser ampliado o reducido al mínimo haciendo clic en el título del gráfico persona individualmente. La actualización predeterminada velocidad de los gráficos es una vez cada 10 segundos, pero que se puede ajustar en la configuración del widget. La gráficos se elaboran de la misma manera como las que se encuentran en Estado Gráfico de Tráfico.

Wake On LAN

El Wake on LAN Widget muestra todas las entradas de WOL configurados en Servicios Wake on LAN, y ofrece un medio rápido para enviar el paquete mágico a cada sistema con el fin de despertarlo.

Estado de la interfaz

El estado de las interfaces de red se puede ver en estado Interfaces. En la primera parte de Figura 26.3, "estado de la interfaz", una conexión PPPoE WAN se ha hecho y la IP, DNS, etc tiene sido obtenido. También puede ver la dirección de la interfaz de red MAC, tipo de papel, de entrada / salida de paquetes, los errores y las colisiones. Tipos de conexión dinámicas como PPPoE y PPTP tienen un botón Desconectar cuando conectado y un botón Conectar cuando esté desconectado. Interfaces obtener una IP de DHCP tienen una autorización botón cuando hay una concesión activa, y un botón Renew cuando no lo hay.

En la parte inferior de la imagen, se puede ver la conexión LAN. Como se trata de una interfaz normal con una dirección IP estática, sólo el juego habitual de los elementos se muestran.

Si el estado de una interfaz, dice "ninguna compañía", entonces por lo general significa que el cable no está enchufado o el dispositivo en el otro extremo es un mal funcionamiento de algún modo. Si se muestran los errores, por lo general son de naturaleza física: cableado o puerto errores. El sospechoso más común es los cables, y son fáciles y barato de reemplazar.

Estado del servicio

Muchos servicios del sistema y los paquetes muestran el estado de sus demonios al Estado Servicios. Cada servicio se muestra con un nombre, una descripción y el estado, como se ve en la Figura 26.4, "Estado de servicio". La estado aparece normalmente como marcha o parado. Desde este punto de vista, un servicio que se ejecuta puede reiniciarse clickingor parado haciendo clic. Un servicio detenido puede iniciarse haciendo clic en. Normalmente, no es necesario para controlar los servicios de esta manera, pero en ocasiones puede haber mantenimiento o razones de solución de problemas para hacerlo.

Figura 26.4. Servicios Estado

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

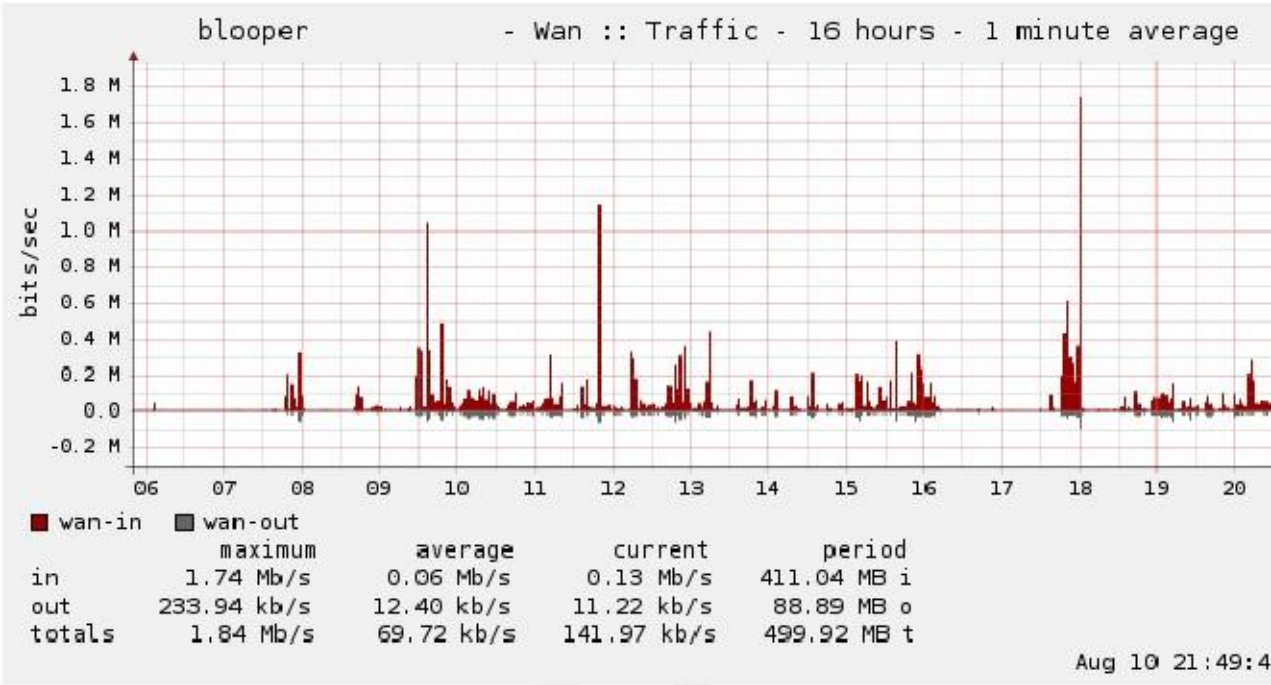
Gráficos RRD

RRD gráficos son otro conjunto útil de los datos proporcionados por pfSense. Mientras que el router está ejecutando mantiene
un seguimiento de varios bits de datos sobre cómo el sistema realiza, y luego almacena estos datos en Round-Robin Base de datos (RRD) archivos. Las gráficas de estos datos están disponibles de Estado RRD gráficos. En esa pantalla hay seis tabletas, cada uno de los cuales se cubren en esta sección: Sistema, Tráfico, paquetes, calidad, colas, y Configuración.

Cada gráfico está disponible en varias veces vanos, y cada uno de éstos se promedia en un período diferente de tiempo en función de cómo se está cubriendo mucho tiempo en un gráfico dado. También en cada gráfica será una leyenda
y un resumen de los datos que son visibles (mínimos, promedios, máximos, valores de corriente, etc.)
Los gráficos están disponibles en una gama de 4 horas con un promedio de 1 minuto, un rango de 16 horas, 1 minuto promedio, un rango de 2 días con un promedio de 5 minutos, un intervalo de 1 mes con un promedio de 1 hora, un 6 meses
ir con una media de 12 horas y un rango de 1 año con un promedio de 12 horas.
Muchos gráficos se pueden ver en el estilo Inverse o estilo Absoluto. Con estilo inverso, el gráfico se divide el tráfico por la mitad horizontalmente y entrante se muestra subiendo desde el centro, y saliente el tráfico se muestra bajando desde el centro. Con estilo Absoluto, se superponen los valores.

En la Figura 26.5, "tráfico WAN Graph", se puede ver que es un gráfico inversa 16 horas de tráfico en la WAN, que ha tenido un uso máximo de 1.74Mbit / s promedio durante un período de 1 minuto.

Figura 26.5. Tráfico WAN Gráfico



Sistema de Gráficos

Los gráficos de la ficha Sistema muestra una visión general de la utilización del sistema, incluyendo la CPU uso, rendimiento total, y los estados de firewall.

Gráfico Procesador

El gráfico muestra el uso de CPU del procesador a los procesos de usuario y del sistema, interrupciones, y el número de los procesos en ejecución.

El rendimiento gráfico

El gráfico muestra el rendimiento del tráfico entrante y saliente totalizado para todas las interfaces.

Estados Graph

El gráfico de estados es un poco más complejo. Se muestra el número de estados del sistema, sino también rompe la valor de varias maneras. Muestra los estados de filtro de reglas de firewall, NAT establece de reglas NAT, la contar de fuente única activa y direcciones IP de destino, y el número de cambios de estado por segundo.

Tráfico Gráficos

Gráficos de tráfico mostrarán la cantidad de ancho de banda utilizado en cada interfaz disponible en bits por segundo notación, y también hay una opción Allgraphs que mostrará todos los gráficos de tráfico en una sola página.

Paquete de gráficos

Los gráficos de paquetes funcionan como los gráficos de tráfico, pero en lugar de información basado en el ancho de banda
utilizado, informa del número de paquetes por segundo (pps) pasaron.

Gráficos de Calidad

El gráfico de calidad de seguimiento de la calidad de la interfaz WAN o WAN-como (los que tienen una puerta de enlace especificado,
o por medio de DHCP). Se muestra en estos gráficos son el tiempo de respuesta desde la puerta de entrada en milisegundos, como se

así como un porcentaje de paquetes perdidos. Cualquier pérdida en el gráfico indica problemas de conectividad o tiempos de
el uso de ancho de banda excesivo.

Queue Gráficos

Los gráficos son un compuesto de la cola de cada cola de la talladora de tráfico. Se muestra cada cola individual, representada por un color único. Usted puede ver bien la gráfica de todas las colas, o el gráfico que representa las gotas de todas las colas.

Configuración

Los gráficos RRD se pueden personalizar para adaptarse mejor a sus preferencias. Incluso puede desactivarlas si prefieren utilizar alguna solución gráfica externa en lugar. Haga clic en Guardar cuando termine de realizar los cambios.

Habilitar gráfica

Marque la casilla para activar un gráfico, o quite la marca para desactivar gráfica.

Default Category

Las selecciones predeterminadas opción Categoría qué pestaña se mostrarán en primer lugar cuando se hace clic en Estado RRD
Gráficos.

Default Style

La opción Default Style recoge que el estilo de los gráficos para utilizar de forma predeterminada, Inverse o Absoluto.

Firewall Unidos

Como se discutió en la sección llamada "stateful Filtering", pfSense es un firewall stateful y utiliza un estado para realizar un seguimiento de cada conexión hacia y desde el sistema. Estos estados se pueden ver de varias maneras, ya sea
en el WebGUI o desde la consola.

Visualización de las WebGUI

Visualización de los estados de la WebGUI se puede hacer mediante Diagnósticos de visita Unidos (Figura 26.6, "Ejemplo Unidos"). Aquí podrás ver el protocolo para cada conexión, su Fuente, Router, y
Destino, y su estado de conexión. Cuando se utilizan entradas de NAT, las tres entradas en el centro
columna representa el sistema que realiza la conexión, la dirección IP y el puerto pfSense está utilizando para la conexión de NAT, y el sistema remoto al que la conexión se ha hecho.

Los estados individuales se pueden eliminar haciendo clic en el final de su fila.

Figura 26.6. Ejemplo Unidos

tcp	192.168.10.10:53650 -> 72.69.194.6:41047 -> 168.143.168.68:443	FIN_WAIT_2:FIN_W
udp	224.0.0.251:5353 <- 192.168.10.17:5353	NO_TRAFFIC:SINGLE
tcp	207.45.186.18:80 <- 192.168.10.11:1289	ESTABLISHED:ESTAB
tcp	192.168.10.11:1289 -> 72.69.194.6:52740 -> 207.45.186.18:80	ESTABLISHED:ESTAB

Viendo con pftop

pftop está disponible desde el menú de la consola del sistema, y ofrece una vista en vivo de la tabla de estado, junto con la cantidad total de ancho de banda consumido por cada estado. Hay varias maneras de alterar la vista mientras

viendo pftop. Prensa hpara ver una pantalla de ayuda que explica las opciones disponibles. El más común usos están utilizando 0a través de 8para seleccionar diferentes puntos de vista, espacio para una actualización inmediata, y qdejar de fumar.

Tráfico Gráficos

Gráficos de tráfico en tiempo real dibujados con SVG (Scalable Vector Graphics) se dispone que constantemente actualizar. Usted puede encontrarlos en Estado Los gráficos de tráfico, y un ejemplo del gráfico pueden encontrarse En la Figura 26.7, "Ejemplo WAN Graph". Estos le permitirá ver el tráfico como es el caso, y dar un visión mucho más clara de lo que está sucediendo "ahora" de confiar en datos promedio de los gráficos RRD.

Sólo una interfaz es visible en un momento, y usted puede elegir la que desee ver desde la interfaz de abandono la lista desplegable. Una vez que se elige una interfaz, la página se actualizará automáticamente y comenzará a mostrar el nuevo gráfico. La característica Dashboard en pfSense 2.0 (también disponible como un paquete beta de 1.2) permite la visualización simultánea de múltiples gráficos de tráfico en una sola página.

Capítulo 27. Paquetes

El sistema de paquetes pfSense ofrece la posibilidad de ampliar pfSense sin añadir la hinchazón y el potencial vulnerabilidades de seguridad a la distribución base. Paquetes sólo se admiten en las instalaciones nuevas, no el Live CD y plataformas más antiguas incrustadas. Las versiones más recientes incrustados que se basan en NanoBSD ahora tienen la capacidad de ejecutar algunos paquetes. Algunos paquetes también pueden ser incorporados en la base

sistema, tales como el paquete SIP Proxy. Para ver los paquetes disponibles, vaya a Sistema Paquetes.

Introducción a los paquetes

Muchos de los paquetes han sido escritos por la comunidad pfSense y no por el pfSense equipo de desarrollo. Los paquetes disponibles varían mucho, y algunos son más maduros y bien-mantenido que otros. Hay paquetes que se instalan y proporcionan una interfaz gráfica de usuario para terceros software, tales como calamar, y otras que amplían la funcionalidad del propio pfSense, como el Dashboard paquete que backports algunas funciones de pfSense 2.0.

Nota

Estos paquetes pfSense son diferentes a los paquetes de Ports de FreeBSD que se tratan en la sección titulada "Uso del software de Puertos Sistema de FreeBSD (paquetes)" en el Tercer Capítulo Party Software.

Con mucho, el paquete más popular disponible para pfSense es para el servidor proxy Squid. Se instala más de dos veces más a menudo como el próximo paquete más popular: SquidGuard, que es un filtro de contenido que trabaja con Squid para controlar el acceso a los recursos de la web por los usuarios. No en vano, la tercera más popular paquete es Lightsquid, que es un paquete de análisis de registro de Squid que le permite ver los sitios web que haber sido visitado por los usuarios detrás del proxy.

Algunos otros ejemplos de paquetes disponibles (que no son Calamar relacionada) son:

• Medidores de tráfico que muestran el tráfico por dirección IP como el de Cambio, BandwidthD, NTOP y darkstat.

• Los servicios adicionales como un servidor DNS, servidor TFTP, FreeRADIUS y FreeSWITCH (una PBX VoIP).

• La representación de otros servicios como el SIP, IGMP y IMSpector.

• Utilidades del sistema como TUERCA para la monitorización de un SAI, lcdproc para el uso de una pantalla LCD, y phpSysInfo.
Utilidades de terceros • populares como nmap, iperf y arping.

• Enrutamiento BGP, edición Cron, Nagios y agentes Zabbix, y muchos, muchos otros.

Al escribir estas líneas hay más de 50 diferentes paquetes disponibles; demasiados para cubrirlos todos en este libro! Si usted desea ver la lista completa, que estará disponible desde dentro de su sistema de pfSense accediendo a System Paquetes.

Usted puede notar que la pantalla de los paquetes puede tomar un poco más en cargar que otras páginas de la web interfaz. Esto se debe a que obtiene la información del paquete XML de nuestros servidores antes de que la página se dictada para proporcionar la información más paquete de la fecha. Si el servidor de seguridad no tiene una funcional Conexión a Internet, incluyendo la resolución de DNS, se producirá un error y que le notifique, como en la Figura 27.1, "Paquete
recuperación de la información no se pudo ". Si ya se ha recuperado correctamente la información del paquete, que se mostrará desde la memoria caché, pero puede no tener la información más reciente. Este es generalmente causado por una configuración de servidor DNS que falta o incorrecta. Para conexiones IP estáticas, compruebe trabajo Los servidores DNS se introducen en el sistema La página de configuración general. Para los que tienen asignada dinámicamente
conexiones, asegurarse de que los servidores asignados por su ISP están funcionando. Es posible que desee reemplazar estos
asignada dinámicamente servidores con OpenDNS [http://www.opendns.com] o otro servidor DNS.

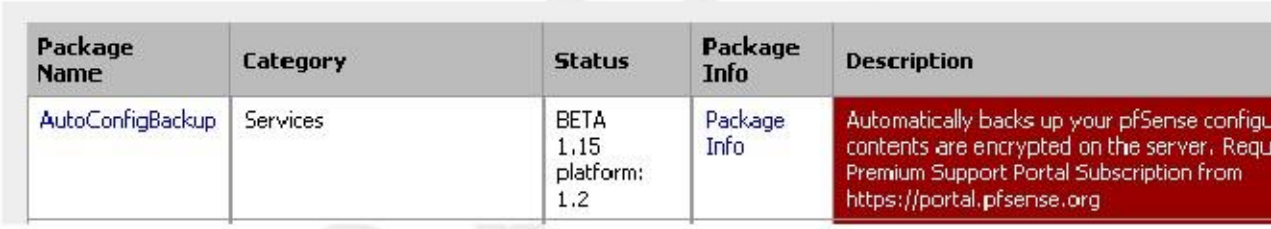
Figura 27.1. Recuperación de la información del paquete fallido

Un número creciente de paquetes tiene un enlace Información de paquetes en la lista de paquetes, apuntando a un sitio con
más información sobre ese paquete específico. Usted debe leer la información en el enlace Información de paquete antes de instalar un paquete. Después de la instalación, se puede encontrar la más reciente enlace Información de paquete para cada
paquete instalado en la ficha Paquetes instalados.

