Universidad del Azuay

Facultad de Ciencias de la Administración

Escuela de Ingeniería de Sistemas

"Gestión de firewall bajo Linux mediante Shorewall"

Trabajo de graduación previo a la obtención del título de Ingeniería en Sistemas

Autores: Arteaga Peña Isaac Patricio
Lituma Velín Gonzalo Iván

Director: Ing. Fabián Carvajal

Cuenca, Ecuador

2006

AGRADECIMIENTOS

A todas las personas que de una u otra forma ayudaron al desarrollo de este trabajo, de manera especial al Ing. Fabián Carvajal por el interés brindado y su acertada dirección

DEDICATORIA

A mis padres, ya que gracias a su amor y esfuerzo supieron guiarme de la mejor manera.
Al amor de mi vida, que siempre fue de gran apoyo en los momentos mas duros.
Sobre todas las cosas a mi Dios Padre Jehová que me dio la vida y esperanza para realizar todas las cosas sobre este mundo.

Isaac

DEDICATORIA

A todas las personas con sed de conocimiento, que luchan desde sus oficios para crecer como sociedad, en especial a mi hermosa madre por su inagotable apoyo, y a todas las personas que confían en mis capacidades.

Iván

Los criterios e ideas expuestas en la presente monografía, que aparecen como propios de sus autores, son de su responsabilidad

Octubre, 2006

Isaac Arteaga P.

Iván Lituma V.

Resumen

Esta monografía enfoca el manejo de un firewall sobre el sistema operativo Linux mediante un software llamado *Shorewall*. En la misma se brinda al lector configuraciones sencillas y prácticas para la puesta en marcha del firewall en cualquier red de presupuesto moderado. El documento consta de conceptos, tipos y estructuras más conocidas de un firewall, contiene ejemplos prácticos de la configuración de un firewall mediante *Shorewall*.

ABSTRACT

This research paper focuses on the handling of a firewall on Linux operative system through a software called *Shorewall*. It offers the reader simple and practical configurations to start the firewall in any moderate budget net. The document contains concepts, the most known firewall types and structures, and practical examples of the configuration of a firewall through *Shorewall*.

INDICE

INTRODUCCIÓN

El presente documento esta dirigido a personas con conocimientos medios del sistema operativo Linux y de redes de computadoras.

Nuestra Intención es brindar al lector una guía detallada y sencilla para facilitar la implementación y manejo de un firewall mediante "*Shorewall*". Se expondrán también ejemplos prácticos de configuraciones para una mejor comprensión.

Debido a la gran difusión del Internet sobre todo en el ámbito Empresarial, nace la necesidad de proteger la información digital, ya sea por el gran crecimiento de software maligno como virus o programas espías, o así también por el mal uso que se le puede dar al Internet en las empresas; por esta razón han surgido los firewalls (software y/o hardware dedicados al control del flujo de información), en el capítulo 1 se darán a conocer sus diferentes estructuras así como los diferentes tipos de firewalls que existen en la actualidad.

El manejo de los firewalls en las redes de computadoras es conocido por su difícil configuración, por esta razón se han creado varias herramientas para facilitar el manejo de los mismos. En nuestro caso usaremos un software llamado "*Shorewall*" el mismo que será tratado de una manera extensa en el capítulo 2. En este se brinda una explicación detallada de la instalación del software y sus distintas configuraciones, para de esta manera dar paso al último capítulo de este documento, en el que mediante ejemplos prácticos se pretende guiar al lector a poder realizar y entender las configuraciones más comunes de un firewall mediante Shorewall.

CAPÍTULO I

Firewall

1 Firewall

1.1 Introducción a firewalls

Por la necesidad de proteger la información se crearon los firewalls, los mismos que permiten controlar el flujo de la información en una red de computadoras, generalmente con acceso a Internet. Hoy en día es muy difícil encontrar una red de computadoras sin un firewall, ya que como veremos estos se han convertido en una herramienta indispensable para cualquier institución que conste de una red.

Existen diferentes estructuras de firewalls las mismas que serán detalladas más adelante en este capítulo.

1.2 Conceptos Generales

Firewall: Un firewall es un software creado con el fin de controlar y gestionar el flujo de la información mediante el uso de reglas, las cuales nos permiten definir que paquetes entran a nuestra red y que paquetes salen de la misma. Un firewall también puede ser implementado en hardware o en una combinación de hardware y software.

1.3 Diferentes Tipos Firewalls

1.3.1 Firewall de filtrado de paquetes

Este firewall funciona a nivel de red de la pila de protocolos TCP/IP a manera de filtro de paquetes IP, puesto que trabaja a este nivel puede realizar su control según los campos de los paquetes IP como es el caso de dirección IP destino y dirección IP origen. Además permite filtrado a nivel de enlace de datos (direcciones MAC), y campos de nivel de transporte (puerto origen y destino).

1.3.2 Firewall de capa de aplicación

Este tipo de firewall puede bloquear tanto el tráfico http como otros protocolos de nivel de aplicación, los firewalls de aplicación pueden evitar que todo el tráfico externo entre a las máquinas protegidas, también sirven para comprobar que los protocolos (ftp, http, etc.) estén funcionando correctamente.

1.3.3 Firewall personal

Un firewall personal puede considerarse como un software de computadoras que filtre las comunicaciones entre dicho computador y el resto de la red.

1.4 Estructuras de firewalls

1.4.1 Router sin firewall

Esta configuración deja un router entre la red interna y la red externa, es una de las configuraciones más conocidas.
Como podemos observar en la figura 1 la red privada prácticamente no tiene protección, la vulnerabilidad de este esquema depende únicamente de un router.

VENTAJAS	**DESVENTAJAS**
Barata	Inflexible
Fácil de configura.	Servidores públicos y Clientes vulnerables a la red Exterior
Fácil de Operar	Defensa superficial depende solo del Enrutador