Instalación de paquetes

Los paquetes se instalan desde System Paquetes. Los listados de allí, ejemplificadas en la figura 27.2, "Listado de paquetes", mostrará de un paquete de nombre, categoría, versión y el estado, un paquete de información enlace y una breve descripción. Preste mucha atención a Estado antes de instalar los paquetes, algunos paquetes son experimentales y nunca deben instalarse en sistemas críticos de producción. Usted debe también mantener los paquetes instalados a lo estrictamente necesario para su implementación.

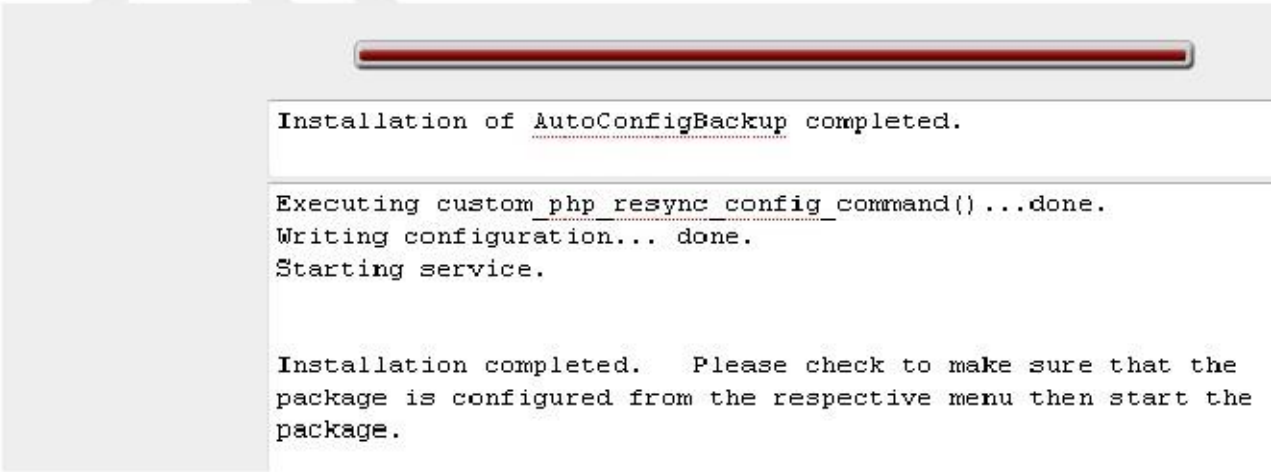
Figura 27.2. El paquete de venta



Package Name	Category	Status	Package Info	Description
AutoConfigBackup	Services	BETA 1.15 platform: 1.2	Package Info	Automatically backs up your pfSense configu contents are encrypted on the server. Requ Premium Support Portal Subscription from https://portal.pfsense.org

Los paquetes se instalan haciendo clic botón para a la derecha de su entrada. Al hacer clic, se quiere ser llevado a la pantalla de instalación del paquete en el que se mostrará el progreso de instalación (Figura 27.3, "Post-Install Package Pantalla").

Figura 27.3. Post-Install Package pantalla



Reinstalación y actualización de paquetes de

Los paquetes se vuelven a instalar y actualizar la misma manera. Empieza por ir a Sistema Paquetes, y haciendo clic en
en la ficha Paquetes instalados. Los anuncios no debería verse como la Figura 27.4, "Lista del paquete instalado".

Encuentra el paquete que desea volver a instalar o actualizar en la lista. Si hay una nueva versión disponible de que haya instalado, la columna Versión del paquete será resaltada en rojo indicando la vieja y la nueva versiones. Clic de actualizar o reinstalar el paquete.

Otra opción sería la reinstalación para reinstalar sólo los componentes GUI XML de un paquete, que se puede hacer por clicking next a la entrada de paquete. A menos que se lo indique un desarrollador, no debe utilizar esta opción, ya que puede perder las actualizaciones de los binarios que los últimos componentes de la GUI de mayo requerir.

Figura 27.4. Lista del paquete instalado

Paquetes de desinstalación

Para desinstalar un paquete, vaya a Sistema Paquetes y haga clic en la pestaña de paquetes instalados. Encuentra el paquete de la lista, y haga clic en el botón. El paquete A continuación, se elimina del sistema.

Algunos paquetes experimentales sobreescribir ficheros distribuidos con el sistema base. Estos paquetes no pueden 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 desplazamiento. Paquetes con esta peculiaridad será etiquetado como tal en su campo de descripción. Si actualiza el sistema, se sobrescribirá el 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, que suelen utilizarse para la experimentación en la no-crítico sistemas.

El desarrollo de paquetes

Los paquetes son relativamente fáciles de desarrollar, y es posible que usted o su organización pueden beneficiarse de la elaboración de un paquete que no existe. Para aquellos interesados en la creación de su paquetes propios, los recursos están disponibles en el Wiki de documentación pfSense [http://doc.pfsense.org/index.php / Developing_Packages]. Si crea un paquete y piensa que puede ser de utilidad para otros, el contacto nosotros y su trabajo puede ser evaluado para su inclusión en el sistema de paquetes para que todos la vean.

Capítulo 28. Software de Terceros y pfSense

Aunque este libro se centra en pfSense, hay una serie de paquetes de software de terceros que pueden ser configurado para interoperar con pfSense o aumentar su funcionalidad. En este contexto, tercero software se refiere a software disponibles de otros proveedores o fuentes que se pueden utilizar junto con pfSense, pero no se considera parte del "sistema de pfSense". Son distintos de los paquetes de pfSense, que son software adicional que se ejecuta en el sistema pfSense y se integra en el GUI del sistema.

RADIUS de autenticación de Windows Server

Windows 2000 Server y Windows Server 2003 se pueden configurar como un servidor RADIUS utilizando Servicio de autenticación de Internet Microsoft (IAS). Esto permite autenticar el PPTP pfSense servidor, portal cautivo, o PPPoE servidor desde sus cuentas de usuario local de Windows Server o Active Directory.

La elección de un servidor para IAS

NIC requiere una cantidad mínima de recursos y es adecuado para la adición a un Windows Server existente en la mayoría de los entornos. Microsoft recomienda instalar en un controlador de dominio de Active Directory para mejorar el rendimiento en entornos en los que la NIC está autenticando en Active Directory. Es también es posible instalarlo en un servidor miembro, lo que puede ser deseable en algunos entornos para reducir la huella de un ataque de los controladores de dominio - cada servicio accesible desde la red proporciona otra potencial vía para comprometer el servidor. NIC tiene un registro de seguridad sólida, especialmente en comparación con otras cosas que deben estar en ejecución en los controladores de dominio de Active Directory para función, así que esto no es una gran preocupación en la mayoría de entornos de red. La mayoría de los entornos de instalación
NIC en uno de sus controladores de dominio.

Instalación de la NIC

En el servidor Windows, vaya a Panel de control, Agregar / quitar programas y seleccione Agregar / quitar Componentes de Windows. Desplácese hacia abajo y haga clic en Servicios de red y, a continuación, haga clic en Detalles. Comprobar
Internet Authentication Service en la lista Servicios de red y haga clic en Aceptar. Luego haga clic en Siguiente y Se instalará la NIC. Es posible que tenga que proporcionar el CD del servidor para esta instalación se complete. ¿Cuándo la instalación se haya completado, haga clic en Finalizar.

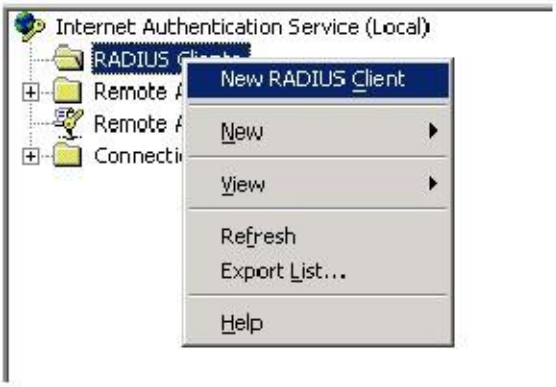
Configuración de la NIC

Para configurar IAS, abra la MMC complemento IAS en Herramientas administrativas, de autenticación de Internet Servicio. En primer lugar se añadirá un cliente RADIUS para pfSense, entonces las políticas de acceso remoto serán configurado.

Adición de un cliente de RADIUS

Haga clic derecho en Clientes RADIUS y haga clic en Nuevo cliente RADIUS, como se muestra en la Figura 28.1, "Añadir nueva
Cliente RADIUS ".

Figura 28.1. Añadir un nuevo cliente RADIUS



Introduzca un "nombre" para su servidor de seguridad, como se muestra en la Figura 28.2, "Añadir un nuevo cliente RADIUS -
nombre y dirección del cliente ", lo que puede ser su nombre de host o FQDN. El campo de dirección del cliente debe ser la dirección IP que pfSense iniciará sus solicitudes RADIUS de, o un FQDN que se resuelve que
Dirección IP. Esta será la dirección IP de la interfaz más cercana al servidor RADIUS. Si el radio
servidor es accesible a través de su interfaz LAN, esta será la IP LAN. En implementaciones en las que pfSense no es su servidor de seguridad perimetral, y su interfaz WAN reside en la red interna donde su
Servidor RADIUS reside, la dirección IP de la WAN es lo que usted debe introducir aquí. Escriba el nombre amistoso y la dirección de pfSense, haga clic en Siguiente.

Deja conjunto cliente-proveedor para RADIUS estándar, y llenar en un secreto compartido, como se muestra en la Figura 28.3,
"Agregar nuevo cliente RADIUS - secreto compartido". Este secreto compartido es lo que va a entrar en pfSense más tarde. Haga clic en Finalizar.

Ahora que ha completado la configuración de IAS. Usted puede ver el cliente RADIUS que acaba de agregar como En la Figura 28.4, "Listado del cliente RADIUS".

Figura 28.4. Listado del cliente RADIUS

Friendly Name	Address	Protocol	Client-Vendor
fw0	10.0.66.22	RADIUS	RADIUS Standard

Ahora ya está listo para configurar pfSense con la información RADIUS configurado aquí, utilizando el Dirección IP del servidor IAS y el secreto compartido configurado previamente. Refiérase a la parte de este libro describe el servicio que desea utilizar con RADIUS para más orientación. RADIUS puede ser utilizado para Portal Cautivo (la sección llamada "Configuración del portal El uso de la autenticación RADIUS"), el Servidor PPTP (la sección llamada "Autenticación"), y el servidor PPPoE (la sección llamada "PPPoE Servidor "), y también en algunos paquetes.

Configuración de usuarios y Política de acceso remoto

Si un usuario se puede autenticar a través de RADIUS se controla mediante el permiso de acceso remoto en cada la cuenta de usuario en la pestaña de acceso telefónico en las propiedades de cuenta en Usuarios y equipos de Active Directory.
No se puede especificar para permitir o denegar el acceso o controlar el acceso a través de la directiva de acceso remoto. Usted tiene la opción de especificar el acceso aquí para cada usuario mediante la especificación de permitir o denegar. Para los pequeños
entornos con requisitos básicos, esto puede ser preferible. Las políticas de acceso remoto escalan mejor para entornos con más usuarios, ya que simplemente puede poner un usuario en un grupo específico de Active Directory para permitir el acceso VPN, y también ofrecen capacidades más avanzadas, como la época de restricciones día.
Más información sobre las directivas de acceso remoto se puede encontrar en la documentación de Microsoft en http://technet.microsoft.com/en-us/library/cc785236% 28WS.10% 29.aspx.

Después de la configuración de usuarios y políticas de acceso remoto si lo desea, usted está listo para probar el servicio que
están utilizando con RADIUS en pfSense.

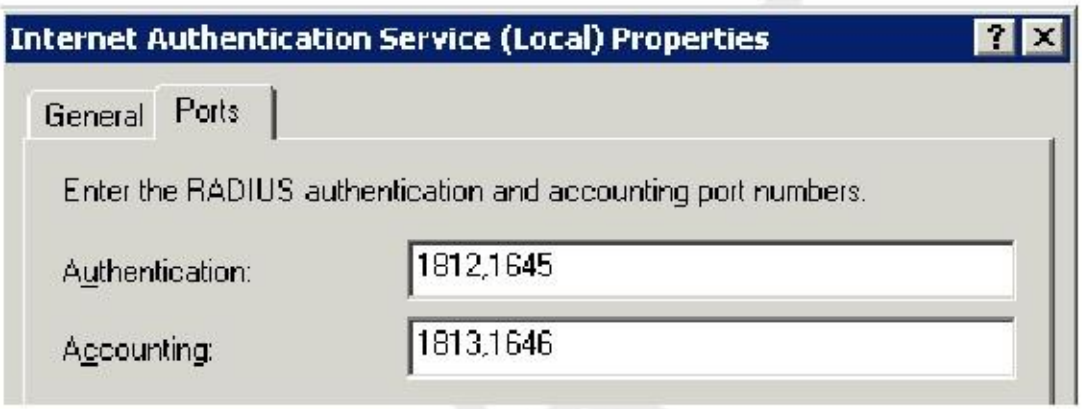
Solución de problemas de la NIC

En caso de la autenticación falla, esta sección se describen los problemas más comunes que los usuarios se encuentran con las NIC.

Verifique puerto

Asegúrese primero el puerto por defecto 1812 se está utilizando. Si el servidor IAS se ha instalado anteriormente, puede se han configurado con los puertos no estándar. En la consola MMC NIC, haga clic derecho en Internet
Servicio de autenticación (local) en la parte superior izquierda de la consola MMC y haga clic en Propiedades. Luego haga clic en el
Ficha Puertos. Puede especificar varios puertos separándolos con una coma (como se muestra en la Figura 28.5, "Puertos NIC"). Puerto 1812 debe ser uno de los puertos configurados para la autenticación. Si está utilizando
Funcionalidad de contabilidad RADIUS, así, el puerto 1813 debe ser uno de los puertos especificados en Contabilidad.

Figura 28.5. NIC Puertos



Compruebe el Visor de sucesos

Cuando un intento de autenticación RADIUS es respondida por el servidor, los registros de NIC en el sistema de registro en
Visor de sucesos con el resultado de la solicitud de autenticación y, si se deniega el acceso, la razón por la que era negado. En el campo Descripción de las propiedades de evento, la línea Razón dice por qué falla la autenticación.
Las dos fallas comunes son: mal nombre de usuario y contraseña, cuando un usuario introduce credenciales incorrectas; y "permiso de acceso remoto para la cuenta de usuario se le negó" cuando la cuenta de usuario se establece en Denegar
Las políticas de acceso o el acceso remoto configurados en la NIC no permiten el acceso de ese usuario. Si la NIC está el registro que la autenticación se ha realizado correctamente, pero el cliente está recibiendo un mal nombre de usuario o contraseña
mensaje, el secreto RADIUS configurado en NIC y pfSense no coincide.

Filtrado de contenido gratuito con OpenDNS

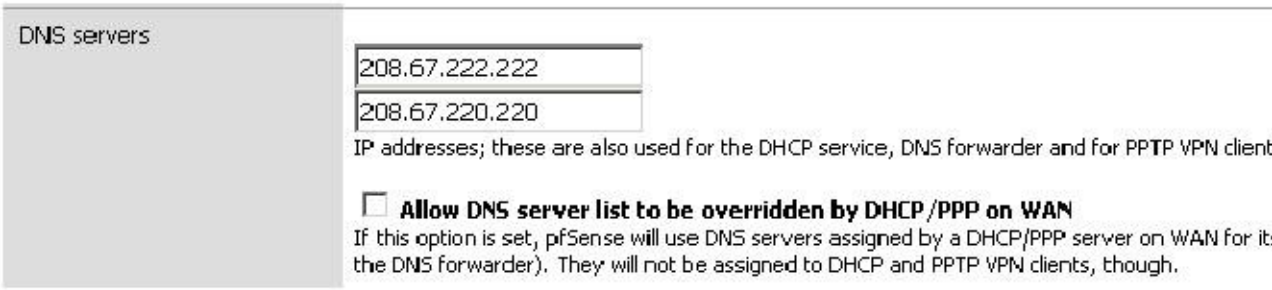
pfSense no incluye ningún software de filtrado de contenidos en el momento de escribir esto, pero hay un gran libre opción en la integración de OpenDNS [http://www.opendns.com]. Primero tendrá que configurar su red
utilizar los servidores DNS de OpenDNS para todos queries.1 recursiva

Configuración de pfSense utilizar OpenDNS

Visite el Sistema Página Configuración general, introduzca dos servidores DNS de OpenDNS allí, y desactive la "Permitir que la lista de servidores DNS para ser anulado por DHCP / PPP en WAN" caja (Figura 28.6, "Configuración de
OpenDNS en pfSense ").

[1]Nota: Yo soy de ninguna manera relacionada con OpenDNS, sólo un usuario muy satisfecho de sus servicios en varias ubicaciones, y he tenido numerosas la gente me agradece por mí refiriéndose a ellos. Ellos realmente tienen una oferta impresionante.

Figura 28.6. Configuración de OpenDNS en pfSense



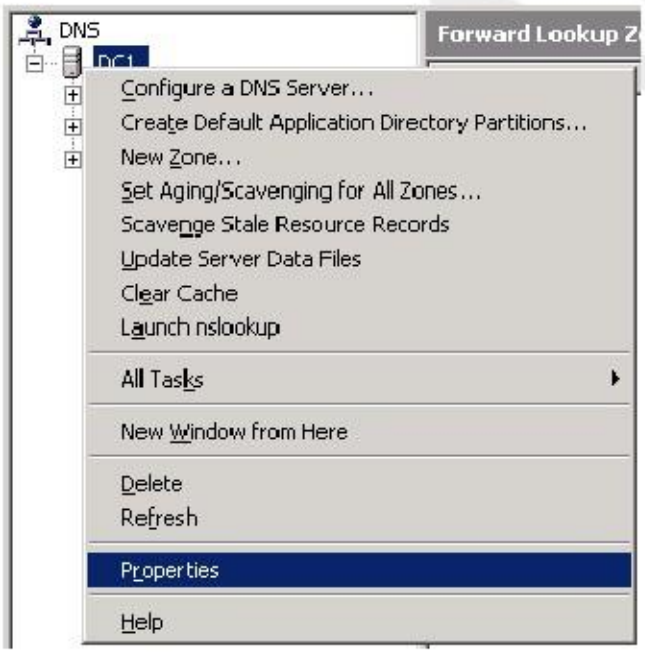
Si sus máquinas internas utilizan reenviador DNS de pfSense como único servidor DNS, esto es todo lo que necesita cambiar de utilizar OpenDNS para su resolución de nombres.

Configurar los servidores DNS internos para utilizar OpenDNS

Si sus equipos internos utilizan un servidor DNS interno, tiene que ser configurado para enviar su recursiva consultas a los servidores de OpenDNS. Voy a explicar cómo lograr esto con el DNS de Windows Server servidor.

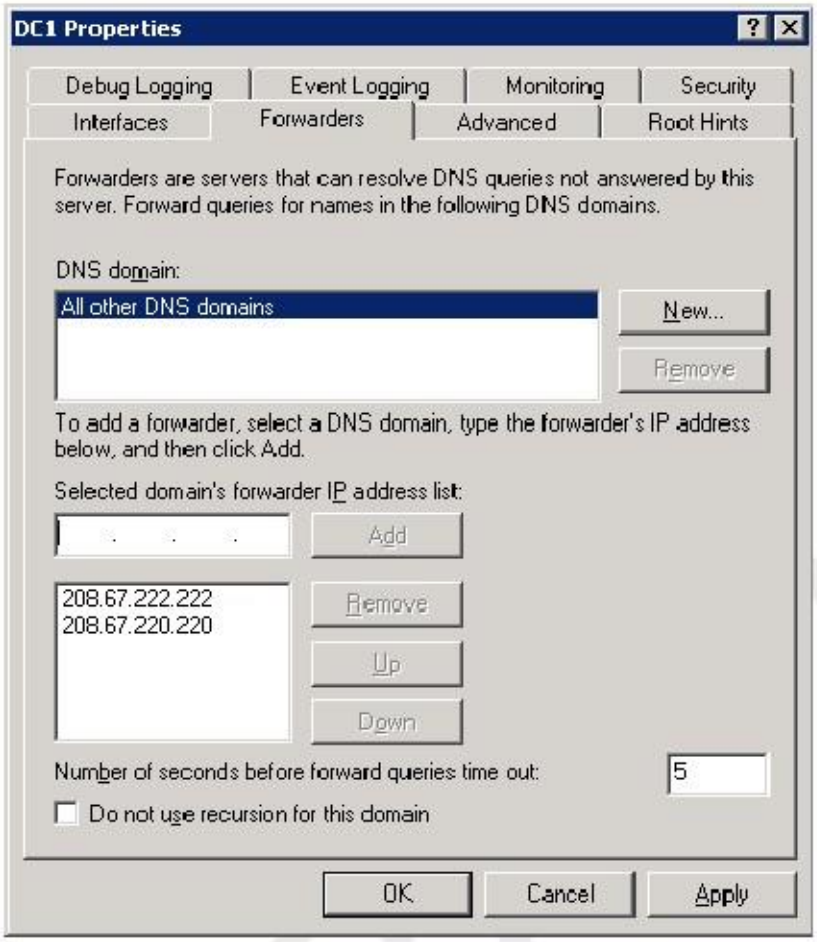
Configuración de Transitarios en DNS de Windows Server

Figura 28.7. Propiedades de DNS de Windows Server



Abra la MMC de DNS en Herramientas administrativas, DNS. Haga clic derecho sobre el nombre del servidor y haga clic en Propiedades, como se muestra en la Figura 28.7, "Propiedades de DNS de Windows Server".

Figura 28.8. De Windows Server Forwarders DNS



Seleccione la ficha reenviadores, y añadir dos servidores DNS de OpenDNS en la lista de transitario para "Todos los demás
Dominios DNS ", como en la Figura 28.8," Windows Server DNS Transportadoras ", a continuación, haga clic en Aceptar.
A continuación, repita esto para cada uno de los servidores DNS
internos.

Filtrado OpenDNS Configuración de contenido

Ahora tiene que configurar el filtrado de contenido como desee en el sitio de OpenDNS.

Regístrese para obtener una cuenta de OpenDNS

Busque http://www.opendns.com y haga clic en el vínculo Iniciar sesión. Luego haga clic en el "Crear una cuenta gratis" vincular y pasar por el proceso de creación de la cuenta.

Definir la red (s) en OpenDNS

Figura 28.9. Adición de una red

OpenDNS primero tiene que ser capaz de determinar qué DNS consultas son de su red para poder
para filtrar de acuerdo a las políticas definidas en su cuenta. Después de iniciar sesión en su cuenta de OpenDNS,
haga clic en la ficha Redes (Figura 28.9, "Adición de una red"). Se mostrará automáticamente la dirección IP pública de su
Sesión HTTPS está viniendo, con un botón para agregar esta red a su cuenta. Haga clic en el cuadro Agregar este botón de la red.

Con ello se abre una ventana preguntándole si su dirección IP es estática o dinámica (Figura 28.10, "Adición una conexión IP dinámica "). Si usted tiene una conexión IP dinámica, tendrá que ejecutar los OpenDNS Updater para Windows en una máquina dentro de la red para asegurarse de que su dirección se mantiene al día con OpenDNS. Su dirección IP es el único medio de identificación OpenDNS tiene de su red. Si su IP no es correcta en la configuración de OpenDNS, el filtrado de contenidos no funcionará como se configura en su cuenta.

Para conexiones IP estáticas, desactive la casilla "Sí, es dinámica" caja y dar a la conexión un nombre (Figura 28.11, "Adición de una conexión de IP estática"). Para conexiones IP estáticas, que no es necesario para ejecutar la
cliente de actualización.

Después de añadir la red a su cuenta, usted lo verá en la lista de redes como la de la figura 28.12, "Red añadido correctamente".

Su red está lista para utilizar OpenDNS, aunque todavía no ha configurado su contenido deseado configuración de filtrado.

Configuración de los ajustes de filtrado de contenidos para su cuenta

Para configurar las opciones de filtrado de contenido, haga clic en la ficha Configuración en la parte superior de la página web de OpenDNS.
, Debería aparecer "Contenido nivel de filtrado" Una lista de niveles como el de la figura 28.13. Verá su nivel de filtrado actual es mínima, lo que bloquea los sitios de phishing conocidos solamente. Puede seleccionar entre cuatro
diferentes niveles de filtrado predefinidas, o elija Personalizado y seleccione las categorías que desea bloquear.
También puede bloquear o permitir determinados dominios, ignorando la configuración de filtrado de contenido general, en la parte inferior de esta pantalla (Figura 28.14, "Administrar dominios individuales").

OpenDNS ofrece una serie de otras opciones de configuración que le permite un gran control sobre DNS para su red. Su sitio contiene una serie de bases de apoyo y los artículos de conocimientos que detalla algunos de las posibilidades y toda la funcionalidad está bien descrita en toda la interfaz de gestión.
Usted no tiene que parar en el filtrado de contenido justo - revisar todo lo demás OpenDNS tiene para ofrecer, como usted puede ser capaz de poner a buen uso.

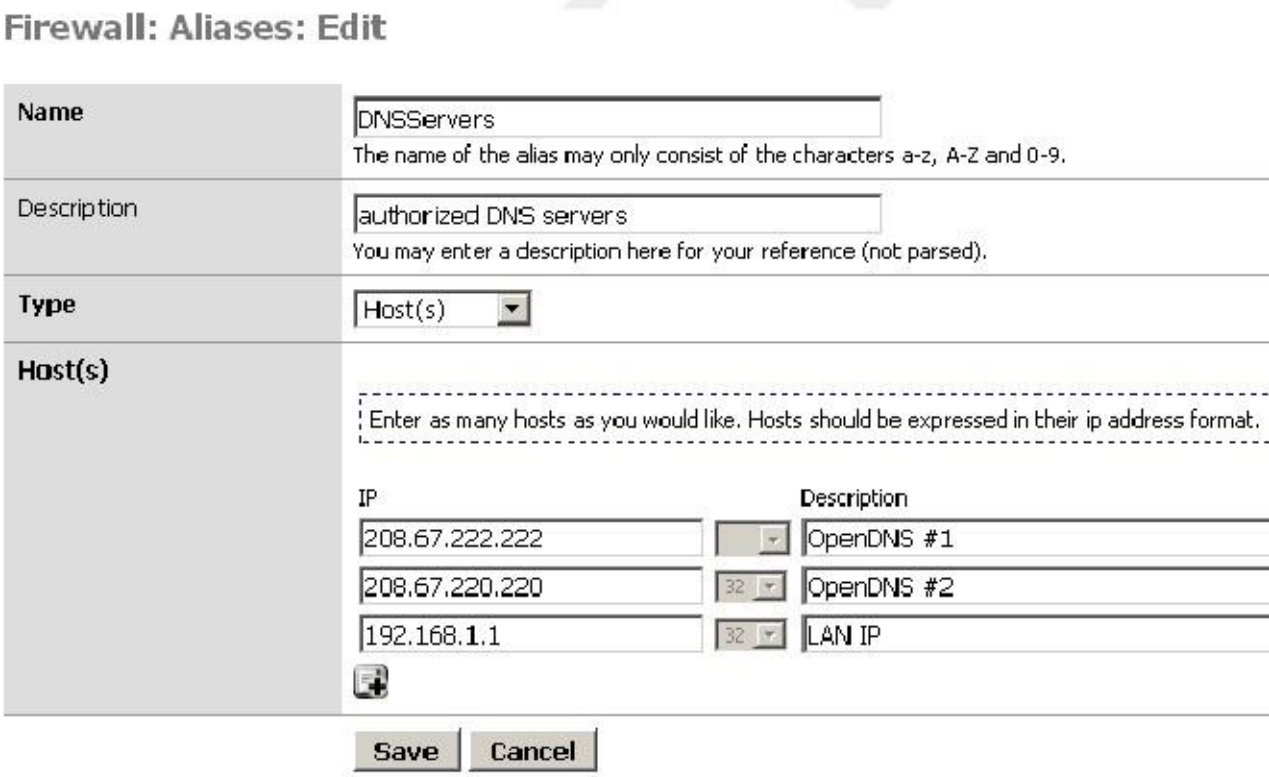
Configuración de las reglas del cortafuegos para prohibir otros DNS servidores

Ahora que sus sistemas internos están utilizando OpenDNS como su servicio de DNS, tendrá que configurar su firewall rige por lo que no otros servidores DNS se puede acceder. De lo contrario, los usuarios internos podría simplemente
cambiar sus máquinas (si tienen los derechos de usuario para hacerlo) para utilizar un servidor DNS diferente que hace no hacer cumplir su filtrado de contenidos y otras restricciones.

Crear un alias de DNS Servers

En primer lugar tendrá que crear un alias que contiene los servidores DNS que los equipos internos se les permite consulta, como el de la Figura 28.15, "servidores DNS alias". La IP LAN aparece porque este ejemplo
red utiliza el reenviador DNS como su servidor DNS interno, y esto permite que las consultas DNS de la LAN a la IP LAN. También permite consultas recursivas desde servidores DNS internos, así como la asignación directa de los servidores DNS de OpenDNS en las máquinas internas. Tenga en cuenta que a menos que deshabilite la regla anti-bloqueo,
no es necesario añadir la IP LAN aquí, pero recomiendo agregarlo independientemente para mayor claridad. Referirse a la sección llamada "Regla Anti-bloqueo" para obtener más información.

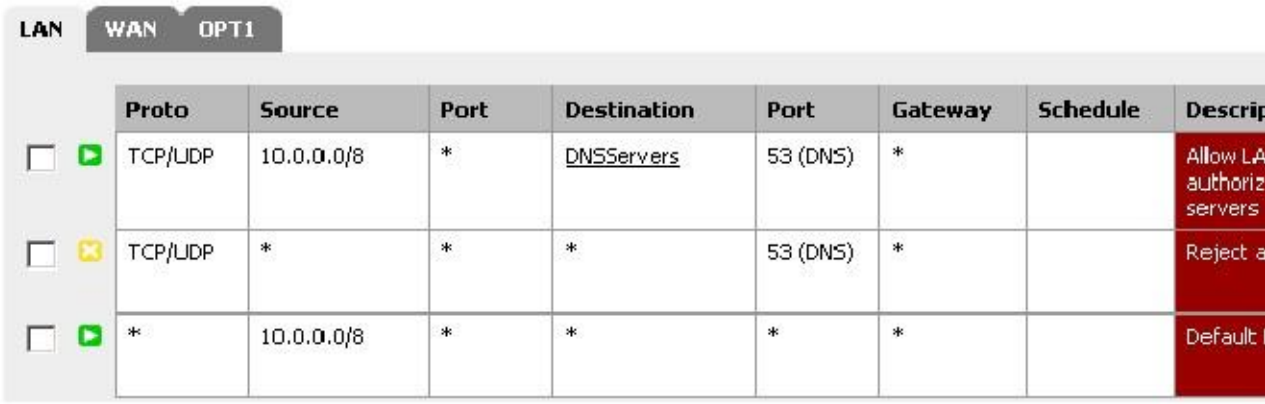
Figura 28.15. Servidores DNS alias



Configurar reglas de firewall

Ahora tiene que configurar sus reglas de LAN para permitir DNS destinado a los alias creados con anterioridad, y bloquear el DNS para otros destinos si alguna de sus otras reglas permitirían DNS, tales como el valor predeterminado Regla de LAN. Como se discutió en el capítulo de firewall, yo prefiero usar rechazar reglas para el tráfico bloqueado en interior
interfaces. El conjunto de reglas en la Figura 28.16, "reglas de LAN para restringir DNS" es corto y simple para la aras de la ilustración - Recomiendo significativamente más fuerte filtrado de salida de esta muestra, tal como se describe en el capítulo cortafuegos.

Figura 28.16. LAN normas para restringir DNS



Finalización y otras preocupaciones

Y eso es todo. Ahora dispone de una solución de filtrado de contenido gratuito integrado con pfSense en un medio que hace que sea muy difícil para el usuario medio para desplazarse. Tenga en cuenta que no es imposible de recorrer, especialmente con tan permisiva de un conjunto de reglas que en el ejemplo de arriba muestra. Hay varias posibilidades para DNS túnel a través de ese conjunto de reglas, con las conexiones VPN, el reenvío de puertos SSH, y más. Pero si usted permite que todo el tráfico a través del firewall, que siempre va a ser una posibilidad. Correctamente bloqueado máquinas de los usuarios finales en combinación con lo anterior proporciona una sólida solución de filtrado de contenido eso es difícil moverse.

Syslog Server en Windows con Kiwi Syslog

pfSense puede enviar los registros a un servidor externo a través del protocolo syslog (la sección llamada "Registro remoto
con Syslog "). Para usuarios de Windows, Kiwi Syslog Server2 es una opción libre agradable para recoger registros de su pfSense instala. Se puede instalar como un servicio para la recopilación de registros a largo plazo, o correr como una aplicación
para las necesidades de corto plazo. Es compatible con las versiones de servidor y escritorio de Windows 2000 y más reciente. La instalación es sencilla y no requiere de mucha configuración. Se puede encontrar ayuda en su documentación después de la instalación.

Uso del software del Sistema de Puertos de FreeBSD (Paquetes)

Debido pfSense se basa en FreeBSD, para un veterano administrador del sistema FreeBSD que muchos conocen Paquetes de FreeBSD también se pueden utilizar. Instalación del software de esta manera no es para los inexpertos, ya que
podría tener efectos secundarios no deseados, y no se recomienda ni admite. Muchas partes de FreeBSD no están incluidos, por lo que la biblioteca y otros temas se pueden encontrar. pfSense no incluye un compilador en el sistema base por muchas razones, y, como tal, el software no puede ser construida localmente. Sin embargo, puede instalar paquetes desde la pre-construido repositorio de paquetes de FreeBSD.

Preocupaciones / Advertencias

Antes de decidirse a instalar software adicional para pfSense que no es un paquete sancionado, hay algunos temas que necesitan ser tomadas en cuenta.

[2] http://www.kiwisyslog.com/

Las preocupaciones de seguridad

Cualquier software adicional agregado a un servidor de seguridad es un problema de seguridad, y debe ser evaluado por completo antes
instalación. Si la necesidad es mayor que el riesgo, puede ser vale la pena correr. Los paquetes oficiales pfSense no son inmune a este problema. Cualquier servicio adicional es otro vector de ataque potencial.