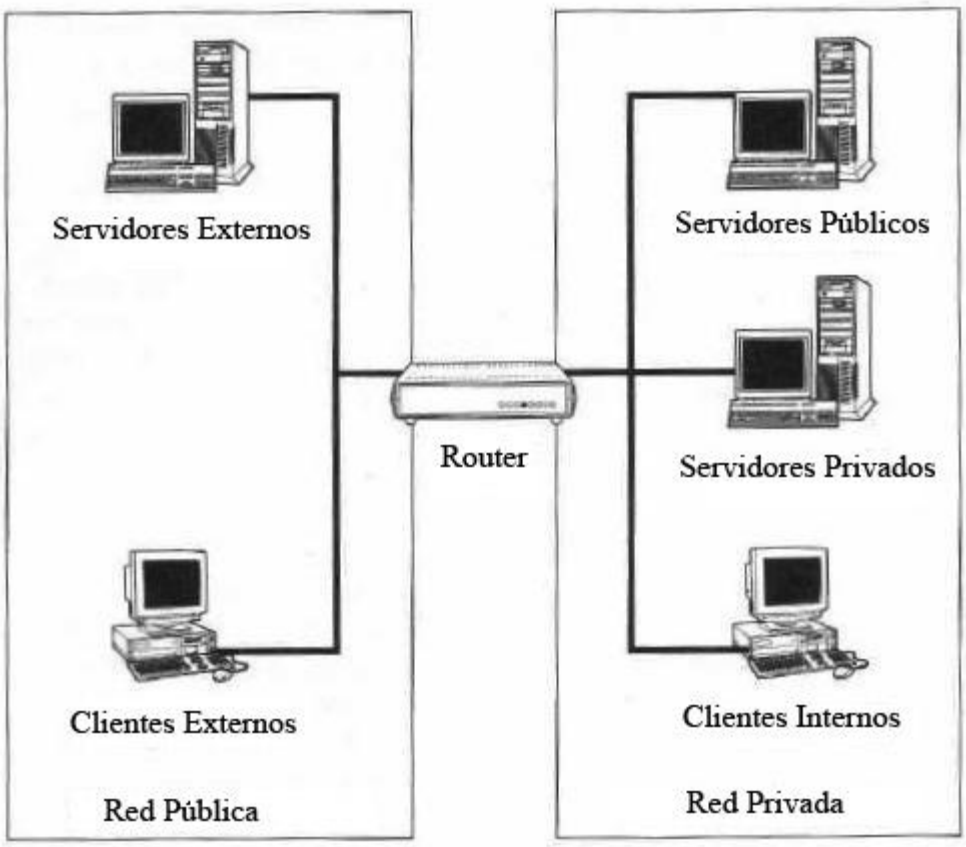

Figura 1.[1] ***Red sin protección***

1.4.2 Firewall con hosts expuestos

Como se puede apreciar en la figura 2 se ha modificado un poco el esquema anterior con el aumento un firewall, el mismo que protege los servidores privados de la red externa publica, al mismo tiempo una nueva sección es creada para los servidores públicos que al igual que en el esquema anterior quedan expuestos a cualquier ataque.

Con esta configuración se pueden evitar intrusiones mal intencionadas sobre los servidores privados y clientes internos.

[1] M.C. Ibarra Francisco. Firewalls en Linux .Instituto Tecnológico Hermosillo. Francisco Ibarra Lemas. 7 de Junio del 2006 [citado 2006-09-15]

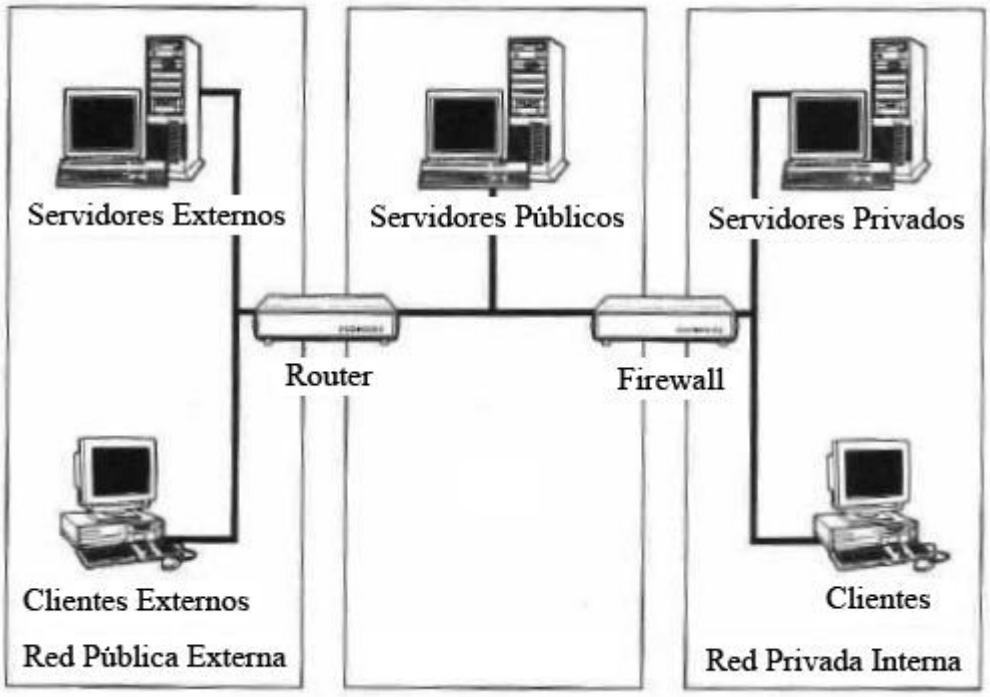

Figura 2.[2] ***Red con un firewall.***

.

VENTAJAS	**DESVENTAJAS**
Más flexible que la anterior	Ligeramente más costosa
Clientes están protegidos por el Firewall	Los servidores públicos se encuentran expuestos
Servidores privados protegidos	Solo un firewall para protección

1.4.3 Esquema con dos firewalls

Este modelo prácticamente puede evitar todo tipo de intrusiones, como se puede observar en la figura 3 el esquema consta de 2 firewalls implementando así una defensa en dos capas. Es un diseño sin fisuras pero con el inconveniente de ser un poco más costoso que el modelo anterior.

[2] M.C. Ibarra Francisco. Firewalls en Linux .Instituto Tecnológico Hermosillo. Francisco Ibarra Lemas. 7 de Junio del 2006 [citado 2006-09-15]

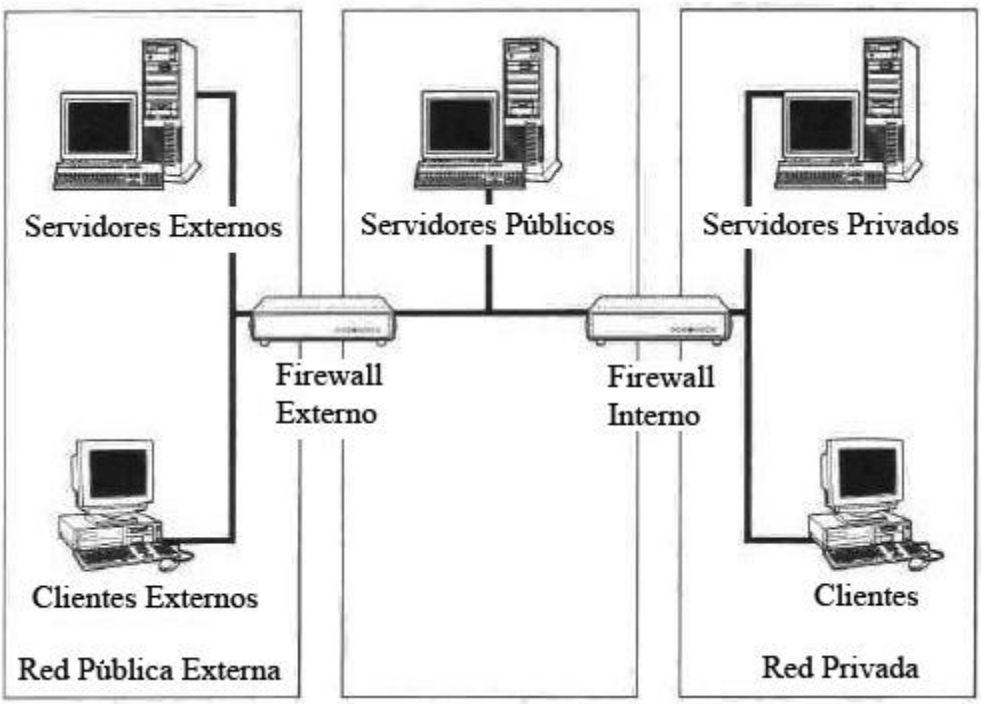

Figura 3.[3] ***Esquema con dos firewalls***

VENTAJAS	**DESVENTAJAS**
Los servidores públicos están protegidos	Más costosa que las anteriores
Los clientes están protegidos	
La defensa está implementada en dos capas	
Servidores privados protegidos	

1.4.4 Firewall de tres interfaces

Con esta configuración se da protección a los servidores así como a los clientes internos, es un diseño muy seguro pero un poco más complicado de configurar. Este esquema permite tener una red muy segura a un costo razonable. Ver figura 4.