Las preocupaciones de rendimiento

La mayoría de los sistemas de pfSense se ejecutan en hardware que puede manejar la carga de tráfico con los que tienen la tarea.
Si usted encuentra que usted tiene potencia de sobra, no puede lastimar el sistema para agregar software adicional. Dicho esto, ser conscientes de los recursos que serán consumidos por el software añadido.

Software en conflicto

Si instala un paquete que duplica la funcionalidad que se encuentra en el sistema base, o sustituye una base paquete de sistema con una nueva versión, que podría causar inestabilidad en el sistema impredecible. Asegúrese de que el
software que está después no existe en el sistema de pfSense antes de tratar de instalar nada.

La falta de integración

Cualquier software adicional instalado no tendrá la integración GUI. Para algunos, esto no es un problema, pero ha habido personas que vayan a instalar un paquete y tienen un GUI aparece por arte de magia por su configuración. Tendrá que ser configurado manualmente Estos paquetes. Si se trata de un servicio, lo que significa también
asegurándose de que todos los scripts de inicio se modifican para adaptarse a los métodos utilizados por pfSense.

También ha habido casos en los que el software se ha instalado páginas web adicionales que no están protegidas por proceso de autenticación de pfSense. Pruebe cualquier software instalado para asegurar que el acceso está protegido o filtrada de alguna manera.

La falta de copias de seguridad

Al instalar los paquetes de esta manera, usted debe asegurarse de que usted copia de seguridad de cualquier configuración o de otro
archivos necesarios para este software. Estos archivos no se copiarán durante una copia de seguridad y normal pfSense podrían perderse o cambiado durante una actualización de firmware. Usted puede utilizar el paquete add-on se describe en el
sección llamada "Archivos de copia de seguridad y directorios con el Paquete de copia de seguridad" para los archivos de copia de seguridad arbitrarias tales
como estos.

Instalación de paquetes

Para instalar un paquete, primero debe asegurarse de que el sitio de paquete apropiado será utilizado. pfSense es compilados contra una rama específica de FreeBSD-RELEASE y los paquetes allí pueden llegar a ser rancio dentro de un corto período de tiempo. Para solucionar este problema, especifique la ruta de acceso al conjunto de paquetes para
-FreeBSD estable antes de intentar instalar un paquete:

```
#setenv PACKAGESITE = ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-7-sta
#pkg_add-r flujo TCP
```

O bien, puede suministrar una URL completa para un
paquete:

```
#pkg_add-r ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-7-stable/Late
```

El paquete debe descargar e instalar, junto con las dependencias necesarias.

También es posible construir un paquete personalizado en otro equipo que ejecute FreeBSD y luego copiar / instalar el archivo de paquete generado en un sistema pfSense. Debido a la complejidad de este tema, no lo hará ser cubiertos aquí.

El mantenimiento de los paquetes

Puede ver una lista de todos los paquetes instalados de este modo:

#pkg_info

Para eliminar un paquete instalado, debe especificar el nombre completo o utilizar un comodín:

#pkg_delete lsof-4.82, 4
#pkg_delete flujo TCP-\ *

Capítulo 29. Paquete de Captura

La captura de paquetes es el medio más eficaz de solución de problemas con la conectividad de red. Paquete de captura (o "sniffing") herramientas como tcpdump mostrar lo que es "en el cable" - que entra y salir de una interfaz. Al ver cómo el tráfico es recibido por el servidor de seguridad y cómo se sale del cortafuegos es una gran ayuda en la reducción a problemas con las reglas del cortafuegos, entradas de NAT y otras redes cuestiones. En este capítulo, cubrimos la obtención de paquetes de captura de la WebGUI, con tcpdump al línea de comandos en un shell, y el uso de Wireshark.

Capturar fotograma de referencia

Tenga en cuenta que el paquete captura mostrar lo que está en el alambre. Es el primero en ver el tráfico cuando se recibe paquetes y última para ver el tráfico de la hora de enviar los paquetes a medida que fluyen a través del firewall. Ve el tráfico
antes de firewall, NAT, y todos los demás procesos en el servidor de seguridad pasa por el tráfico que viene en esa interfaz, y después de todo lo que se produce el procesamiento de tráfico que sale de esa interfaz. Para el tráfico entrante, capturas mostrarán el tráfico que llega a esa interfaz en el servidor de seguridad, independientemente de si esa tráfico será bloqueado por la configuración de su firewall. Figura 29.1, "Referencia de captura", ilustra donde tcpdump y también WebGUI paquetes de captura lazos de interfaz en el orden de procesamiento.

Selección de la interfaz adecuada

Antes de empezar cualquier captura de paquetes, lo que necesita saber desde donde se debe tomar la captura. Una captura de paquetes se verá diferente dependiendo de la interfaz elegida, y en ciertos escenarios es mejor para capturar en una interfaz específica, y en otros, la ejecución de varias capturas simultáneas en diferentes interfaces es preferible. En utilizando tcpdump en la línea de comandos, tendrá que saber la nombres "reales" de interfaz que van con los nombres descriptivos se muestran en la WebGUI. Usted puede recordar éstos
de cuando las interfaces se asignaron originalmente, pero si no, usted puede visitar Interfaces (Asignar) y tome nota de que las interfaces físicas, como `fxp0,` corresponden con las interfaces Pfsense, tales como WAN. Tabla 29.1, "El Real Interfaz vs nombres descriptivos" lista algunos nombres de interfaz que se puede encontrar, dependiendo de su configuración.

Tabla 29.1. Bienes Interfaz vs nombres descriptivos

Bienes / Nombre físico	Nombre descriptivo
ng0 ... ng <x>	Clientes WAN (PPPoE o PPTP WAN) o PPTP
ENC0	IPsec, el tráfico cifrado
tun0 ... tun <x>	OpenVPN, el tráfico cifrado
lo0	Interfaz de bucle invertido
pfsync0	interfaz pfsync - utilizado internamente
pflog0	registro de pf - utilizado internamente

Cuando se selecciona una interfaz, normalmente deseará comenzar con el lugar donde los flujos de tráfico en pfSense. Por ejemplo, si usted está teniendo problemas para conectarse a un puerto hacia adelante desde fuera de su red, inicio con la interfaz WAN ya que es donde se origina el tráfico. Alternativamente, si usted tiene un PC cliente que no puede acceder a Internet, comenzar con la interfaz LAN. En caso de duda, pruebe con múltiples interfaces y el filtro para las direcciones IP o puertos en cuestión.

Limitar el volumen de captura

Cuando la captura de paquetes, es importante limitar el volumen de los paquetes capturados, pero aún así asegurar que todos
tráfico relevante para el problema que se está troubleshooted es capturado. En la mayoría de las redes, al capturar sin filtrar el tráfico capturado, incluso con capturas de cortos plazos, se termina con un enorme

cantidades de datos para cavar a través de encontrar el problema. Puedes realizar un filtrado posterior a la captura mediante el uso de filtros de visualización
en Wireshark, pero filtrando adecuadamente en el momento de la captura es preferible mantener el archivo de captura tamaño abajo. Los filtros se analizan más adelante en este capítulo.

Captura de paquetes desde los WebGUI

La WebGUI ofrece un frontal fácil de utilizar para tcpdump que le permitirá obtener capturas de paquetes que a continuación, se puede ver o descargar de un análisis más profundo en Wireshark. Debido a su simplicidad, que puede sólo ofrecen algunas opciones limitadas para filtrar el tráfico deseada, lo que puede complicar la tarea en función en el nivel de tráfico de la red y las necesidades de filtrado. Dicho esto, para muchas personas es suficiente y se hace el trabajo. Si usted se siente limitado por las opciones disponibles, no dude en pasar a la siguiente sección sobre el uso de tcpdump directamente.

Conseguir una captura de paquetes

En primer lugar, vaya a Diagnósticos Captura de paquetes para iniciar el proceso. A partir de ahí, elegir la Interface en el que usted desea capturar el tráfico. Si desea filtrar el tráfico que va hacia o desde un específico el anfitrión, introduzca su dirección IP en el campo Dirección del host. El puerto también puede ser limitada si está capturando
El tráfico TCP o UDP.

Puede ajustar Longitud del paquete capturado si se desea. Por lo general, usted querrá el paquete completo, pero para captura funcionar durante períodos de tiempo donde las cabeceras ser más importante que la carga útil de los paquetes más largos,
limitar esta a 64 bytes o menos se traducirá en un archivo de captura mucho más pequeña que puede tener aún adecuada datos para solucionar problemas. El cuadro Recuento determina cuántos paquetes para capturar antes detenerse. Si no limitar la captura de ninguna manera, tener en cuenta que esto puede ser muy "ruidosa" y puede que tenga que aumentar este mucho más grande que el valor por defecto de 100.

El Nivel de opción Detalle sólo afecta a la salida, como se muestra cuando finaliza la captura. No hace cambiar el nivel de detalle en el archivo de captura si decides descargarlo cuando esté terminado.

No se recomienda generalmente para comprobar Reverse DNS búsquedas cuando se realiza una captura, ya que retrasará la salida como se realiza el DNS inverso. También es comúnmente más fáciles de solucionar problemas cuando ver las direcciones IP en lugar de nombres de host y DNS inverso a veces puede ser inexacta. Esta lata ser útil en ocasiones sin embargo.

Pulse Iniciar para empezar la captura de datos. La pantalla mostrará el mensaje "Packet Capture está funcionando" a través del
parte inferior, lo que indica la captura está en proceso. Pulse Detener para finalizar la captura y ver la salida. Si especificado un máximo de paquete cuenta se detendrá automáticamente cuando se alcance esa cuenta, o puede clic Deténgase para acabar con ella en cualquier momento.

Visualización de los datos capturados

La salida de la captura se puede ver en el WebGUI o descargarse para su posterior visualización en un programa como Wireshark. Para obtener más detalles sobre el uso de Wireshark para ver un archivo de captura, consulte la sección llamada
"Visualización de paquetes de captura de archivos" más adelante en este capítulo. Haga clic en Descargar Capture para descargar este archivo
para su posterior visualización.
El resultado que se muestra en los paquetes marco capturadas se muestran en la norma tcpdump estilo.

Utilizando tcpdump desde la línea de comandos

tcpdump es la línea de comando de la utilidad de captura de paquetes siempre con la mayor parte de UNIX y UNIX distribuciones de sistemas operativos, incluyendo FreeBSD. También se incluye con pfSense, y utilizables a partir de una shell en la consola o por SSH. Es una herramienta muy poderosa, pero que también hace que sea desalentador para el usuario no iniciados. La tcpdump binario en FreeBSD 7.2 soporta 36 indicadores de línea de comandos diferentes, posibilidades ilimitadas con expresiones de filtro, y su página de manual, proporcionando sólo un breve resumen de todos

sus opciones, es cerca de 30 páginas impresas 8.5x11 "de largo. Después de aprender a usarlo, usted también debe saber cómo
para interpretar los datos que proporciona, lo cual puede requerir una comprensión en profundidad de los protocolos de red.
Una revisión completa de captura de paquetes y la interpretación de los resultados se encuentra fuera del alcance de este libro. De hecho, libros enteros se han escrito sobre este tema solo. Para aquellos con sed de más de conocimientos básicos en la materia, se proporcionan algunas recomendaciones para la lectura adicional en el final de este capítulo. Esta sección está pensada para proporcionar una introducción a este tema, y te dejan con el conocimiento suficiente para solucionar problemas básicos.

tcpdump indicadores de línea de comandos

En la siguiente tabla se muestran los indicadores de línea de comandos más utilizados con tcpdump. Cada opción se discutirá con más detalle en esta sección.

Tabla 29.2. Banderas tcpdump uso común

Bandera	Descripción
`-I` <interface>	Escuchar en el <interface>, . Por ejemplo, `-I fxp0`
`-N`	No resolver IPs utilizando DNS inversa.
`-W` <filename>	Guardar la captura en formato pcap a <filename>, por ejemplo, `-w / tmp / wan.pcap`
`-S`	Ajustar la longitud - la cantidad de datos a ser capturado 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 encabezado de capa de enlace en cada línea. Muestra el origen y destino la dirección MAC y VLAN etiquetar información sobre el tráfico etiquetado.

-I

La `-I` bandera especifica la interfaz en la que tcpdump escuche. Utiliza nombre de la interfaz de FreeBSD aquí, tales como `fxp0, em0, rl0,` etcétera

-N

No resolver IPs utilizando DNS inversa. Cuando no se especifica esta opción, tcpdump llevará a cabo un revertir DNS (PTR) de búsqueda para cada dirección IP. Esto genera una cantidad significativa de tráfico de DNS en las capturas al mostrar grandes volúmenes de tráfico. Es posible que desee desactivar esto 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 la realización de la búsqueda inversa. También las direcciones IP suelen ser más fáciles para leer y comprender que sus registros PTR. Esa es una cuestión de preferencia personal, sin embargo, y en entornos estoy familiarizado con el lugar donde yo sé los registros PTR proporcionarán los nombres de host reales de los dispositivos, que pueden funcionar 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 forma remota una preocupación, es que si quieres ser "astuto". Uno de los medios de detección de captura de paquetes está en busca de espigas
y los patrones en las búsquedas de DNS PTR.

-W

tcpdump le permite guardar archivos de captura en formato pcap, para su posterior análisis o análisis en otro sistema. Esto se hace habitualmente desde la línea de comandos sólo dispositivos como pfSense por lo que el archivo puede ser
copiado en un host que ejecuta Wireshark [http://www.wireshark.org] u otro protocolo de red gráfica

analizador y revisado allí. Al guardar un archivo utilizando `-W`, las tramas no se mostrarán en su terminal como que de otro modo son. (Consulte la sección "Uso de Wireshark con pfSense" sobre el uso de Wireshark con pfSense.)

Bandera-s

Por defecto, cuando se captura a un archivo, tcpdump sólo ahorrará los primeros 64 bytes de cada trama. Es suficiente para obtener la IP y el encabezado de protocolo para la mayoría de los protocolos, pero limita la utilidad de los archivos de captura.
Mediante el uso de la `-S` bandera, se puede decir tcpdump qué parte de la estructura para capturar, en bytes. Esto se llama
la longitud de resorte.

Tabla 29,3. Ejemplos de uso de tcpdump-s

Bandera	Descripción
`-S 500`	Capture los primeros 500 bytes de cada trama
`-S 0`	Captura cada cuadro en su totalidad

Por lo general, que desee utilizar `-S 0` cuando se captura a un archivo para su análisis en otro sistema. El único excepción a esto es los escenarios donde se necesita para capturar una gran cantidad de tráfico a través de un largo período de tiempo. Si conoce la información que está buscando se encuentra en el encabezado, puede guardar sólo la por defecto 64 bytes de cada trama y obtener la información que necesita, al tiempo que reduce significativamente el tamaño
del archivo de captura resultante.

-C

Puede indicar a tcpdump para capturar un cierto número de marcos y luego la salida mediante el uso de la `-C` bandera. Ejemplo de uso: la salida de tcpdump voluntad después de capturar 100 imágenes especificando `-C 100.`

Bandera-p

Normalmente, cuando la captura de tráfico con tcpdump, pone su interfaz de red en modo promiscuo.
Cuando no está funcionando en modo promiscuo, su NIC sólo recibe las tramas destinadas por su propia MAC de dirección, así como de difusión y multidifusión direcciones. Cuando se enciende en modo promiscuo, el interfaz muestra cada fotograma en el cable. En una red conmutada, por regla general, tiene poco impacto en su captura. En las redes donde el dispositivo está capturando desde está conectado a un concentrador, usando `-P` puede limitar significativamente el ruido en su captura cuando el único tráfico de interés es que desde y hacia el sistema desde el que se está capturando.

Bandera-v

La `-V` bandera controla el detalle o la verbosidad de la salida. El uso de más opciones "v" brinda mayor detalle, así que usted puede utilizar `-V,-vv,` o `-Vvv` para ver aún más detalle en la salida impresa a la consola. Este opción no afecta el detalle almacenado en un archivo de captura cuando se utiliza el `-W` cambiar, pero en su lugar hacer que el proceso de informar el número de paquetes capturados cada 10 segundos.

Indicador-e

Normalmente tcpdump no muestra ninguna información de capa de enlace. Especificar `-E` para mostrar el origen y direcciones MAC de destino y la información de etiquetas VLAN para el tráfico etiquetado con VLANs 802.1q.

Ejemplo de captura sin-e

Esta captura muestra la salida predeterminada, que no contiene información de capa de enlace.

```
#tcpdump-ni em0-c 5
tcpdump: salida detallada suprimida, el uso-v o-vv para decodificar protocolo completo
escuchando en em0, enlace de tipo EN10MB (Ethernet), el tamaño de captura de 96 bytes
```

```
23:18:15.830706 IP   10.0.64.210.22> 10.0.64.15.1395: P 2023587125:2023587241 (116
23:18:15.830851 IP   10.0.64.210.22> 10.0.64.15.1395: P 116:232 (116) ack 1 victoria 65
23:18:15.831256 IP   10.0.64.15.1395> 10.0.64.210.22:. ack 116 win 65299
23:18:15.839834 IP   10.0.64.3> 224.0.0.18: VRRPv2, Publicidad, vrid 4, prio 0
23:18:16.006407 IP   10.0.64.15.1395> 10.0.64.210.22:. ack 232 win 65183
5 paquetes capturados
```

Ejemplo de captura utilizando-e

Aquí puede ver la información de la capa de enlace incluido. Tenga en cuenta los de origen y destino direcciones MAC en
Además de las direcciones IP de origen y destino.

#tcpdump-ni em0-e-c 5

```
tcpdump: salida detallada suprimida, el uso-v o-vv para decodificar protocolo completo
escuchando en em0, enlace de tipo EN10MB (Ethernet), el tamaño de captura de 96 bytes
23:30:05.914958 00:0 c: 29:0 b: c3: ed> doce y trece: d4: f7: 73: d2, ethertype IPv4 (0x
23:30:05.915110 00:0 c: 29:0 b: c3: ed> doce y trece: d4: f7: 73: d2, ethertype IPv4 (0x
23:30:05.915396 doce y trece: d4: f7: 73: d2> 00:0 c: 29:0 b: c3: ed, ethertype IPv4 (0x
23:30:05.973359 00:00:5 e: 00:01:04> 01:00:05 e: 00:00:12, ethertype IPv4 (0x0800),
23:30:06.065200 doce y trece: d4: f7: 73: d2> 00:0 c: 29:0 b: c3: ed, ethertype IPv4 (0x
5 paquetes capturados
```

tcpdump Filtros

En la mayoría de los servidores de seguridad, tcpdump sin filtros producirán tanto de salida que va a resultar muy difícil para encontrar el tráfico de interés. Hay numerosas expresiones de filtrado disponibles que le permiten limitar el tráfico muestra o se capturó sólo a lo que usted está interesado pulg

Filtros de host

Para filtrar por un host específico, añada `anfitrión` y la dirección IP a la tcpdump comando. Para filtrar por el anfitrión 192.168.1.100 puede utilizar el siguiente comando.

#tcpdump-ni 192.168.1.100 anfitrión em0

Eso capturar todo el tráfico hacia y desde ese host. Si sólo desea capturar tráfico que se inició por ese host, puede utilizar el `src` Directiva.

#tcpdump-ni em0 src 192.168.1.100 anfitrión

Del mismo modo, también puede filtrar el tráfico destinado a esa dirección IP especificando `dst.`

#tcpdump-ni dst em0 192.168.1.100 anfitrión

Filtros de red

Filtros de red le permiten optimizar su captura a una subred específica utilizando el `neto` expresión.
Siguiente `neta,` puede especificar una cuaterna (192.168.1.1), salpicado de triple (192.168.1), salpicado par (192,168) o simplemente un número (192). Una cuaterna es equivalente a especificar `el anfitrión,` un punteado
triples utiliza una máscara de subred 255.255.255.0, un par de puntos utiliza 255.255.0.0 y usos varios solos 255.0.0.0.

El comando siguiente muestra el tráfico hacia o desde cualquier host con una dirección IP 192.168.1.x.

#tcpdump-ni em0 red 192.168.1

El siguiente comando es un ejemplo que captura el tráfico hacia o desde cualquier host con una dirección IP 10.xxx.

```
#tcpdump-ni em0 neto 10
```

Esos ejemplos se capturar todo el tráfico hacia o desde la red especificada. También puede especificar `src` o `dst` lo mismo que con `anfitrión` filtros para capturar sólo el tráfico iniciado por o destinado a la especificada red.

```
#tcpdump-ni em0 src neto 10
```

También es posible especificar una máscara CIDR como argumento para `net`.

```
#tcpdump-ni em0 src red 172.16.0.0/12
```

Filtros de protocolo y puerto

Precisar por host o red a menudo no es suficiente para eliminar el tráfico innecesario de tu captura. O puede que no se preocupan por el origen o destino del tráfico, y simplemente desean capturar un cierto tipo de tráfico. En otros casos es posible que desee filtrar todo el tráfico de un tipo específico de reducir ruido.

TCP y filtros de puerto UDP

Para filtrar los puertos TCP y UDP se utiliza el `puerto` Directiva. Esta captura tanto el tráfico TCP y UDP utilizando el puerto especificado ya sea como fuente o puerto de destino. Se puede combinar con `tcp` o `udp` a especificar el protocolo y `src` o `dst` para especificar un puerto de origen o destino.

Capturar todo el tráfico HTTP

```
#tcpdump-ni puerto tcp em0 80
```

Capturar todo el tráfico DNS

Capturar todo el tráfico DNS (normalmente UDP, pero algunas consultas utilizan TCP).

```
#puerto em0 tcpdump-ni 53
```

Filtros de protocolo

Puedes realizar un filtrado mediante protocolos específicos utilizando el `proto` Directiva. Protocolo se puede especificar mediante la Número de protocolo IP o uno de los nombres `ICMP`, `IGMP`, `IGRP`, `pim`, `ah`, `esp`, `vrrp`, `udp`, o `tcp`. Especificar `vrrp` también capturará tráfico CARP ya que los dos utilizan el mismo número de protocolo IP. Uno el uso común de la `proto` Directiva es filtrar el tráfico CARP. Debido a que los nombres normales de protocolo son palabras reservadas, deben ser escapados con una o dos barras invertidas, dependiendo del shell. La shell disponible en pfSense requiere dos barras invertidas para escapar de estos nombres de protocolo. Si recibe una error de sintaxis, compruebe que el nombre del protocolo se escapó correctamente. En la siguiente captura se muestran todas CARP y VRRP tráfico en la `em0` interfaz, que puede ser útil para asegurar que el tráfico está siendo CARP enviados y recibidos en la interfaz especificada.

```
#tcpdump-ni em0 proto \\ vrrp
```

Negando una coincidencia de filtro

Además de hacer coincidir los parámetros específicos, se puede negar una coincidencia de filtro especificando `no` en delante de la expresión de filtro. Si está solucionando algo distinto de CARP y su multicast latidos del corazón se saturan su salida de la captura, puede excluirlo de la siguiente manera.

```
#em0 tcpdump-ni no proto \\ vrrp
```

Combinación de filtros

Puede combinar cualquiera de los filtros mencionados utilizando `y` o `o`. Las siguientes secciones ofrecen algunos ejemplos.

Ver todo el tráfico HTTP hacia y desde un anfitrión

Para mostrar todo el tráfico HTTP desde la 192.168.1.11 host, utilice el siguiente comando.

#tcpdump-ni 192.168.1.11 anfitrión em0 y el puerto TCP 80

Ver todo el tráfico HTTP hacia y desde varios hosts

Para mostrar todo el tráfico HTTP desde la 192.168.1.11 hosts y 192.168.1.15, utilice el siguiente comando.

#tcpdump-ni 192.168.1.11 anfitrión em0 o 192.168.1.15 host y el puerto TCP 80

Filtrar uso la expresión

Las expresiones de filtro deben venir después de cada bandera de línea de comandos utilizado. Adición de cualquier bandera después de un filtro
expresión resultará en un error de sintaxis.

Ordenación incorrecta

#tcpdump-ni en1 proto \\ vrrp-c 2
```
tcpdump: error de sintaxis
```

Ordenación correcta

#tcpdump-ni en1-c 2 proto \\ vrrp
```
tcpdump: salida detallada suprimida, el uso-v o-vv para decodificar protocolo completo
escuchando en en1, enlace de tipo EN10MB (Ethernet), el tamaño de captura de 96 bytes
18:58:51.312287 IP 10.0.64.3> 224.0.0.18: VRRPv2, Publicidad, vrid 4, prio 0
18:58:52.322430 IP 10.0.64.3> 224.0.0.18: VRRPv2, Publicidad, vrid 4, prio 0
2 paquetes capturados
80 paquetes recibidos por el filtro
0 paquetes descartados por el kernel
```

Más acerca de Filtros

Esta sección cubre el más utilizado tcpdump filtrar expresiones, y probablemente cubre todos los sintaxis que va a necesitar. Sin embargo, esto apenas roza la superficie de las posibilidades. Hay muchos documentos en la web que cubre tcpdump en general, y específicamente el filtrado. Vea la sección llamada "Referencias adicionales" al final de este capítulo para obtener enlaces a referencias adicionales sobre el tema.

Ejemplos de solución de problemas prácticos

En esta sección se detalla un enfoque preferido por nosotros para solucionar algunos problemas específicos. Hay múltiples formas de abordar cualquier problema, pero rara vez se captura de paquetes puede ser vencido por su eficacia. Examinando el tráfico de transmisión proporciona un nivel de visibilidad de lo que realmente está sucediendo en el red

Puerto delantero no funciona

Usted acaba de agregar un puerto hacia adelante, y están tratando de usarlo desde un host en Internet, pero no dados. La pasos de solución de problemas descritos en la sección llamada "Port Forward Solución de problemas" ofrece una forma abordar esto, pero a veces la captura de paquetes es la única o la más fácil de encontrar la fuente de la problema.

Empezar desde WAN

En primer lugar usted necesita para asegurarse de que el tráfico está llegando a su interfaz WAN. Iniciar un tcpdump período de sesiones sobre
su interfaz WAN, y el reloj para el tráfico a venir pulg

```
#tcpdump-ni puerto tcp vlan0 5900
tcpdump: salida detallada suprimida, el uso-v o-vv para decodificar protocolo completo
escuchando en vlan0, enlace de tipo EN10MB (Ethernet), el tamaño de captura de 96 bytes
11:14:02.444006 IP 172.17.11.9.37219> 10.0.73.5.5900: S 3863112259:3863112259 (0
```

En este caso, vemos un paquete vienen en desde la WAN, por lo que está haciendo tan lejos. Tenga en cuenta que la primera parte
del protocolo de enlace TCP, un paquete con SYN solo set (el S se muestra), que nos está llegando. Si el futuro del puerto es
que trabaja verá un paquete SYN ACK en respuesta al SYN. Sin tráfico regreso visible, podría
ser una regla de firewall o el sistema de destino pueden ser inalcanzable (desactivado, sin escuchar a la especificada puerto, el host cortafuegos bloqueando el tráfico, etc.)

Compruebe la interfaz interna

El siguiente paso sería la de ejecutar un tcpdump sesión en la interfaz interna asociado con el puerto adelante.

```
#tcpdump-ni fxp0 puerto tcp 5900
tcpdump: salida detallada suprimida, el uso-v o-vv para decodificar protocolo completo
escuchando en fxp0, enlace de tipo EN10MB (Ethernet), el tamaño de captura de 96 bytes
11:14:38.339926 IP 172.17.11.9.2302> 192.168.30.5.5900: S 1481321921:1481321921
```

Mirando el tráfico interno, vemos que la conexión dejó la interfaz en el interior, y lo local
Dirección IP se ha traducido correctamente. Si esta dirección local coincida con la que esperaba, entonces tanto el puerto hacia adelante y la regla de firewall están funcionando correctamente, y la conectividad con el PC local debe ser confirmado por otros medios. Si usted vio ninguna salida en absoluto, entonces hay un problema con la regla de firewall o el delantero puerto puede haber sido definido incorrectamente. Para este ejemplo, yo había desconectado el PC.

IPsec túnel no se conecta

Porque tcpdump tiene un cierto conocimiento de los protocolos que se utilizan, que puede ser muy útil en calcular problemas fuera con túneles IPsec. Los próximos ejemplos muestran cómo ciertas condiciones de error puede presentarse en el seguimiento con tcpdump. Los registros de IPsec pueden ser más útiles en algunos
de los casos, pero esto se puede confirmar lo que en realidad se está viendo por el router. Para el tráfico cifrado, tales como
IPsec, captura de paquetes del tráfico es de menor valor que no se puede examinar la carga útil de los capturados paquetes sin parámetros adicionales, pero es útil para determinar si el tráfico desde el extremo remoto es alcanzando su firewall y qué fases completa.

Este primer túnel tiene un par inalcanzable:

```
#tcpdump-ni acogida vr0 192.168.10.6
tcpdump: salida detallada suprimida, el uso-v o-vv para decodificar protocolo completo
escuchando en vr0, enlace de tipo EN10MB (Ethernet), el tamaño de captura de 96 bytes


19:11:11.542976 IP 192.168.10.5.500> 192.168.10.6.500: ISAKMP: Fase 1 I agg
19:11:21.544644 IP 192.168.10.5.500> 192.168.10.6.500: ISAKMP: Fase 1 I agg
```

Este intento túnel tiene una PSK no coincidentes, observe cómo se intenta pasar a la fase 2, pero luego se detiene:

```
#tcpdump-ni acogida vr0 192.168.10.6
tcpdump: salida detallada suprimida, el uso-v o-vv para decodificar protocolo completo
escuchando en vr0, enlace de tipo EN10MB (Ethernet), el tamaño de captura de 96 bytes
19:15:05.566352 IP 192.168.10.5.500> 192.168.10.6.500: ISAKMP: Fase 1 I agg
19:15:05.623288 IP 192.168.10.6.500> 192.168.10.5.500: ISAKMP: Fase 1 R agg
19:15:05.653504 IP 192.168.10.5.500> 192.168.10.6.500: isakmp: 2/others fase I
```

Ahora la Fase 1 está bien, pero hay una falta de coincidencia en la información de la Fase 2. Se intentará repetidamente fase
2 de tráfico, pero no verá ningún tráfico en el túnel.

```
#tcpdump-ni acogida vr0 192.168.10.6
tcpdump: salida detallada suprimida, el uso-v o-vv para decodificar protocolo completo
```

```
escuchando en vr0, enlace de tipo EN10MB (Ethernet), el tamaño de captura de 96
bytes                                                                  1 I AGG
19:17:18.447952 IP 192.168.10.5.500> 192.168.10.6.500: ISAKMP: fase    1 R agg
19:17:18.490278 IP 192.168.10.6.500> 192.168.10.5.500: ISAKMP: fase    1 I AGG
19:17:18.520149 IP 192.168.10.5.500> 192.168.10.6.500: ISAKMP: fase    2/others R
19:17:18.520761 IP 192.168.10.6.500> 192.168.10.5.500: ISAKMP: fase    2/others I
19:17:18.525474 IP 192.168.10.5.500> 192.168.10.6.500: ISAKMP: fase    2/others I
19:17:19.527962 IP 192.168.10.5.500> 192.168.10.6.500: ISAKMP: fase
```

Por último, un túnel completamente de trabajo con tráfico en ambas direcciones después de la Fase 1 y la Fase 2 han terminado!

#tcpdump-ni acogida vr1 192.168.10.6

```
tcpdump: salida detallada suprimida, el uso-v o-vv para decodificar protocolo completo
escuchando en vr1, enlace de tipo EN10MB (Ethernet), el tamaño de captura de 96 bytes
21:50:11.238263 IP 192.168.10.5.500> 192.168.10.6.500: ISAKMP: Fase 1 I agg
21:50:11.713364 IP 192.168.10.6.500> 192.168.10.5.500: ISAKMP: Fase 1 R agg
21:50:11.799162 IP 192.168.10.5.500> 192.168.10.6.500: ISAKMP: Fase 1 I agg
21:50:11.801706 IP 192.168.10.5.500> 192.168.10.6.500: isakmp: 2/others fase I
21:50:11.812809 IP 192.168.10.6.500> 192.168.10.5.500: ISAKMP: 2/others fase R
21:50:12.820191 IP 192.168.10.5.500> 192.168.10.6.500: isakmp: 2/others fase I
21:50:12.836478 IP 192.168.10.6.500> 192.168.10.5.500: ISAKMP: 2/others fase R
21:50:12.838499 IP 192.168.10.5.500> 192.168.10.6.500: isakmp: 2/others fase I
21:50:13.168425 IP 192.168.10.5> 192.168.10.6: ESP (spi = 0x09bf945f, ss = 0x1), len
21:50:13.171227 IP 192.168.10.6> 192.168.10.5: ESP (spi = 0x0a6f9257, ss = 0x1), len
21:50:14.178820 IP 192.168.10.5> 192.168.10.6: ESP (spi = 0x09bf945f, ss = 0x2), len
21:50:14.181210 IP 192.168.10.6> 192.168.10.5: ESP (spi = 0x0a6f9257, ss = 0x2), len
21:50:15.189349 IP 192.168.10.5> 192.168.10.6: ESP (spi = 0x09bf945f, ss = 0x3), len
21:50:15.191756 IP 192.168.10.6> 192.168.10.5: ESP (spi = 0x0a6f9257, ss = 0x3), len
```

El tráfico que atraviesa un túnel IPsec

Con algunos ajustes adicionales para inicializar el proceso, también se puede ver el tráfico que atraviesa su IPsec túneles. Esto puede ayudar a determinar si el tráfico está tratando de llegar al otro extremo mediante el uso del túnel. En Las versiones anteriores a la versión 1.2.3, antes de tcpdump trabajará en la interfaz IPsec había que establecer dos sysctl variables que controlan lo que es visible para tcpdump. Si está utilizando 1.2.3 o posterior liberación, tcpdump funcionará sin ninguna manipulación adicional.

En el siguiente ejemplo, un host en un lado del túnel está enviando con éxito un eco ICMP petición (ping) a la parte más alejada, y recibir respuestas.