[3] M.C. Ibarra Francisco. Firewalls en Linux .Instituto Tecnológico Hermosillo. Francisco Ibarra Lemas. 7 de Junio del 2006 [citado 2006-09-15]

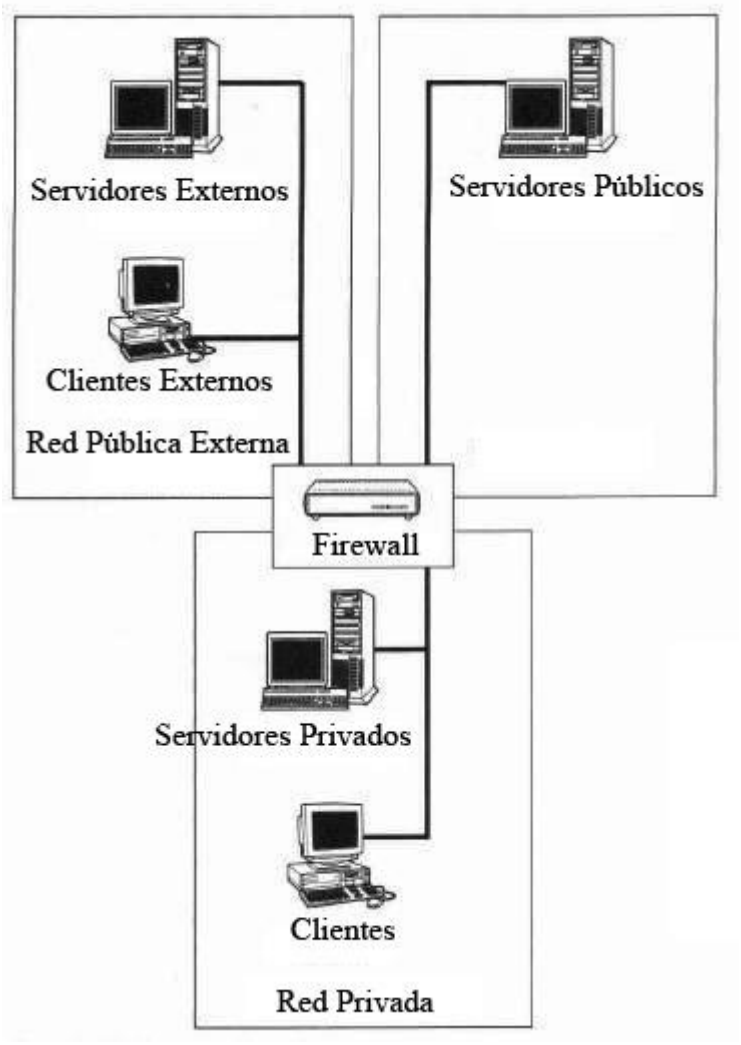

Figura 4[4]. ***Firewall de tres interfaces***

VENTAJAS	**DESVENTAJAS**
Más barata que la anterior	Más complicada de configurar y administrar que las anteriores
Servidores públicos, privados y Clientes protegidos	

[4]M.C. Ibarra Francisco. Firewalls en Linux .Instituto Tecnológico Hermosillo. Francisco Ibarra Lemas. 7 de Junio del 2006 [citado 2006-09-15]

1.5 Conclusiones

En este capítulo pudimos considerar los diferentes tipos y estructuras de firewalls, entendiendo así su funcionamiento e importancia.

Los firewalls han llegado a ser prácticamente indispensables en cualquier red de computadores (con o sin acceso a Internet). Como hemos visto, estos son útiles tanto para el control de intrusiones como para mejorar la eficiencia de una red mediante el manejo adecuado de sus protocolos.

En el siguiente capítulo veremos las configuraciones más importantes de un firewall aplicadas al programa shorewall.

CAPÍTULO II

SHOREWALL

2 Shorewall

2.1 Introducción a Shorewall

Debido a la complejidad de las reglas de Iptables han aparecido varias herramientas para la generación de las mismas, una de estas es "*Shorewall"* (Shoreline Firewall) una robusta utilidad para la configuración de un firewall. La misma que mediante el ingreso de parámetros en algunos archivos de texto simple, generara las reglas correspondientes a la configuración deseada.

Este capítulo contiene una documentación detallada de los archivos de Shorewall, si usted desea realizar una configuración habitual puede dirigirse al contenido de configuraciones de este capítulo (2.5 Configuración).

2.2 Definición

Shorewall es un software que nos permite llevar a cavo una implementación sencilla de firewall, con la ayuda de Iptables. Para la configuración de Netfilter shorewall puede ser usado sobre un sistema de firewall dedicado, multifuncional o inclusive en un computador personal con GNU/Linux.

Probablemente esta es la herramienta para la configuración de *Netfilter* más flexible de hoy en día.

2.3 Instalación

Existen dos formatos de archivos para la instalación:

- Archivo .tar.gz
- Archivo .rpm

Los cuales pueden ser descargados desde http://www.shorewall.net/

2.3.1 Requisitos.

- Sistema Operativo GNU/Linux
- Paquete shorewall 3.x
- Una o más interfaces, dependiendo de la estructura de la red

2.3.2 Procedimientos.

Para instalar el paquete .tar.gz debemos copiar el archivo a un directorio y escribir lo siguiente:

```
tar –vzgf archivo.tar.gz
```

Esto descomprimirá el contenido del archivo en una carpeta, generalmente con el mismo nombre. Luego de esto debemos acceder a la carpeta en donde se encuentra el archivo "configure.sh" y escribir ./configure.sh para compilarlo, por último escribiremos make install para que el paquete sea instalado.

Para instalar el paquete .rpm debemos copiar el archivo a un directorio y escribir lo siguiente:

```
rpm –i archivo.rpm
```

2.4 Componentes de Shorewall

Los componentes de Shorewall se encuentran en la ruta /etc/shorewall/

2.4.1 Archivo shorewall.conf

Es necesario definir los valores de los dos primeros parámetros, en los restantes por lo general se podrá dejar el valor predeterminado.

A continuación explicamos los parámetros.

a) STARTUP_ENABLED

Su valor predeterminado es “No”; una vez configurado Shorewall, debe cambiar la especificación de este parámetro a “Yes”, para que Shorewall pueda iniciarse.

b) CLAMPMSS[=<value>]

Este parámetro habilita el *TCP Clamp MSS* para PMTU característica de Netfilter usualmente requerida cuando la conexión de Internet es a través de PPPoE o PPTP. Si establece “Yes”, habilitara esta característica. Si deja en blanco o coloca “no”, deshabilita esta característica.

Puede también especificar un valor numérico. Ej.

CLAMPMSS=1400.

c) IPTABLES

Ruta completa para el ejecutable de Iptables, que Shorewall usa para crear el firewall. Si no se especifica o se especifica un valor vacío (IPTABLES=“”), entonces el ejecutable de Iptables usará la ruta especificada en PATH.

d) PATH

Modifique esto si quiere cambiar el orden en que Shorewall buscará los directorios para archivos ejecutables. Ej.

PATH=/sbin:/bin:/usr/sbin:/usr/bin:/usr/local/bin:/usr/local/sbin

e) SHELL

El script del firewall es interpretado normalmente por /bin/sh. Si desea cambiar el shell usado para interpretar ese script, especifique el shell aquí. Ej

SHOREWALL_SHELL=/bin/sh

f) SUBSYSTEM LOCK FILE

Aquí se coloca el nombre del archivo protegido esperado por su script de inicio. Para Redhat esto debe ser /var/lock/subsys/shorewall. Si su script de inicio no usa archivos protegidos, establezca el valor nulo "". Ej.