#sysctl-w net.enc.out.ipsec_bpf_mask = 0x00000001

```
net.enc.out.ipsec_bpf_mask: 0000000000 -> 0x00000001
```

#sysctl-w net.enc.in.ipsec_bpf_mask = 0x00000001

```
net.enc.in.ipsec_bpf_mask: 0000000000 -> 0x00000001
```

#ENC0 tcpdump-ni

```
tcpdump: ADVERTENCIA: ENC0: ninguna dirección IPv4 asignada
tcpdump: salida detallada suprimida, el uso-v o-vv para decodificar protocolo completo
escuchando en ENC0, enlace de tipo ENC (OpenBSD encapsulado IP), el tamaño de captura de
bytes
22:09:18.331506 (auténtico, confidencial): SPI 0x09bf945f:
                IP 10.0.20.1> 10.0.30.1:
                ICMP de solicitud de eco, 14140 id, 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:
                ICMP de respuesta de eco, id 14140, ss 0, longitud 64 (ipip proto-4)
22:09:19.336613 (auténtico, confidencial): SPI 0x09bf945f:
                IP 10.0.20.1> 10.0.30.1:
                ICMP de solicitud de eco, 14140 id, seq 1, longitud 64
22:09:19.339590 (auténtica y confidencial): SPI 0x0a6f9257:
                IP 192.168.10.6> 192.168.10.5: IP 10.0.30.1> 10.0.20.1:
                ICMP de respuesta de eco, id 14140, seq 1, longitud 64 (ipip proto-4)
```

Si el tráfico no estaba entrando en el túnel correctamente, usted no verá ninguna salida. Si hay un servidor de seguridad o problema de enrutamiento interno en el otro lado, es posible que vea el tráfico que sale, pero nada de vuelta.

Solución de problemas de salida NAT

Para entornos complejos donde es necesario Advanced Outbound NAT, tcpdump puede ser de gran asistencia en la solución de problemas de la configuración de NAT Saliente. Una buena captura de usar es la búsqueda de el tráfico con direcciones IP privadas en su interfaz WAN, como todo lo que ve en su WAN debe ser NAT a una IP pública. En la siguiente captura se mostrará ningún tráfico con RFC 1918 direcciones IP como origen o destino. Esto le mostrará a todo el tráfico que no coincide con uno de su salida NAT normas, proporcionando información para ayudar a revisar la configuración de NAT de salida para encontrar el problema.

```
#tcpdump-ni em0 neta 10 o netos 192,168 o red 172.16.0.0/12
```

Uso de Wireshark con pfSense

Wireshark, antes conocido como Ethereal, es una herramienta de captura de análisis de protocolo y GUI de paquetes que pueden
puede utilizar para ver y capturar el tráfico al igual que tcpdump. Es un software de código abierto y de libre acceso en http://www.wireshark.org/. También se puede utilizar para analizar archivos de captura generados por el pfSense WebGUI, tcpdump, Wireshark, o cualquier otro software que graba los archivos en el formato de archivo pcap estándar.

Viendo el Paquete de captura de archivo

Para ver un archivo de captura de Wireshark, inicie el programa y luego ir a Archivo Abrir. Localice la captura archivo, y luego haga clic en el botón Abrir. También puede hacer doble clic en cualquier archivo con un `. Pcap` extensión en
De Windows y OS X con la configuración predeterminada después de la instalación de Wireshark. Usted verá una pantalla similar
a la Figura 29.2, "Wireshark captura View" en el que se muestran los datos del archivo de captura.
Como se observa en la Figura 29.2, "Wireshark captura View", una lista que resume los paquetes en el archivo de captura se muestra en la lista de la parte superior, con un paquete por línea. Si hay demasiados, puede filtrar los resultados usando el botón Filtro de la barra de herramientas. Al hacer clic en un paquete, los marcos inferiores se mostrarán los detalles
de lo que se contiene. El primer panel inferior muestra un desglose de la estructura del paquete, y cada uno de estos elementos se puede ampliar para más detalles. Si el paquete es de un protocolo soportado, en algunos casos se pueden interpretar los datos y mostrar aún más detalles. El panel inferior muestra un hexadecimal y Representación ASCII de los datos contenidos en el paquete.

Visualización de la captura de esta manera, es fácil ver el flujo de tráfico con tanto o tan poco detalle como sea necesario.

Análisis Wireshark Herramientas

Mientras que algunos problemas requieren un considerable conocimiento de cómo funcionan los protocolos subyacentes, las herramientas de análisis integradas en Wireshark que ayuda a disminuir la necesidad de muchos protocolos. En el marco del Análisis de
y los menús de Estadísticas, encontrará algunas opciones para automatizar algunos de los análisis y proporcionan opiniones resumidas de lo que está contenido en la captura. Las opciones de Información de expertos en el marco del Análisis de
menú muestra una lista de los errores, advertencias, notas y conversaciones de red que figuran en la captura.

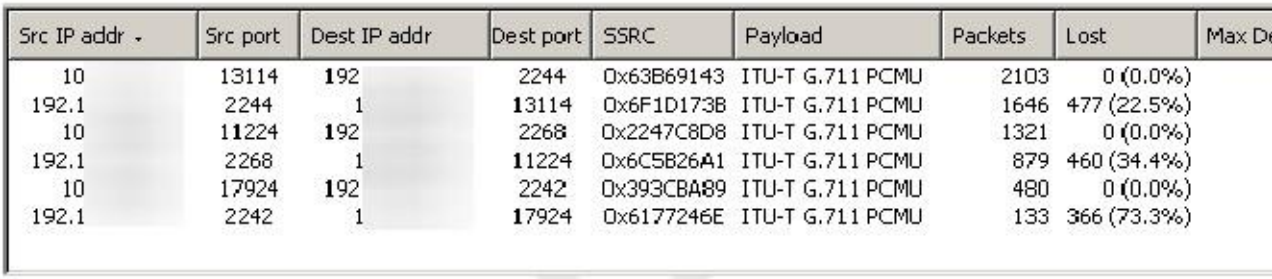
Nota

Usted verá comúnmente errores en Wireshark para checksums incorrectos. Esto es porque la mayoría NIC añadir la suma de comprobación de hardware directamente antes de ponerlo en el cable. Este es el único excepción a la nota anterior decía lo que se ve en una captura de paquetes es lo que está en el alambre. El tráfico enviado desde el sistema en el que se toma la captura tendrá checksums incorrectos donde se hacen en hardware, aunque el tráfico que viene desde un sistema remoto deben siempre tienen sumas de control correctas. Puede desactivar la descarga de suma de comprobación para asegurarse de que está
ver el tráfico como el anfitrión es ponerlo en el cable, aunque por lo general esto es algo que simplemente

ignorar. Si necesita verificar las sumas de comprobación, es probable que desee para capturar el tráfico de otro sistema utilizando un grifo o conmutador de red de puerto palmo.

El menú de la telefonía es un ejemplo de análisis automatizado Wireshark puede realizar para hacer más fácil para ver los problemas con VoIP. En este caso particular, el tráfico de VoIP atravesaba un circuito de MPLS WAN con los routers del proveedor conectado a la interfase OPT de pfSense en ambos lados. Una captura del la interfaz OPT en el extremo de iniciar mostró ninguna pérdida, lo que indica que el tráfico estaba siendo enviado a la enrutador de proveedor, pero la interfaz OPT en el extremo opuesto mostraron una considerable pérdida de paquetes en un solo
dirección cuando varias llamadas simultáneas fueron activos. Estas capturas de paquetes ayudaron a convencer a la proveedor de un problema en su red, y se encuentren y resuelvan un problema de configuración de QoS en su lado. Al ver una captura del paquete que contiene el tráfico RTP, haga clic en Telefonía, RTP, Mostrar todos los flujos para ver esta pantalla.

Figura 29.3. Análisis Wireshark RTP



Src IP addr	Src port	Dest IP addr	Dest port	SSRC	Payload	Packets	Lost	Max De
10	13114	192	2244	0x63B69143	ITU-T G.711 PCMU	2103	0 (0.0%)	
192.1	2244	1	13114	0x6F1D173B	ITU-T G.711 PCMU	1646	477 (22.5%)	
10	11224	192	2268	0x2247C8D8	ITU-T G.711 PCMU	1321	0 (0.0%)	
192.1	2268	1	11224	0x6C5B26A1	ITU-T G.711 PCMU	879	460 (34.4%)	
10	17924	192	2242	0x393CBA89	ITU-T G.711 PCMU	480	0 (0.0%)	
192.1	2242	1	17924	0x6177246E	ITU-T G.711 PCMU	133	366 (73.3%)	

Captura en tiempo real a distancia

Desde un host UNIX que tiene Wireshark disponible, puede ejecutar una captura remota en tiempo real mediante la reorientación de
la salida de una sesión de SSH. Esto ha sido probado y se sabe que funciona en FreeBSD y Ubuntu.

Para utilizar esta técnica, SSH debe estar habilitado en el sistema pfSense y usted tendrá que utilizar un Llave SSH (ver la sección llamada "Secure Shell (SSH)"). La clave primero se debe cargar en ssh-agent o generados sin una frase de paso, porque la redirección no permitirá que ingrese una contraseña. Uso ssh-agent es muy recomendable, ya que cualquier llave sin una frase de paso es muy inseguro.

Antes de intentar esta técnica, asegúrese de que usted puede conectar a su router usando un pfSense SSH tecla sin necesidad de escribir la contraseña. La primera vez que se conecte, se le pide que guarde la clave de host, por lo que también se debe hacer antes de intentar iniciar Wireshark. Usted puede comenzar ssh-agent desde
una ventana de terminal o shell de este modo:

```
#eval `ssh-agent`
Agent pid 29047
#ssh-add
Escriba la frase de contraseña para / home / jim / .ssh / id_rsa:
Identidad añadió: / home / jim / .ssh / id_rsa (/ home / jim / .ssh /
id_rsa)
```

A continuación, inicie una sesión SSH, como de costumbre:

```
#root@192.168.1.1 ssh
La autenticidad de acogida '192 .168.1.1 (192.168.1.1) 'no se puede establecer.
DSA huella digital es 9e: c0: b0: 5a: b9: 9b: f4: ec: 7f: 1d: 8a: 2d: 4a: 49:01:1 b.
¿Está seguro de que desea continuar la conexión (sí / no)? sí
Advertencia: Permanentemente añadido '192 .168.1.1 '(DSA) de la lista de hosts
conocidos.

*** Bienvenidos a pfSense 1.2.3-pfSense en EXCO-rtr ***
[...]
```

Después de confirmar que la conexión SSH funciona, inicie la captura remota de la siguiente manera:

#Wireshark-k-i <(root@192.168.1.1 ssh tcpdump-i vr0 -U-w - puerto no tcp 22)

Cuando la parte de la dirección IP es la dirección de su sistema pfSense. El "no tcp puerto 22 " parte excluirá el tráfico de su sesión de SSH, que de otro modo va a obstruir la salida de la captura. La arriba está escrito en la sintaxis "al estilo de bash", pero puede funcionar con otros shells. Se puede ajustar el tcpdump argumentos para la interfaz y agregar expresiones adicionales, pero el `-U` y `-W -` son necesarias por lo que escribe la salida a la salida estándar, y escribe cada paquete que llega.

Ver también la captura Setup / Pipes [http://wiki.wireshark.org/CaptureSetup/Pipes] página en el Wireshark wiki para otras técnicas relacionadas.

Llanura Depuración Protocolo Texto flujo TCP

flujo TCP es otro paquete similar a tcpdump que le permitirá ver el contenido de texto de los paquetes en tiempo real en lugar de la cabecera del paquete y otra información de transporte. flujo TCP usa una sintaxis similar a tcpdump, con una notable excepción: Por defecto se escribe el texto del paquete a los archivos en lugar del consola. Para ver la salida de la consola, utilice la `-C` opción.

Mientras que no está disponible en una instalación de stock pfSense, flujo TCP se puede añadir desde la línea de comandos
instalar el paquete de FreeBSD. Se trata de un pequeño paquete sin dependencias, por lo que la instalación no debería dañar el sistema. Para instalar flujo TCP en pfSense, ejecute el siguiente comando desde un shell pfSense:

```
#pkg_add-r flujo TCP
#refrito
```