SUBSYSLOCK=/var/lock/subsys/shorewall

g) DIRECTORIO DEL MODULO KERNEL

Si su modulo kernel de netfilter esta en un directorio distinto a /lib/modules/$(uname -r)/kernel/net/ipv4/netfilter entonces especifíquelo en esta variable. Ej.

MODULESDIR=/etc/modules

De lo contrario déjelo vacío. Ej.

MODULESDIR=

h) HABILITAR EL REENVIO IP

Si establece "on", habilita el reenvío de paquetes de IPV4. Si establece "off" el reenvío de paquetes estará deshabilitado.

IP_FORWARDING=On

i) AUTOMATICAMENTE AGREGUE DIRECCIONES IP A NAT.

Si establece "Yes", Shorewall automáticamente agregara direcciones IP para cada dirección externa NAT que haya especificado en /etc/shorewall/nat. Si establece "No", usted deberá agregar esos alias.

ADD_IP_ALIASES=Yes

j) AUTOMATICAMENTE AGREGUE DIRECCIONES IP A SNAT.

Si establece "Yes", Shorewall automáticamente agregara direcciones IP para cada dirección externa SNAT que haya especificado en /etc/shorewall/masq. Si establece "No", usted deberá agregar esos alias.

ADD_SNAT_ALIASES=No

k) ROUTE_FILTER

Si coloca “Yes” entonces el filtrado de ruta (anti-spoofing) se habilitara sobre todas las interfaces de red levantadas mientras Shorewall esta en estado de inicio, el valor predeterminado es “No”.

m) DETECT_DNAT_ADDRS

Si coloca “Yes” Shorewall detectara la primera dirección IP de la interface para la zona de origen e incluirá esta dirección en las reglas de DNAT, así como la dirección IP de destino original. Si coloca “No” Shorewall no detectara esta dirección y cualquier dirección IP de destino cumplirá con la regla DNAT.

Si no se especifica o se deja vacío, se asume:

DETECT_DNAT_ADDRS=Yes

n) MUTEX TIMEOUT

El valor de esta variable determina el número de segundos que los programas esperaran para acceder al archivo protegido de Shorewall. Si se deja vacío, se asume un valor de 60 (60 segs). Ej.

MUTEX_TIMEOUT=60

Un valor apropiado para este parámetro sería dos veces la cantidad de tiempo que tarda su sistema de firewall para procesar el comando “shorewall restart”.

o) ADMINISABSENTMINDED

El valor de esta variable afecta cuando Shorewall esta detenido.

Cuando ADMINISABSENTMINDES=No, solo el tráfico hacia/desde las direcciones listadas en /etc/shorewall/routestopped es aceptado cuando Shorewall esta parado.

Cuando ADMINISABSENTMINDED=Yes, además de el tráfico hacia/desde las direcciones listadas en /etc/shorewall/routestopped y las conexiones que estaban activas cuando Shorewall fue parado continúan trabajando, además todas las nuevas conexiones del propio sistema de firewall son permitidas.

Si esta variable no se especifica o se deja vacía el valor asumido es: ADMINISABSENTMINDED=No.

p) BLACKLISTNEWONLY

BLACKLISTNEWONLY=Yes Solo consulta blacklists (/etc/shorewall/blacklist) para nuevas conexiones requeridas.

BLACKLISTNEWONLY=No Consulta blacklists para todos los paquetes.

Si no se establece el valor o se deja vacío se asume “no”:

q) DELAYBLACKLISTLOAD

Los usuarios con una extensa blacklist (/etc/shorewall/blacklist) encuentran que “Shorewall [re]start” toma un largo tiempo y las nuevas conexiones son deshabilitadas durante ese tiempo. Con DELAYBLACKLISTLOAD=Yes, Shorewall habilita las nuevas conexiones antes de cargar la blacklist.

Valor predeterminado DELAYBLACKLISTLOAD=No.

r) BRIDGING

Si desea restringir conexiones a través de bridge, entonces coloque BRIDGING=Yes.

Si no especifica el valor se asume:

BRIDGING=No

s) DYNAMIC ZONES

Si necesita poder agregar o borrar hosts de zonas dinámicamente entonces coloque

DYNAMIC_ZONES=Yes. De otra forma, coloque DYNAMIC_ZONES=No.

t) MACLIST cacheando

Si sus Iptables y kernel soportan el "Recent Match", los resultados de las direcciones MAC pueden ser guardados en el archivo /etc/shorewall/maclist y así reducir el exceso de cabeceras asociado con la verificación de direcciones MAC.

u) MACLIST_TTL si este parámetro es dejado en blanco como por ejemplo MACLIST_TTL="" el archivo 'maclist' no guardara ninguna dirección MAC.

v) BLACKLIST DISPOSICION

En esta variable se establece la acción que se desea en cuanto al comportamiento de los paquetes que constan en la Blacklist (lista negra), los valores DROP o REJECT sirven para rechazarlos. El parámetro por defecto esta en:

BLACKLIST_DISPOSITION=DROP

w) MAC List Disposición

Esta variable determina la disposición de la respuesta a las conexiones que llegan de un dispositivo que no esta en esta lista, los valores pueden ser ACCEPT, DROP o REJECT. Si es que no se especifica nada el valor por defecto es:

MACLIST_DISPOSITION=REJECT

2.4.2 Archivo zones

Una zona es una subred que goza de los mismos privilegios (políticas). Una zona puede ser uno o varios hosts.

Este archivo es usado para definir las zonas (divisiones de la red o subredes).
Para cada zona existe una entrada en este archivo, su ruta es /etc/shorewall/zones.
Sus columnas son las siguientes:

a) ZONE

Nombre corto para la zona. El nombre debe ser de 5 caracteres de longitud o menos, y consistir de letras minúsculas o (y) números. Los nombres cortos deben comenzar con una letra. El nombre asignado al firewall está reservado para el uso de Shorewall.

El nombre “all” no se puede usar como nombre de zona, tampoco puede asignarse el nombre de zona por medio de la variable FW en /etc/shorewall/shorewall.conf.

b) TYPE

ipsec - Todo el tráfico desde/hacia esta zona es encriptado.

ipv4 - Por omisión, el tráfico desde/hacia algunas de las máquinas en esta zona no es encriptado. Cualquier máquina encriptada es designada usando la opción ipsec en /etc/shorewall/hosts.

firewall - Designa al firewall mismo. Usted debe tener exactamente una única zona 'firewall'. No se permiten opciones a la zona 'firewall'.

c) OPTIONS, IN OPTIONS, OUT OPTIONS

Parámetros opcionales que identifican la política de seguridad y las asociaciones de seguridad utilizadas en las comunicaciones con las máquinas en la zona respectiva.

El orden de las entradas en el archivo /etc/shorewall/zones es significativo en algunos casos.

2.4.3 Archivo interfaces

Este archivo se usa para especificar al firewall cual de las interfaces de red esta conectada a una zona. Habrá una entrada en /etc/shorewall/interfaces para cada una de sus interfaces. Las columnas son las siguientes:

a) ZONE

Aquí se especifica la zona con el mismo nombre que fue definida en el archivo /etc/shorewall/zones. Si especifica “-” usted deberá usar el archivo /etc/shorewall/hosts para definir los accesos a las zonas.

b) INTERFACE

Sirve para definir el nombre de la interfaz (ejemplo: eth0, ppp0, ipsec+). Cada interfaz puede listarse en una única entrada en este archivo.

Nota: No necesita incluir la interfaz de realimentación (lo) en este archivo.

c) BROADCAST

Aquí se definen la(s) dirección(es) de difusión (broadcast) para la(s) subred(es) conectadas a las interfaces. Esto debería dejarse sin especificar para el caso de interfaces P-T-P (ppp*, ippp*); si necesita especificar opciones para tales interfaces escriba "-" en esta columna. Si suministra el valor especial "detect" en esta columna, el firewall automáticamente determinará la dirección de broadcast.

Para usar "detect":

La interfaz debe estar levantada antes de arrancar el firewall.

La interfaz sólo debe estar conectada a una única subred (i.e., debe existir una única dirección de broadcast).

d) OPTIONS

Especifica una lista de opciones separadas por comas. Las opciones posibles incluyen:

arp_filter

Esta opción hace que /proc/sys/net/ipv4/conf/<interfaz>/arp_filter sea puesto, lo que resulta en que esa interfaz solo responda solicitudes ARP desde máquinas que están al alcance de esa interfaz. El activar esta opción facilita las pruebas del firewall cuando se conectan múltiples interfaces al mismo HUB/Switch (todas las interfaces conectadas al mismo HUB/Switch deberían tener esta opción especificada).

"Note que usar tal configuración en un ambiente de producción no es nada recomendable."

arp_ignore

arp_ignore[=<number>] responde a las solicitudes ARP basándose en el valor de <number>. Ej.

Valor

1 Responder si la dirección IP destino es dirección local configurada en la interfaz entrante

2 Responder sólo si la dirección IP destino es dirección local configurada en la interfaz entrante y la dirección IP de quien envía es parte de la misma subred en esa interfaz

3 No responder para direcciones locales configuradas con alcance de máquina, sólo resoluciones para direcciones globales y de enlace son respondidas

4 -7 Reservado

8 No responder para todas las direcciones locales

Si no se especifica <number> se asume el valor 1

No especifique arp_ignore para interfaces involucradas en Proxy ARP.

routeback

Esta opción hace que Shorewall configure el manejo de los paquetes en enrutamiento que llegan en esta interfaz para que salgan de vuelta por esta misma. Si esta opción se especifica la columna ZONE no puede contener “-”.

tcpflags

Esta opción hace que Shorewall realice verificaciones de las banderas en los encabezados TCP que llegan por esta interfaz. Las verificaciones incluyen banderas Nulas, SYN+FIN, SYN+RST y FIN+URG+PSH; estas combinaciones de banderas son típicamente usadas para hacer escaneos de puertos "silenciosos". Los paquetes que fallen estas verificaciones son registrados de acuerdo a la TCP_FLAGS_LOG_LEVEL en /etc/shorewall/shorewall.conf y se dispone de ellos de acuerdo a la opción TCP_FLAGS_DISPOSITION.

blacklist

Esta opción hace que los paquetes entrantes en esta interfaz sean verificados contra la lista negra (blacklist).

dhcp

El firewall será configurado para permitir el tráfico DHCP desde y hacia esta interfaz incluso si este está detenido.

routefilter

Invoca la habilidad del Kernel para filtrar rutas (anti-spoofing) en esta interfaz. El kernel rechazará cualquier paquete entrante en esta interfaz que tenga dirección origen tal que deba ser enrutado hacia afuera por medio de otra interfaz en el firewall.

Si especifica esta opción para una interfaz, esta debe estar activada antes de arrancar el firewall.

maclist

Si se especifica esta opción todas las solicitudes de conexión desde esta interfaz están sujetas a verificación MAC. Sólo puede especificarse para interfaces Ethernet.

detectnets

Si esta opción se especifica la zona que se nombre en la columna ZONE contendrá sólo las máquinas enrutadas por medio de la interfaz nombrada en la columna INTERFACE. No ponga esta opción en su interfaz (Internet) externa. La interfaz debe estar ARRIBA antes de (re)iniciar el Shorewall.

nosmurfs

Si se especifica esta opción las solicitudes de conexión entrante serán verificadas para asegurar que ellas no tienen una dirección de broadcast o multicast como origen. Cualquiera de estos paquetes serán descartados después registrar esta actividad y de acuerdo a los ajustes de SMURF_LOG_LEVEL en /etc/shorewall/shorewall.conf.

2.4.4 Archivo policy.

Este archivo se usa para describir la política del firewall acerca del establecimiento de conexiones. El establecimiento de conexión está descrito en términos de clientes que inician conexiones y servidores que reciben dichas solicitudes de conexiones. Las políticas definidas en este archivo describen qué zonas están permitidas a establecer conexiones con otras zonas.

Las políticas establecidas en este archivo actúan así: Si no aplica ninguna regla en el archivo */etc/shorewall/rules* a una solicitud de conexión en particular entonces la política de */etc/shorewall/policy* se aplica.

Se definen seis políticas:

ACCEPT .- Se permite la conexión.

DROP .- La solicitud de conexión se ignora.

REJECT .- La solicitud de conexión se rechaza con un paquete RST (eTCP) o un paquete ICMP destination-unreachable (destino inalcanzable) de notificación al cliente.

QUEUE .- Envía la solicitud de conexión a un proceso en espacio-usuario por medio del destino Iptables QUEUE (útil cuando usa Snort-inline).

CONTINUE .- La conexión no es aceptada (ACCEPT), descartada (DROP) ni rechazada (REJECT). CONTINUE puede usar cuando una o ambas zonas nombradas en la entrada son subzonas de o intersecan con otra zona. Más adelante hablaremos detalladamente de esta política.

NONE .- Shorewall no debería configurar ninguna infraestructura para manejar tráfico desde la zona SOURCE hacia la zonas DEST. Cuando se especifica esta política las columnas LOG LEVEL y BURST:LIMIT deben dejarse en blanco.

Para cada política puede indicar que quiere enviar un mensaje al registro del sistema (log), cada vez que se aplica la política.

Las entradas en el archivo */etc/shorewall/policy* tiene cinco columnas como:

a) Columna SOURCE

El nombre de una zona cliente (una zona definida en el archivo /etc/shorewall/zones, el nombre de la zona del firewall o "all").

b) Columna DEST

El nombre de una zona destino (una zona definida en el archivo /etc/shorewall/zones, el nombre de la zona del firewall o "all"). Shorewall automáticamente permite todo tráfico del firewall a el mismo, así el nombre de la zona del firewall no puede aparecer en ambas columnas (SOURCE y DEST).

c) Columna POLICY

La política predeterminada para la conexión requerida de la zona SOURCE (origen) a la zona DESTINATION (destino).

d) Columna LOG LEVEL (Opcional).

Si deja vacío no se generaran mensajes cuando la política sea aplicada. De otra forma, esta columna debe contener un entero o un nombre que indique un nivel *syslog*.

e) Columna LIMIT:BURST – (Opcional)

Si deja vacío, la conexión TCP requerida desde la zona SOURCE (origen) hacia la zona DEST (destino), no será una tasa limitada. De otra forma, esta columna especifica la máxima tasa a la cual la conexión TCP requerida será aceptada seguida por (":") y seguida por el máximo tamaño de ráfaga que tolerará. Ej.

10/sec:40 especifica que la máxima tasa de conexión TCP requerida permitida será de 10 por segundo y tolerara una ráfaga de 40 conexiones. Las conexiones requeridas que excedan estos límites serán ignoradas.

En las columnas SOURCE y DEST, puede colocar “all” para indicar todas las zonas.

A continuación se muestra la configuración mínima de este archivo */etc/shorewall/policy*:

SOURCE	DEST	POLICY	LOG LEVEL	LIMIT:BURST
loc	net	ACCEPT		
net	all	DROP	info	
all	all	REJECT	info	

Esta tabla se interpreta así:
La Primera línea dice.- Todas las conexiones desde (SOURCE) la red local (loc) hacia (DEST) cualquier host en Internet son aceptadas (ACCEPT).
La segunda línea dice.- Todas las conexiones requeridas desde(SOURCE) Internet (net) hacia (DEST), cualquier destino(all), son ignoradas y registradas.
La tercera línea dice.- Todas las otras conexiones requeridas (all a all) son rechazadas y registradas.