Si estás teniendo problemas con una conexión FTP de una LAN, se puede controlar el canal de control en el lado WAN, así:

```
#flujo TCP-i-c vlan0 anfitrión 172.17.11.9 y el puerto 21
flujo TCP [13899]: escucha en vlan0
172.017.011.009.00021-010.000.073.005.23747: 220 Bienvenido a ExampleCo web FTP sí
Fieldtech USUARIO: 010.000.073.005.23747-172.017.011.009.00021
172.017.011.009.00021-010.000.073.005.23747: 331 Por favor, especifique la contraseña.
Abc123 PASS: 010.000.073.005.23747-172.017.011.009.00021
172.017.011.009.00021-010.000.073.005.23747: 230 Inicio de sesión exitoso.
010.000.073.005.23747-172.017.011.009.00021: PORT 10,0,73,5,194,240
200 PORT command successful: 172.017.011.009.00021-010.000.073.005.23747. Consideracione
010.000.073.005.23747-172.017.011.009.00021: NLST
172.017.011.009.00021-010.000.073.005.23747: 150 Aquí viene el Listín directorio
172.017.011.009.00021-010.000.073.005.23747: 226 Directorio enviar 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 de salida en ambas direcciones, y lo más importante que usted puede ver que el proxy FTP hizo su trabajo y tradujo el comando PORT para utilizar la dirección IP de la WAN de pfSense en su lugar, permitiendo que el modo activo para que funcione correctamente. Si en cambio vio la dirección LAN IP que aparece en el
Comando PORT, sabría para comprobar la configuración del proxy FTP o cambiar al modo PASV sobre el cliente.

Tener flujo TCP todo ha sido muy útil en mi experiencia, y hace un buen complemento para tcpdump cuando usted quiere centrarse en el contenido de los paquetes en lugar de su estructura.

Referencias adicionales

Esta captura sólo la punta del iceberg de las posibilidades con las capturas de paquetes. Éstos son algunos recursos adicionales para los interesados en un mayor conocimiento en profundidad. Captura de paquetes es una medios muy poderosos de los problemas de conectividad de la red de resolución de problemas, y usted encontrará que su habilidades de solución de problemas mejoraron grandemente si usted aprende las posibilidades en mayor profundidad.

ComputerNetworking: Internet Protocolos en Acción [Http://www.amazon.com/gp/product/0471661864?

ie = UTF8 & tag = pfSense-20 y linkCode = as2 y campo = 1,789 y = 9,325 y creativa creativeASIN = 0471661864] por Jeanna Matthews

TcpdumpFilters[Http://www.whitehats.ca/main/members/Malik/malik_tcpdump_filters/malik_tcpdump_filters.html] Jamie French

Filtros Tcpdump avanzadas [Http://acs.lbl.gov/ ~ jason / tcpdump_advanced_filters.txt] por Sebastien Wains

Tcpdump Filtros [Http://www.cs.ucr.edu/ ~ marios / etéreo-tcpdump.pdf] por Marios Iliofotou

FreeBSDManPagefortcpdump[Http://www.freebsd.org/cgi/man.cgi?query = tcpdump y apropos = 0 & sektion = 0 & = ruta de manual de FreeBSD 7.2-RELEASE & format = html]

Apéndice A. Menu

Esta guía para las opciones de menú estándar disponibles en pfSense debería ayudar a identificar rápidamente el propósito de una determinada opción de menú, y se refieren a lugares en el libro donde se discuten las opciones con más detalle.

Los paquetes se pueden agregar elementos a cualquier menú, así que puede que tenga que comprobar todos ellos para buscar las opciones de menú
para los paquetes instalados. Normalmente, los paquetes se instalan en el menú Servicios, pero hay un montón de los que ocupan los otros menús también.

Sistema

El menú del sistema contiene opciones para el propio sistema, opciones generales y avanzados, firmware actualizaciones, paquetes de add-on, y las rutas estáticas.

Avanzado	Configuración avanzada del sistema para los cortafuegos, hardware, SSH, SSL Certificates, y muchos otros. Consulte la sección "Opciones de configuración avanzada".
Cert Gerente	Administre autoridades de certificación, los certificados y revocación de certificados Listas (x.509). Consulte el Capítulo 8, Gestión de certificados.
Firmware	Actualizar o cambiar la versión del firmware del sistema. (Por ejemplo, actualizar de pfSense 1.2.2 a 1.2.3). Consulte la sección "Actualización con la WebGUI".
Configuración general	La configuración del sistema en general, tales como el nombre de host, dominio, servidores DNS, etc Ver la sección titulada "Opciones generales de configuración".
Alta Disponibilidad. Sincroniza	Anteriormente conocido como "Ajustes CARP", esta sección controla cómo pfSense nodos de una alta disponibilidad (HA) de clúster sincronizan los estados y configuración. Consulte el Capítulo 24, Firewall de redundancia / alta disponibilidad.
Salir	Cierra la sesión de la interfaz gráfica de usuario, que regresan al usuario de vuelta a la pantalla de inicio de sesión. Ver Capítulo 7, Gestión de usuarios y autenticación.
Paquetes	Software adicional complementos para pfSense para ampliar su funcionalidad. Ver Capítulo 27, Paquetes.
Enrutamiento	Aquí es donde usted define gateways, rutas estáticas, y grupos de pasarela para multi-WAN. Consulte el Capítulo 12, Routing.
Asistente para la instalación	El asistente de configuración le guiará a través del proceso de realización de la base configuración inicial. Vea la sección llamada "Asistente de configuración".
Administrador de usuarios	Gestión de usuarios, grupos y servidores de autenticación (RADIUS o LDAP) para Acceso GUI, acceso VPN, y así sucesivamente. Consulte el Capítulo 7, Gestión y usuario Autenticación.

Interfaces

El menú Interfaces tiene artículos para la asignación de interfaces y un elemento para cada interfaz asignada. WAN y LAN aparecerá siempre, mientras que otros aparecen como OPTX o el nombre que se les ha dado.

(Asignar)	Asigne interfaces para funciones lógicas (por ejemplo, LAN, WAN, OPT), y crear / mantener VLANs y otros tipos de interfaces virtuales. Consulte la sección "Asignación de las interfaces", Capítulo 6, Tipos de interfaz y configuración, y el Capítulo 14, LAN virtuales (VLAN).
WAN	Configurar la interfaz WAN. Vea la sección llamada "Configuración Fundamentos Interfaz".
LAN	Configure la interfaz LAN. Vea la sección llamada "Configuración Fundamentos Interfaz".

OPTX	Configure las interfaces opcionales adicionales. Vea la sección llamada "Interface Conceptos básicos de configuración ".

Firewall

Los elementos del menú de Firewall son para configurar varias partes de las reglas del cortafuegos, las reglas de NAT, y su
la estructura de soporte.

Alias	Permite gestionar colecciones de direcciones IP, redes o puertos para simplificar creación y gestión de reglas. Vea la sección llamada "Alias".
NAT	Mantener reglas NAT que controlan hacia delante del puerto, NAT 01:01 y de salida NAT comportamiento. Consulte el Capítulo 11, La traducción de direcciones de red.
Reglas	Configurar reglas de firewall. Debe haber una ficha en esta pantalla para cada interfaz configurada. Vea la sección llamada "Introducción a las reglas de firewall pantalla ".
Horarios	Planificaciones de normas basadas en el tiempo de configuración. Vea la sección llamada "Reglas basadas en el tiempo".
Traffic Shaper	Configure (QoS) de la modulación del tráfico / Calidad de Servicio. Consulte el Capítulo 20, Traffic Shaper.
IPs virtuales	Configurar las direcciones IP virtuales para permitir pfSense manejar el tráfico de más de un Dirección IP por interfaz, por lo general para las reglas de NAT o failover CARP. Consulte la sección llamada "IP virtual".

Servicios

El menú Servicios contiene elementos que permiten controlar diferentes servicios prestados por los demonios que se ejecuta en pfSense. Consulte el Capítulo 25, Servicios.

Portal Cautivo	Controla el servicio de portal cautivo que le permite dirigir a los usuarios una página web en primer lugar para la autenticación antes de permitir el acceso a Internet. Ver Capítulo 23, Portal Cautivo.
Relé DHCP	Configura el servicio de retransmisión de DHCP que examinará las solicitudes DHCP de proxy de un segmento de red a otro. Vea la sección llamada "DHCP Relay".
Servidor DHCP	Configura el servicio DHCP que proporciona la dirección IP automática configuración para los clientes en las interfaces internas. Vea la sección llamada "DHCP Server".
DHCPv6 Relay	Configura el servicio de retransmisión de DHCP para IPv6 que hará el servicio proxy DHCP pide de un segmento de red a otro.
DHCPv6 servidor / RA	Configura el servicio de DHCP para IPv6 y anuncios de enrutador que proporcionar configuración automática de direcciones IPv6 a los clientes sobre Interna interfaces.
Reenviador DNS	Configura integrado de resolución de DNS de almacenamiento en caché de pfSense. Vea la sección llamada "Forwarder DNS".
DNS dinámico	Configura los servicios de DNS dinámico (DynDNS) que actualizar un control remoto sistema cuando la dirección IP de WAN del router pfSense ha cambiado. Consulte la sección llamada "Dynamic DNS".
Equilibrador de carga	Configura el equilibrador de carga, que equilibra las conexiones entrantes a través de múltiples servidores. Consulte el Capítulo 21, Equilibrio de carga del servidor.

NTP	Configure el daemon servidor de protocolo de tiempo de red. Vea la sección llamada "NTPD".
PPPoE servidor	Configurar el servidor PPPoE que permiten pfSense para aceptar y autenticar conexiones de clientes PPPoE. Vea la sección llamada "PPPoE Server".
RIP	Configura el daemon de enrutamiento RIP. Vea la sección llamada "RIP".
SNMP	Configura el protocolo simple de administración de redes (SNMP) demonio para permitir colección basada en la red de las estadísticas de este router. Consulte la sección llamado "SNMP".
UPnP y NAT-PMP	Configurar el Plug and Play universal (UPnP), que puede configurar automáticamente NAT y reglas de firewall para los dispositivos que soportan el estándar UPnP. Vea la sección "UPnP".
Wake on LAN	Configure Wake on LAN servicios que le permiten despertar remotamente PCs accesibles desde el sistema pfSense cliente. Vea la sección llamada "Wake on LAN ".

VPN

El menú VPN contiene elementos que pertenecen a redes privadas virtuales (VPN), incluyendo IPsec, OpenVPN y PPTP. Consulte el Capítulo 16, Redes Privadas Virtuales.

IPsec	Configurar túneles VPN IPsec, las opciones y los usuarios móviles de IPsec y certificados. Ver Capítulo 17, IPsec.
L2TP	Configurar los servicios de L2TP y usuarios. Consulte el Capítulo 18, PPTP VPN.
OpenVPN	Configurar los servidores y clientes OpenVPN, así como la configuración específica del cliente. Ver Capítulo 19, OpenVPN.
PPTP	Configurar los servicios de PPTP y usuarios, o de relé. Consulte el Capítulo 18, PPTP VPN.

Estado

El menú Estado le permite comprobar el estado de los diferentes componentes y servicios del sistema, así como ver los registros.

Portal Cautivo	Cuando Captive Portal está habilitada, puede ver el estado de usuario aquí. Ver Capítulo 23, Portal Cautivo.
CARP (failover)	Vea el estado de las direcciones IP de la carpa en este sistema. Mostrará MAESTRO / Estado BACKUP. Vea la sección llamada "Verificar estado CARP".
Salpicadero	Un atajo para volver a la página principal del enrutador pfSense que muestra en general información del sistema. Vea la sección llamada "Dashboard".
Concesiones DHCP	Ver una lista de todos los arrendamientos DHCP IPv4 asignadas por este router. También puede eliminar offline arrendamientos, enviar Wake on LAN peticiones a los sistemas fuera de línea, o crear arriendos estáticos de las entradas actuales. Vea la sección llamada "Arrendamientos".
Arrendamientos DHCPv6	Ver una lista de todos los arrendamientos DHCP IPv6 asignadas por este router. También puede eliminar offline arrendamientos, enviar Wake on LAN peticiones a los sistemas fuera de línea, o crear arriendos estáticos de las entradas actuales. Vea la sección llamada "Arrendamientos".
Filtrar Actualizar	Muestra el estado de todas las solicitudes de recarga de filtro que son (o eran) a la espera. La filtro se vuelve a cargar cada vez que se aplican los cambios. Si no hay cambios han sido hecho, esta pantalla simplemente debe informar que una actualización se ha completado.

Gateways	Muestra el estado de las puertas de enlace y grupos de pasarela de las multi-WAN. Ver Capítulo 12, Routing.
Interfaces	Le permite ver el estado del hardware de las interfaces de red, lo que equivale a la utilización de ifconfig en la consola. Vea la sección llamada "estado de la interfaz".
IPsec	Visto el estado de los túneles IPsec configurados. Consulte el Capítulo 17, IPsec.
Equilibrador de carga	Visto el estado de las piscinas de Load Balancer. Para el equilibrio de carga de puerta de enlace, consulte la sección llamada "Prueba de conmutación por error". Para el equilibrio de carga del servidor ver el sección llamada "estado de equilibrio de carga de visión".
NTP	Considera el estado del daemon servidor de protocolo de tiempo de red. Consulte la sección llamada "NTPD".
OpenVPN	Visto el estado de las instancias de OpenVPN configurados. Consulte la sección llamado "Comprobación del estado de clientes y servidores OpenVPN".
Registros del paquete	Ver los registros de determinados paquetes soportados.
Colas	Vea el estado de las colas para la conformación de tráfico. Vea la sección llamada "Supervisión de las colas".
Gráficos RRD	Ver grafica los datos para las estadísticas del sistema, tales como ancho de banda utilizado, uso de CPU, estados de cortafuegos, etc. Vea la sección llamada "los gráficos RRD".
Servicios	Supervisar el estado del sistema y de los paquetes de servicios / demonios. Consulte la sección llamado "Estado del servicio".
Los registros del Sistema	Ver los registros de los servicios del sistema y del sistema, como el firewall, DHCP, VPNs, etc están en la sección "Registros del sistema".
Gráfico de Tráfico	Vea un gráfico del tráfico en tiempo real basados en SVG dinámica de una interfaz. Consulte la sección llamada "Traffic Gráficos".
UPnP y NAT-PMP	Ver una lista de todos los delanteros del puerto UPnP activos actualmente. Vea la sección llamada "UPnP".
Sin hilos	Ver una lista de las redes inalámbricas disponibles actualmente en el rango. Consulte la sección llamada "Mostrando las redes inalámbricas disponibles y fuerza de la señal".

Diagnóstico

Elementos del menú Diagnósticos realizar diversas tareas de diagnóstico y administrativos.

Tablas ARP	Ver una lista de los sistemas como se ha visto a nivel local por el router. La lista incluye una Dirección IP, dirección MAC, nombre de host, y la interfaz donde el sistema fue visto.
Autenticación	Pruebas de autenticación a un radio definido o un servidor LDAP. Consulte la sección llamada "Solución de problemas".
Backup / Restore	Copia de seguridad y restauración de archivos de configuración. Vea la sección llamada "Hacer Las copias de seguridad en el WebGUI ", la sección llamada" Restauración con la WebGUI ", y la sección denominada "Restauración de la historia Config".
Símbolo del sistema	Ejecutar comandos de shell o código PHP, y subir / descargar archivos a la sistema pfSense. Utilizar con precaución.
Búsqueda de DNS	Ejecuta una búsqueda DNS para resolver nombres de hosts con fines de diagnóstico y para probar la conectividad de los servidores DNS.

Editar archivo	Edición de un archivo en el sistema pfSense.
Valores predeterminados de fábrica	Restablece la configuración a los valores predeterminados. Tenga en cuenta, sin embargo, que esta no altera el sistema de archivos o desinstalar los archivos del paquete; que sólo los cambios ajustes de configuración.
Sistema Halt	Apague el router y apagar la unidad cuando sea posible.
Limitador Info	Muestra el estado de los limitadores y el tráfico que fluye en su interior. Ver Capítulo 20, Traffic Shaper.
NDP Tabla	Ver una lista de los sistemas locales de IPv6 como se ha visto por el router. La lista incluye una dirección IPv6, la dirección MAC, nombre de máquina (si es conocido por el cortafuegos), y la interfaz.
NanoBSD	Sólo es visible en el (integrado) Plataforma NanoBSD. Permite la clonación de la rebanada de trabajo sobre la rebanada alternativa y elegir cuál de ellos debe haber utilizado para arrancar el router.
Captura de paquetes	Realizar una captura de paquetes de inspeccionar el tráfico, y luego ver o descargar la resultados. Vea la sección llamada "Captura de paquetes de la WebGUI".
PFINFO	Muestra las estadísticas sobre el filtro de paquetes, incluyendo las tasas de tráfico general, las tasas de conexión, información de tabla de estado, y varios otros contadores.
pfTop	Muestra una lista de los mejores conexiones activas de una métrica de selección tal como bytes, tasa, la edad, y así sucesivamente.
Ping	Enviar tres peticiones de eco ICMP a una dirección IP determinada, enviado a través de un elegido interfaz. No es compatible con multi-wan.
Reinicie el sistema	Reinicie el router pfSense. Dependiendo del hardware, esto podría tomar varios minutos.
Rutas	Muestra el contenido de la tabla de enrutamiento del sistema. Vea la sección llamada "Visualización de rutas".
Estado de SMART	Muestra información de diagnóstico acerca de las unidades IDE, si es compatible con el de hardware. También puede ejecutar pruebas de disco duro.
Enchufes	Muestra una lista de los procesos en el servidor de seguridad que están vinculados a los puertos de la red, escuchando las conexiones o hacer conexiones salientes desde el servidor de seguridad en sí.