Precaución para la configuración de políticas:
El script del firewall procesa el archivo /etc/shorewall/policy desde arriba hacia abajo y usa la primera política aplicable que encuentra.

2.4.4.1 Tráfico Intra-zonal

Shorewall permite a una zona estar asociada con más de una interfaz o con múltiples redes a través de una sola interface. Shorewall aceptará (ACCEPT) todo el tráfico desde una zona hacia esta misma, en otras palabras:

- Una zona debe ser homogénea con respecto a los requerimientos de seguridad.
- El tráfico dentro de una zona no requiere de reglas o políticas.
- Shorewall no restringirá el tráfico dentro de una zona.

2.4.4.2 La política CONTINUE:

Donde las zonas están anidadas o solapadas, la política CONTINUE permite a los hosts, que están dentro de zonas múltiples, ser manejados bajo las reglas de todos de esas zonas.

Veamos en un ejemplo:

Archivo /etc/shorewall/zones:

#ZONE	TYPE	OPTION
$FW	firewall	
sam	ipv4	
net	ipv4	
loc	ipv4	

Archivo /etc/shorewall/interfaces:

#ZONE	INTERFACE	BROADCAST	OPTIONS
-	eth0	detect	dhcp,norfc1918
loc	eth1	detect	

Archivo /etc/shorewall/hosts:

#ZONE	HOST(S)	OPTIONS
net	eth0:0.0.0.0/0	
sam	eth0:206.191.149.197	

Nota.- El sistema home de Sam es un miembro de ambas zonas, la zona sam y la zona net, como se describe arriba, eso significa que sam debe ser listado antes de net en el archivo /etc/shorewall/zones.

/etc/shorewall/policy:

SOURCE	DEST	POLICY	LOG LEVEL
loc	net	ACCEPT	
sam	all	CONTINUE	
net	all	DROP	info
all	all	REJECT	info

La segunda entrada arriba especificada, dice que cuando sam es el cliente, la conexión requerida debe primero ser procesada bajo las reglas donde la zona origen (SOURCE) es sam, y si no cumple entonces la conexión requerida debe ser tratada bajo las reglas donde la zona origen (SOURCE) es net.
Es importante que esta política (CONTINUE), sea listada ANTES de la política (net to all).
Porción del archivo: /etc/shorewall/rules:

```
#ACTION   SOURCE    DEST          PROTO    DEST PORT(S)
---
DNAT      sam       loc:192.168.1.3 tcp      ssh
DNAT      net       loc:192.168.1.5 tcp      www
---
```

Dando esas dos reglas(el orden de las reglas no es significante), en la primera línea.- sam puede conectarse a la interface de Internet del firewall con ssh y el requerimiento de conexión será reenviado a 192.168.1.3.
En la segunda línea.- como todos los hosts en la zona net, Sam puede conectarse a la interface de Internet del firewall activando TCP puerto 80 y la conexión requerida será reenviada a 192.168.1.5.

2.4.5 Archivo rules

El archivo /etc/shorewall/rules define excepciones a las políticas establecidas en el archive /etc/shorewall/policy. Hay una entrada en este archivo para cada regla. Las entradas en este archivo solo se rigen para el establecimiento de nuevas conexiones. Los paquetes que son parte de una conexión existente, o que establecen una conexión que esta relacionada a una conexión existente son automáticamente aceptados.

Las reglas para cada par de zonas (zona origen, zona destino), son evaluadas en el orden que aparecen en el archivo.
Regla LOG hace que la conexión requerida sea registrada, luego continua procesando la siguiente regla en el archivo.

Regla CONTINUE hace que la conexión requerida sea procesada usando un diferente par (zona origen, zona destino).

El archivo /etc/shorewall/rules puede estar por secciones. Cada sección esta establecida por una línea que inicia con la palabra SECTION la cual esta seguida por el nombre de la sección. Las secciones están listadas abajo y deben aparecer en el orden mostrado.

Las secciones son las siguientes:

Sección ESTABLISHED

Las reglas en esta sección se aplican a paquetes en estado establecido.

Sección RELATED

Las reglas en esta sección se aplican a paquetes en estado relacionado.

Sección NEW

Las reglas en esta sección se aplican a paquetes en estado nuevo e invalido.

Las reglas en las secciones ESTABLISHED y RELATED están limitadas a las siguientes ACCIONES:

ACCEPT, DROP, REJECT, QUEUE, LOG y acciones definidas por el usuario.

Al final las secciones ESTABLISHED y RELATED, hay una regla implícita ACCEPT.

RESTRICCION: Si usted especifica FASTACCEPT=Yes en el archivo /etc/shorewall/shorewall.conf, las secciones ESTABLISHED y RELATED deben estar vacías.

Las entradas en el archivo tienen las siguientes columnas:

a) Columna ACTION puede contener las acciones ACCEPT, DROP, REJECT y CONTINUE.

Estos tienen el mismo significado aquí como en el archivo policy visto anteriormente, también se aceptan las siguientes acciones.

ACCEPT+

Trabaja como ACCEPT pero también exceptúa las conexiones de las reglas correspondientes a DNAT y REDIRECT.

NONAT

Exceptúa conexiones correspondientes de reglas DNAT y REDIRECT.

DNAT

Hace que la conexión requerida sea reenviada al sistema especificado en la columna DEST.

REDIRECT

Hace que la solicitud de conexión sea redirigida a un puerto dentro del sistema local (firewall).

REDIRECT-

La ACTION (REDIRECT) de arriba genera dos reglas Iptables:
Una regla header-rewriting en la tabla Netfilter “nat”
Una regla ACCEPT en la tabla Netfilter “filter”.
REDIRECT- trabaja como REDIRECT pero solo genera la primera regla.

QUEUE

Reenvía el paquete a una aplicación user-space.
El uso de DNAT o REDIRECT requiere que tenga habilitado NAT en su configuración del kernel.

b) Columna SOURCE

Describe los hosts de origen para los cuales se aplica las reglas. El contenido de este campo debe iniciar con el nombre de la zona definida en /etc/shorewall/zones, $FW, “all” o "none". Si la ACTION es DNAT o

REDIRECT, las subzonas pueden estar excluidas de la regla anteponiendo “!” al nombre de la zona y una coma para separar la lista a ser excluidas.
Si el origen es "none" la regla es ignorada.

c) Columna DEST
Describe el host destino, el cual se aplica a la regla.
Podría definir de varias maneras, para describir mostraremos dos:
Una dirección IP seguida por dos puntos y el numero de puerto que el servidor esta escuchando. Ej. loc:192.168.0.1:80

d) Columna SUBNET
Hace referencia al pedido de conexión desde cualquier host en la subred especificada (Ej. net:10.0.0.1/24). Se puede especificar un rango de direcciones IP siempre y cuando el kernel lo soporte.

Restricciones:
Usted no necesita especificar los dos, la dirección IP y el nombre de interface en la columna DEST.
En las reglas DNAT solo la dirección IP es permitida, los nombres DNS no son permitidos.
Así como en la columna SOURCE, un rango de direcciones pude ser especificado en la columna DEST. Cuando la columna ACTION es DNAT o DNAT-, las conexiones deberían ser asignadas a las direcciones en un rango.
La dirección MAC no debe ser específica.

e) Columna PROTO
El protocolo debe ser especificado con un nombre de /etc/protocols, un número o “all”. Especifica el protocolo de la petición de conexión.

f) Columna DEST PORT(S)
Puerto o un rango de puertos a ser conectado. Podría solo ser especificado si el protocolo es tcp, udp o icmp. Para icmp el contenido de esta columna es interpretado como de tipo icmp. Si usted no desea especificar el DEST

PORT(S) pero necesita incluir información en una de las columnas de la derecha debe introducir "-" en esta columna. Si desea introducir una lista de puertos puede separarlos con comas.

g) Columna SOURCE PORTS(S)

Esta columna puede ser usada para restringir una regla para el puerto o rango de puertos de un cliente en particular. Si usted no desea restringir los puertos pero desea especificar algo en la columna siguiente debe introducir "-" en esta columna. Los puertos pueden ser separados por comas.

Los puertos pueden ser nombres del archivo /etc/services.

h) Columna ORIGINAL DEST

Esta columna no puede estar vacía si la acción es DNAT o REDIRECT.

Si DNAT o REDIRECT es la acción y la columna ORIGINAL DEST es dejada en blanco, cualquier pedido de conexión que llegue al firewall desde SOURCE que coincida con la regla será reenviada o redireccionada. Esto funciona bien para pedidos de conexión que llegan desde el Internet, donde el firewall tiene una sola dirección IP externa.

Cuando el firewall tiene varias direcciones IP externas o cuando la columna SOURCE no es el Internet, ahí usualmente la regla solo aplica a los pedidos de conexión para una dirección IP particular. Esta dirección IP es especificada en ORIGINAL DEST y puede ser separada por comas.

i) Columna RATE LIMIT

Usted puede usar reglas ACCEPT, DNAT[-], REDIRECT[-] o LOG para el rate-limit con una entrada en la columna. Ej.

ACCEPT<4/sec:5> net dmz tcp 80

Al inicio esta regla es cumplida, el paquete sería aceptado efectivamente, puesto que la ráfaga es 5, los primeros 5 paquetes serían aceptados, después de esto se aceptará un paquete cada 250 mili segundos (un segundo dividido para el rate de 4).

Si usted desea especificar algo en las siguientes columnas pero sin un límite de tasa (rate) deje "-" en la columna.

2.4.6 Archivo masq para enmascaramiento.

El archivo */etc/Shorewall/masq* es usado para definir el clásico enmascaramiento de IP y la traducción de direcciones de red origen (SNAT). En este archivo hay que ingresar una entrada para cada subred que se desee enmascarar, a fin de usar esta característica se debería tener habilitado el NAT.

Las columnas de este archivo son: INTERFACE, SUBNET, ADDRESS y PROTO

a) Columna INTERFACE

La columna INTERFACE es normalmente la interface de Internet, en este campo también se puede especificar direcciones IP, si es que se escribe ":" seguido de la interfaz, esto indicaría que solo los paquetes provenientes de esa dirección serán enmascarados. Ej.

eth0:192.0.2.8/29,192.0.2.32/29

Si se escribe después de ":" el signo de admiración "!" indicaremos que todos los paquetes que no vengan de esa dirección serán enmascarados. Ej.

eth0:!192.0.2.8/29,192.0.2.32/29

Si tu has configurado el campo ADD_SNAT_ALIASES=Yes en el archivo */etc/shorewall/shorewall.conf*, podrías hacer que S*horewall* creara un alias del nombre de la interfaz. Ej.

eth0:0

Un alias creado de esta manera es visible para la utilidad *Ipconfig*.

Normalmente las reglas definidas en MASQUESQUERADE/NAT son evaluadas después de las reglas de NAT definidas en el archivo /etc/shorewall/nat, pero si se escribe el signo "+" antes de la interfaz las reglas serán evaluadas antes de las reglas NAT. Ej.

+eth0

+eth1:192.0.2.32/27

b) Columna SUBNET

En esta columna se especifica la subred que deseamos se enmascarada a través de la INTERFACE, este debería ser expresado como una solo dirección IP, esta columna tiene una sintaxis similar a la de la columna INTERFACE permitiéndonos utilizar los caracteres ":","!", con el mismo efecto del campo de interfaces.

c) Columna ADDRESS

Aquí se especifican las direcciones a ser usadas para los paquetes que salen, esta columna es opcional, si se la deja en blanco la primera dirección IP de la interface será usada.

d) Columna PROTO

Se puede también especificar en este archivo un rango de puertos después de la dirección IP, ingresando también el protocolo en la columna PROTO. Ej.

```
#INTERFACE    SUBNET     ADDRESS               PROTO
eth0          10.0.0.0/8 192.0.2.44:7000-8000  udp

#INTERFACE SUBNET        ADDRESS               PROTO
eth0          192.168.1.0/24:4000-5000         tcp
```

Algunas aplicaciones de Internet que establecen múltiples conexiones para un cliente asumen que cuando SNAT esta siendo utilizado entre el cliente y un servidor remoto, estos tienen la misma dirección IP externa. Usted puede asegurar que este es el caso precediendo el rango de direcciones por "SAME:". Ej.

```
#INTERFACE SUBNET        ADDRESS
eth0       10.0.0.0/8    SAME:192.0.2.44-192.168.2.50
```

2.4.7 Archivo nat

El archivo /etc/shorewall/nat es usado para definir el NAT uno a uno, esto significa una entrada en el archivo para cada una de las relaciones de NAT que se desee definir.
A fin de hacer uso de esta característica usted debería tener habilitado NAT.

2.4.8 Archivo blacklist

Cada línea en este archivo contiene direcciones IP y direcciones MAC en formato de shorewall o direcciones de subredes. Ej.
150.202.102.60
201.101.140.0/24
Los paquetes de los hosts listados en el archivo blacklist (lista negra) deberían ser dispuestos de acuerdo a los valores asignados en las variables BLACKLIST_DISPOSITION y BLACKLIST_LOGLEVEL del archivo /etc/shorewall/shorewall.conf.

Solo los paquetes que llegan en las interfaces que tienen la opción de blacklist en el archivo /etc/shorewall/interfaces son chequeados contra la blaklist, La lista negra es diseñada para prevenir que los hosts listados en hosts/subnets del acceso a los servicios en su red.

Las columnas del archivo blacklist son:
ADDRESS/SUBNET: direcciones IP
PROTOCOL: puede ser tcp, udp o icmp
PORTS: numero de puertos

2.5 Configuración

Todas las configuraciones de *Shorewall* se realizan en modo texto, para lo cual se puede usar un editor como el tradicional "vi" o alguno de su preferencia. Si desea dejar un campo sin valor en el archivo *rules* deberá escribir "-".

2.5.1 Archivo de configuración /etc/shorewall/shorewall.conf

Este es el archivo principal para el funcionamiento y arranque de Shorewall. Es usado para definir parámetros del firewall.

Parámetro STARTUP_ENABLED utilizado para activar Shorewall, por defecto se encuentra en "No" lo modificaremos a "Yes".

```
STARTUP_ENABLED=YES
```

Parámetro CLAMPSS, utilizado para conexiones PPP (PPTP o PPPoE), y para definir el MSS (tamaño máximo de segmento), seteado en "Yes" shorewall calculara el MSS más apropiado para la conexión.

```
CLAMPSS=YES
```

2.5.2 Archivo de configuración /etc/shorewall/zones

Utilizado para especificar las zonas que se administraran con shorewall.
Para nuestra exposición nos basaremos en el siguiente esquema.