Unidos	Ver los estados de firewall activas actualmente. Vea la sección llamada "Visualización en el WebGUI ".
Unidos Resumen	Muestra información acerca de la tabla de estado, para ver la actividad resumida por Dirección IP.
Actividad del sistema	Muestra el uso de memoria y una lista de los procesos activos y los hilos del sistema de el servidor de seguridad, la salida es desde top-SH.
Tablas	Le permite ver y editar el contenido de varias tablas del sistema y alias.
Traceroute	Trace la ruta tomada por los paquetes entre el router pfSense y un control remoto sistema. Vea la sección "Uso de traceroute".

Índice

Símbolos

NAT 01:01, 141, 141
  (Véase también el NAT, 01:01)

La

ACPI, 68
Opciones avanzadas, 52
Alias, 118
  Configuración, 118
  Los anfitriones, 118
  Equilibrio de carga y, 338
  Redes, 118
  Puertos, 118
  Utilizando, 118
ALTQ (ver Traffic Shaping)
Appliance, 3
  DHCP Server, 4
  DNS, 3
  Sniffer, 3
  VPN, 3
AutoConfigBackup paquete, 105
Automática NAT Saliente
  Ver NAT, salida automática, 136

B

Las copias de seguridad, 104
  AutoConfigBackup paquete, 105
  Historia de configuración, 109
  Manualmente en WebGUI, 104
  Restauración a partir de, 108
Mejores Prácticas
  Las copias de seguridad, 104
  Reglas de firewall, 120
  Logs, 122
  Multi WAN-Paths Circuit, 189
  Documentación Red, 121
  Segmentos de red, 6
  Acceso SSH, 54
  Actualizaciones del sistema, 39
  WebGUI Access, 52
BGP, 162
Bittorrent, 326, 382
Bloque Bogon Redes, 46, 123
  Actualización de la lista Bogon, 124
Bloque de redes privadas, 46, 123
bnsmpd, 381
Menú de inicio, 68
Border Gateway Protocol, 162
Border Router, 2
Tender un puente, 167
  Bucles de Capa 2, 167
  Wireless y, 344
Broadcast Domain, 167
  CARP y, 372
  Combinando, 167
  definido, 13
  DHCP y, 378
  Los troncos y, 121
  Múltiples interfaces, 128
  VLAN y, 173
  Wireless y, 344, 346

C

Portal Cautivo, 354
  Tender un puente y, 168
  Páginas personalizados, 356
  Limitaciones, 354
  RADIUS y, 354
  Normas basadas en el tiempo y, 130
  Solución de problemas, 357
  VLAN y, 174
  Wireless y, 350
CARPA, 129, 358
  Tender un puente y, 168, 370
  Ejemplo de configuración, 360
  IPsec y, 210
  Layer 2 Redundancia, 369
  Multi-WAN y, 192
  OpenVPN y, 315
  Capturas de paquetes, 417
  Configuración, 364
  Pruebas, 367
  Solución de problemas, 371
  Sin NAT, 368
CIDR
  Notación, 10
  Recapitulación, 12
estorbo, 388
Co-Location, 121
Los despliegues comunes, 2
Compact Flash, 5, 5, 27
  Requisitos de tamaño, 16
config.xml (ver archivo de configuración)
Configuración
  Opciones avanzadas, 52
  Opciones generales, 51
Archivo de configuración, 38, 72, 104
  Edición manual, 72
  Ubicación, 72
  Mudarse a USB / Floppy, 67
Límites de conexión, 126
Menú Console, 63
  Proteger con contraseña, 55
Filtrado de Contenido, 404, 404
  (Véase también el DNS, OpenDNS)
Crash Dumps, 26
La aceleración criptográfica, 60, 60
  (Véase también el hardware, aceleración criptográfica)

D

Denegar por defecto, 124

Puerta de enlace predeterminada, 10, 10
(Véase también la puerta de enlace)
Contraseña por defecto, 42
Denegación de servicio, 113, 127
Desarrollador Shell, 65
DHCP Relay, 378
DHCP Server, 42, 349, 374
Intervalo de direcciones, 374
Tender un puente y, 167
CARP y, 364, 365, 367
Eliminar Lease, 377
Denegar clientes desconocidos, 374
Servidores DNS, 375
DNS dinámico, 375
Failover, 375
Gateway, 375
Selección de la interfaz, 374
Lease Times, 375
Arrendamientos (Visionado), 377
Logs, 377
De inicio de redes, 376
Servidores NTP, 376
Asignaciones estáticas, 376, 377
Estado, 377
Servidores WINS, 375
DMZ, 144
definido, 7
DNS, 43, 51, 71
Permitir alteración dinámico, 51
Forwarder DNS, 378
Multi-WAN y, 192
DNS dinámico, 380
Multi-WAN y, 193
OpenDNS, 404
Split DNS, 146, 379
DNS Revinculación, 53
Descarga de pfSense, 21

E

Edge Router, 2
Filtrado de salida, 113
Wireless y, 352
Embedded, 5, 60
Descargar, 21
Requisitos de hardware, 16
Instalación, 27
Instalación con VMware, 34
NanoBSD, 6
Paquetes y, 399
Restauración de copias de seguridad para CF, 110
Puertos serie (ver Puertos serie)
Apagado, 64
Sincronización de la hora y, 67
Actualización, 39

F

Valores predeterminados de fábrica, 64
Filtrar Unidos, 112, 112
(Véase también Unidos)
Firewall, 112
Tráfico bloqueado Reglas Pass, 134
Reglas Configuración, 125
Denegar por defecto, 124
Desactivar, 56
Desactivar Scrub, 56
El límite de conexiones, 126
Múltiples subredes, 129
Opciones de optimización, de 56
Regla del archivo (temporal), 74
Opciones de Regla, 125
Acción, 125
Regla Programación, 127, 130
Solución de problemas, 134
Protección contra virus, 126
Estados de Firewall, 112, 112
(Véase también Unidos)
Fragmentar
Clear Bit DF, 55
Instalación completa, 22

T

Juegos
NAT y, 151
Traffic Shaping y, 323, 327
UPnP y, 382
Gateway, 10, 193
Tender un puente y, 168, 172
Clientes y, 71
Por defecto, 10
definido, 163
DHCP y, 375
DHCP con CARP y, 364
Reglas de firewall, 127
CARP y, 367
IPsec y, 124
Grupos, 190
Redirecciones de ICMP, 158
IPsec y, 222, 253
Tipo de equilibrio de carga (ver el equilibrio de carga)
Monitorización de la Calidad, 396
OPT WAN y, 7
Política de enrutamiento y, 190
Port Delanteros, 152
PPPoE, 387
PPTP, 267
Rutas PPTP, 276
Igual en múltiples redes WAN, 191
Rutas estáticas, 157
WAN, 49
Opciones generales, 51
Gráficos, 395, 398

H

Sistema Halt, 429

Desde Console, 64
Hardware, 15
Compatibilidad, 15
La aceleración criptográfica, 60, 60, 213, 213, 281
(Véase también el VPN)
Sondeo de dispositivos, 58
Tarjetas de red, 15
ALTQ Capaz, 323, 323
(Véase también el Traffic Shaping)
VLAN Capaz, 173, 173, 173, 173
(Véase también la VLAN)
Inalámbrica, 342
Requisitos, 16
La selección, 16
Acerca de, 17
Solución de problemas, 36
Sin hilos
Punto de Acceso Capaz, 346
Ayuda, 7
Alta disponibilidad, 358, 358
(Véase también el CARP)
Cheques HTTP Referer, 53

Yo

NIC, 402
Ingress Filtering, 46, 113
Instalación, 21
Técnicas Alternativas, 32
Fácil instalación, 25
Instalación de recuperación, 38
Instale Rescue, 110
Para la impulsión dura, 25
Solución de problemas, 34
Actualización, 39
Interfaz
Configuración, 49, 84
Asignación Interface, 24, 49
Estado de la interfaz, 394
IPsec, 61, 124, 136, 203, 209
CARP y, 210
Software de Cliente, 205
Comparación, 207
Dead Peer Detection, 215
DH, 214
DPD, 215
Opciones de cifrado, 213
Amabilidad Firewall, 206
Reglas de firewall, 216
Algoritmos Hash, 214
Selección de la interfaz, 210
Vidas, 214
Clientes móviles, 232
Shrew Soft, 246
Túneles móviles, 225
Multi-WAN y, 192, 210
Múltiples subredes, 223
Capturas de paquetes, 419
Túneles paralelos, 223
PFS, 216
Fase 1, 209
Fase 2, 209
SAD, 209
Asociación de Seguridad, 209
Política de Seguridad, 209
Un sitio a otro, 217
SPD, 209
Terminología, 209
Prueba de conectividad, 251
Dispositivos de terceros, 259
Cisco IOS, 260
Cisco PIX 6.x, 259
Cisco PIX 7.x/8.x, 260
El tráfico de pfSense, 224
Solución de problemas, 251, 419
Wireless y, 211, 350
IPv6
Multi-WAN y, 192, 200
Opciones IPv6, 58

K

Kernel, 26
Kernel timeCounter, 69
Claves
IPsec, 218
SSH, 54
WPA, 348
Kiwi Syslog Server, 409

L

LAN
Configuración, 47, 49, 84
definido, 6
Configure IP desde la Consola, 64
LAN del router, 2
Equilibrio de carga, 335
Gateway, 190, 194
Server, 335
Estado, 339
Conexiones Sticky, 60, 336
Solución de problemas, 340
Verificación, 340
Logs, 388
DHCP, 377
Firewall, 65, 72, 121, 132, 134
IPsec, 222, 254, 257
OpenVPN, 317, 319
PPTP, 277
LZO compresión, 282

M

MLPPP, 201
Monitoreo, 388, 388
(Véase también el Seguimiento del Sistema)
Multi-Link PPP, 201
Multi-WAN, 189

Ancho de banda de agregación, 198
Tender un puente y, 172
CARP y, 365
IPsec y, 192 de 210
Servicios locales y, 192
IPs de Monitor, 191
NAT y, 194
En un palo, 199
OpenVPN y, 312
Segregación Servicio, 198
Casos especiales, 193
Normas basadas en el tiempo y, 130
Traffic Shaping y, 323
Solución de problemas, 202
Costo desigual / Ancho de banda, 199
Verificación, 196
VPN Compatibilidad, 207
Múltiples subredes, 129

N

NAT, 136
01:01, 141
Configuración, 142
Reglas de firewall, 146
FTP y, 150
Multi-WAN y, 194
Reflexión NAT y, 146
Riesgos, 142
WAN IP y, 144
Salida automática, 136
Elegir una configuración, 148
FTP y, 148
Modo Activo, 149
Limitaciones, 148
Modo pasivo, 149
GRE y, 150
Inbound (ver Port Forwards)
Outbound, 72, 147
Por defecto, 136
Desactivación, 148
Puerto estático, 147
Port Delanteros, 136
Configuración, 137
FTP y, 149
Servicios locales y, 137
Riesgos, 136
Redireccionamiento de tráfico, 141
PPTP y, 150
Procesamiento de pedidos, 144
Compatibilidad Protocolo, 148
Reflexión, 57, 146
TFTP y, 150
Solución de problemas, 151, 418
Reflexión NAT, 146, 146
(Véase también el NAT, Reflejo)
netgraph, 382
Segmentación de la red, 6
Conceptos de redes, 9
Cliente NTP, 43
NTP Server, 385

O

One-to-One NAT, 141, 141
(Véase también el NAT, 01:01)
Open Shortest Path First, 162
OpenNTPD, 385
OpenVPN, 165, 203, 278
Grupo de direcciones, 283
En puente, 315
CARP y, 315
Cipher, 281
Instalación del cliente, 292
Certificados, 296
Archivo de configuración, 296
Software de Cliente, 206
FreeBSD, 295
Linux, 295
Mac OS X, 295
De Windows, 294
Comparación, 207
Compresión, 282
Configuración, 279
Criptográficos Aceleradores, 290
Opciones personalizadas, 284, 317
Puerta de enlace predeterminada, 317
IP dinámica, 283
Filtrado de Tráfico, 309
Amabilidad Firewall, 206
Reglas de firewall, 280, 308
Inter-Cliente Comunicación, 282
Red Local, 282
Puerto local, 280
LZO compresión, 282
Multi-WAN y, 192, 312, 313
NAT de salida, 309
Remote Network, 282
Opciones de ruta, 317
Sitio con el ejemplo del sitio (Shared Key), 303
Sitio con el ejemplo del sitio (SSL / TLS), 305
Especificación de la dirección IP, 317
IPs estáticas, 283
TCP vs UDP, 280
Solución de problemas, 318
Túnel de red, 281
Inalámbrica, 350
OPT, 7, 7
(Véase también opcionales Interfaces)
Interfaces opcionales, 7, 49, 84
como WAN adicional, 7, 7
(Véase también el multi-WAN)
Asignación, 24, 49
Reglas del cortafuegos en la, 116
Por inalámbrica, 346, 352
Traffic Shaping y, 323
Detección OS, 125
OSPF, 162

P

p0f, 125
P2P (ver redes Peer-to-Peer)
Paquetes, 399
  AutoConfigBackup, 105
  Copia de seguridad de los archivos (del paquete), 111
  BGP, 162
  Desarrollar, 401
  de FreeBSD, 409
  Acerca del hardware, 20
  Instalación, 400
  OSPF, 162
  Reinstalación, 400
  flujo TCP, 423
  Desinstalación, 401
  Actualización, 400
  Viendo disponible, 399
Capturas de paquetes, 412
  Desde Shell, 413
  Desde WebGUI, 413
  Selección de la interfaz, 412
  Captura en tiempo real a distancia, 422
  tcpdump, 413
  flujo TCP, 423
  Solución de problemas con, 418
  Vista en el WebGUI, 413
Detección pasiva OS, 125
Contraseña, 42
pcap, 414
Redes Peer-to-Peer, 114, 326
  Traffic Shaping y, 323
Perímetro Firewall, 2
PFI, 38
Versiones pfSense, 4
pfsync, 359
pftop, 65, 397
PHP Shell Access, 65
physdiskwrite, 27
Ping, 64
PKI, 96 (véase la Infraestructura de Clave Pública)
  (Ver la infraestructura de clave pública también)
Plataformas, 5
Port Delanteros, 136, 136
  (Véase también NAT, Forwards Portuarias)
PPPoE, 43, 44, 45, 71
  Multi-WAN y, 192
  Server, 387
PPTP, 124, 203, 262
  Adición de usuarios, 264
  Configuración del cliente, 266
    Mac OS X, 272
    Usar puerta de enlace predeterminada, 267
    Windows 7, 272
    Windows Vista, 268
    Windows XP, 266
  Software de Cliente, 206
  Comparación, 207
  Configuración, 263
  Amabilidad Firewall, 206
  Reglas de cortafuegos y, 262, 264
  Limitaciones, 262
  Multi-WAN y, 192, 262
  RADIUS y, 263
  Redirigir, 275
  Trucos de enrutamiento, 276
  Solución de problemas, 275
  Inalámbrica, 351
PPTP (WAN Type), 44, 46, 71
  Multi-WAN y, 192
Direcciones IP privadas, 9
VLAN privada, 174
Las direcciones IP públicas, 10
Infraestructura de Clave Pública, 96
PVLAN, 174

Q

QinQ, 174
QoS (ver Traffic Shaping)
Calidad de servicio (ver Traffic Shaping)
Colas, 322

R

RADIUS, 263, 354, 387
  Windows Server, 402
Detección Temprana Aleatoria, 330
Reboot, 429
  Desde Console, 64
Redundancia, 358, 358
  (Véase también el CARP)
RFC 1918 subredes, 9, 9
  (Ver direcciones IP también privados)
RIP, 162
Enrutamiento, 154
  Asimétrica, 157
  Redirecciones de ICMP, 158
  Múltiples subredes, 129
  Protocolos, 162
  IPs públicas, 158
  Rutas estáticas, 10
    Filtrado, 57
  Solución de problemas, 163
  Flora, 163
RRD gráficos, 395

S

SCP, 54, 54
  (Ver también SSH)
  Las copias de seguridad y, 107
Secure Copy (ver SCP)
Secure Shell (SSH ver)
Serial Console
  Habilitación, 55
Clientes consola serie, 31
Puertos serie, 31

Estado del servicio, 394
Servicios, 374
Asistente para la instalación, 42
Shell Access, 65
Shrew Soft IPsec, 246, 246
(Véase también IPsec, clientes móviles)
Apagado (véase Sistema Halt)
Simple Service Discovery Protocol, 382
Punto único de fallo, 370
SNMP, 381
Protocolo Spanning Tree, 169
Split DNS, 146, 146
(Véase también DNS)
Tráfico Parodiado
Prevención, 123
SSDP (ver Simple Service Discovery Protocol)
SSH, 54, 67, 422
Las copias de seguridad y, 108
Cambio Puerto, 54
ssh-agent, 422
Tunneling, 75
Unidos, 112, 397
Ajuste máximo, 56
Opciones de seguimiento, 126
Flora, 397
ARP estática, 375
Puerto estático, 147, 147
(Véase también el NAT, salida, puerto estático)
Rutas estáticas, 10, 10
(Véase también el enrutamiento, las rutas estáticas)
Conexiones Sticky, 336, 336
(Véase también el equilibrio de carga, conexiones Sticky)
STP, 169
Calculadora de subred, 12
Máscara de subred, 10, 10
(Véase también la notación CIDR)
Supernetting, 12, 12
(Véase también el CIDR Summarization)
Opciones de Soporte, 8
SYN Floods, 127
syslog, 389, 409
Supervisión del sistema, 388

T

Banderas TCP, 132, 332
tcpdump, 412, 412
(Véase también el Paquete de Captura)
Filtros, 416
flujo TCP, 423
Vuelca texto, 26
TFTP, 150
Server, 399
Tema, 51
De software de terceros, 402
Sincronización de la hora, 67
Zonas horarias, 43, 67
TinyDNS, 3, 3
(Véase también DNS)
Ruta de seguimiento, 165
Gráficos Tráfico, 395 de 395, 398
(Véase también los gráficos RRD)
Asignación de tráfico, 322
ACK, 330
Concepto Explicación, 322
Asistente de configuración, 324
ECN, 330
Notificación explícita de congestión, 330
Juegos, 323, 327
Hardware, 323
HFSC (ver jerárquica Feria de Servicio Curve)
Jerárquica Curve Feria servicio, 330
Limitaciones, 323
Velocidad de enlace, 324
Low Delay, 330
Otras aplicaciones, 327
Redes Peer-to-Peer, 323, 326
Penalty Box, 326
Prioridades, 330
Procesamiento de pedidos, 322
Propósitos, 322
Colas
Edición, 329
Monitoreo, 328
Detección Temprana Aleatoria, 330
ROJO, 330
Reglas, 331
Curva de servicio, 330
Solución de problemas, 333
Congestión Upstream, 322
VoIP, 325
Llamadas VoIP, 323
Solución de problemas
Portal Cautivo, 357
CARPA, 371
Firewall, 134
Hardware, 36
Instalación, 34
El acceso a Internet, 70
IPsec, 251, 419
Equilibrio de carga, 340
Multi-WAN, 202
NAT, 151, 418
OpenVPN, 318
PPTP, 275
Enrutamiento, 163
Asignación de tráfico, 333
UPnP, 385
WebGUI, 70
Inalámbrica, 353
Trunking, 173

U

Modernización
Desde Console, 66
Actualización del firmware, 39, 39
(Ver también Instalación, actualización)

UPnP, 382
Configuración, 383
Las preocupaciones de seguridad, 383
Estado, 384
Traffic Shaping y, 333
Solución de problemas, 385

V

VIPs (ver IPs virtuales)
IPs virtuales, 129, 153
CARP y, 361
LAN virtuales (VLAN ver)
Virtualización, 33
CARP y, 372
Timer Kernel, 69
virusprot, 126
VLAN, 173
Puerto de acceso, 174
Configuración de la consola, 176
Configuración de WebGUI, 178
Hardware, 173
Interfaz de Padres, 174
Privado, 174
QinQ, 174
Requisitos, 173
Seguridad, 174
Configuración de conmutación, 179
Cisco CatOS, 181
Cisco IOS, 180
Dell PowerConnect, 188
HP ProCurve, 181
Netgear, 183
Trunking, 173
VLANs
Por defecto VLAN Uso, 175
Cuestiones Switch, 175
ID de VLAN, 174
VLAN1 Uso, 175
Voz sobre IP (VoIP ver)
VoIP, 399
SIP, 147
SIP Proxy, 399
TFTP y, 150
Traffic Shaping y, 323
VPN, 203
Autenticación, 205
Reglas automáticas, 57
Escoger, 204
Software de Cliente, 205
Comparación, 207
Criptográficamente seguro, 207
Amabilidad Firewall, 206
Limitaciones, 203
Acceso remoto, 204
Enrutamiento, 165
Secure Relay, 204
Sitio a sitio, 203
SSL, 278
Wireless y, 204

W

Wake on LAN, 377, 386
WAN
Configuración, 44, 49, 84
definido, 7
MAC Address, 44
MTU, 45
PPPoE, 45
PPTP ISP, 46
IP estática, 45
Tipos, 44
WAN Router, 3
webConfigurator (ver WebGUI)
WebGUI, 1, 42
Anti-Bloqueo de Regla, 53, 122
Cambio Puerto, 52
Conexión a, 42
Cheques Revinculación DNS, 53
Cheques HTTP Referer, 53
HTTP / HTTPS, 52
Locked Out, 73
Ataque Man-In-The-Medio / Advertencia, 54
Restablecer contraseña, 64
Al reiniciar, el 65
Restricción de acceso, 122
Solución de problemas, 70
WEP, 348
Inalámbrica, 342
Punto de acceso, 346
Canal, 348
Estado del cliente, 349
DHCP y, 349
Cifrado, 348
Reglas de firewall, 349
SSID, 347
Estándar inalámbrico, 347
Como WAN, 343
Tender un puente, 344
Elegir Bridged o enrutamiento, 346
Los conductores, 342
Puntos de acceso externo, 345
IPsec y, 211, 350
Proteger con VPN, 349
Hotspot Secure, 351
Estado, 343
Solución de problemas, 353
Gire Routers en los puntos de acceso, 345
Visualización de las redes disponibles, 344
Wireshark
Capturas de paquetes, 421
WoL (consulte Wake on LAN)
WPA, 348

X

X.509, 96, 96

(Ver la infraestructura de clave pública también)
Configuración del archivo XML (véase el archivo de configuración)
Sync XML-RPC, 359