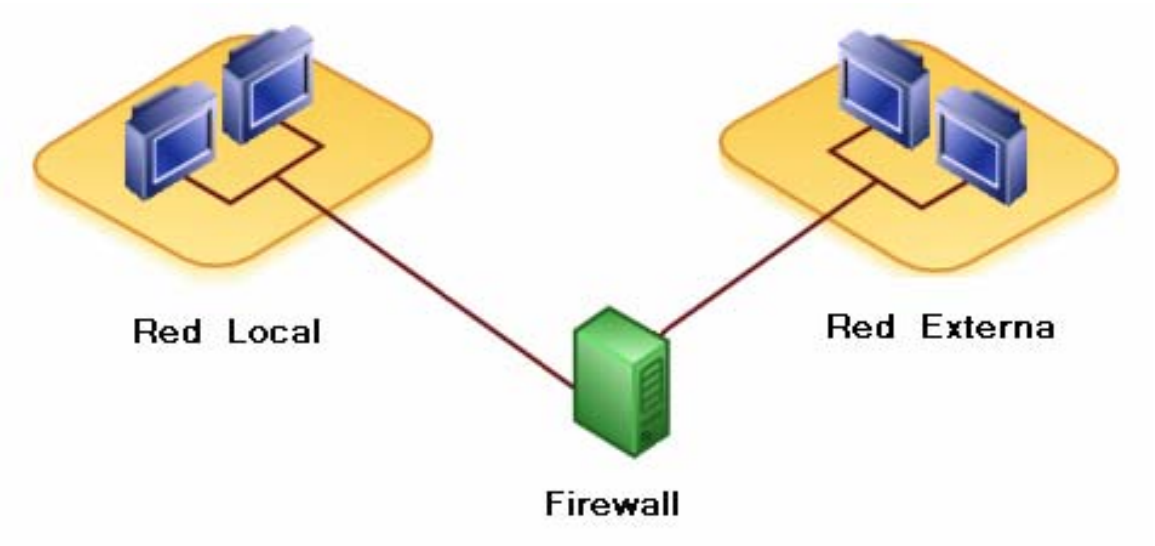

Figura 5. ***Firewall con dos interfaces***

Tipos de Zonas (firewall, ipv4, ipsec zona encriptada)

Loc = Red Local

Net = Red Externa

Fw = Firewall

#ZONE	DISPLAY	OPTIONS
fw	firewall	
loc	ipv4	
net	ipv4	

2.5.3 Archivo de configuración /etc/shorewall/interfaces

En este archivo se establecen las interfaces para las diferentes zonas, en nuestra exposición usaremos dos interfaces Ethernet, eth1 para acceder a la zona net y eth0 para acceder a la zona loc. En todas estas se calcula automáticamente la dirección de *broadcast* mediante el parámetro "detect" en la respectiva columna.

#ZONE	INTERFACE	BROADCAST	OPTIONS
net	eth1	detect	
loc	eth0	detect	

La zona firewall denominada fw esta implícita.
Si existiera un servicio de dhcp habría que especificarlo en el campo *option*.

2.5.4 Archivo de configuración /etc/shorewall/policy

En este archivo se especifican las políticas del firewall para el establecimiento de conexiones, a continuación describimos que zonas se les permite establecer conexiones con otras zonas.

#SOURCE	DEST	POLICY	LOG	LIMIT:BURST
loc	net	ACCEPT		
net	loc	DROP	info	
fw	net	ACCEPT		
all	all	REJECT	info	

Si no se aplica ninguna regla para la solicitud de conexión en el archivo /etc/shorewall/rules, entonces las políticas de /etc/shorewall/policy son aplicadas.

Políticas principales:

- ACCEPT se permite la conexión
- REJECT se rechaza la conexión con una notificación al cliente
- DROP la solicitud de conexión se ignora

2.5.5 Archivo de configuración /etc/shorewall/rules

En este archivo se definen las excepciones a las políticas establecidas en el archivo /etc/shorewall/policy, aquí los puertos están cerrados por defecto. "*Las entradas para este archivo solo actúan para el establecimiento de nuevas conexiones, los paquetes que son parte de una conexión existente o que establecen una conexión que esta relacionada a una conexión existente son automáticamente aceptadas*".[5]

#ACCION	SOURCE	DEST	PROTO(S)	DEST PORT
ACCEPT	net	loc	tcp	80
REJECT	net	loc	icmp	echo-request

2.5.6 Archivo de configuración /etc/shorewall/masq

Este archivo es usado para definir como se realizará el enmascaramiento o NAT(network address translation).

#INTERFACE	SUBNET	ADDRESS	PROTO
eth1	eth0		

Con esta configuración estamos haciendo NAT hacia la red interna.

2.5.7 Archivo de configuración /etc/shorewall/routestopped

Este archivo se usa para definir aquellas máquinas que pueden acceder al firewall cuando Shorewall esté detenido o cuando esta siendo [re]iniciado.

#INTERFACE	HOST(S)
eth0	10.0.0.9
eth1	192.168.0.2

[5]Eastep, Tomas. www.shorewall.net 2001-2005 Tomas M. Eastep [citado: 2006-08-09]. Disponible en World Wide Web: www.shorewall.net

De esta forma indicamos que los hosts con las direcciones 10.0.0.9 y 192.168.0.2 podrán acceder al firewall cuando este detenido.

2.6 Comandos de Shorewall

Para iniciar shorewall:	shorewall start
Para reiniciar shorewall:	shorewall restart
Para detener shorewall:	shorewall stop
Para limpiar iptables shorewall:	shorewall clear
Para mostrar las reglas en cada cadena:	shorewall show <cadena>
Para mostrar los últimos mensajes de LOG:	shorewall show log
Para mostrar reglas en la tabla nat:	shorewall show nat

Para probar una nueva configuración de shorewall se puede copiar la carpeta /etc/shorewall con la nueva configuración en otro lugar y escribir el comando:

shorewall try <nombre directorio>

Si se esta usando una versión de Linux como Centos o Redhad, no se recomienda utilizar los comandos: *service shorewall start*, *restart y stop*, ya que shorewall no se ejecutará correctamente.

2.6 Alternativas a Shorewall

Existen varios programas para la configuración de firewalls bajo Linux a continuación listamos algunos de ellos.

"Firestarter - *http://www.fs-security.com/*

Es muy flexible y amigable. Permite definir un firewall bastante sofisticado de una manera muy simple.

Herramienta gráfica de configuración y MONITOREO de Netfilter.

Firewall Builder *-* *http://www.fwbuilder.org/*

Herramienta gráfica de configuración de Netfilter. Permite describir firewalls complicados a la vez que permite al usuario promedio una seguridad aceptable con muy pocos conocimientos de Netfilter. No es tan flexible como Shorewall y requiere X-Window (y Qt?).

Arno's IPTABLESFirewall Script *-* *http://rocky.eld.leidenuniv.nl/*

Script BASH de configuración de Netfilter. Solo es necesario configurar unas pocas variables para obtener un firewall aceptable. Orientado a topologías de red tradicionales. Posee detección de escaneo de puertos.

Webmin *-* *http://www.webmin.com/*

*La herramienta de administración de computadoras con sistemas operativos *NIX Webmin posee un modulo de administración de Netfilter bastante completa. Es conveniente para administración remota del firewall. También posee un modulo de administración de Shorewall.*

FireHOL *-* *http://firehol.sourceforge.net/*

Herramienta similar de Shorewall. El lenguaje de configuración es un tanto más abstracto que el de Shorewall, pero parece ser igual de flexible."[6]

[6] www.gerulic.org.ar. 2005. [citado 2006-08-15]. Disponible en World Wide Web: www.gerulic.org.ar

2.7 Ventajas y desventajas de trabajar con Shorewall

2.7.1 Ventajas

- Existe una gran variedad documentación
- Ampliamente difundido
- Fácil de instalar y configurar
- Implementación rápida y sencilla
- Software gratuito y fácil de encontrar
- Esta en constante desarrollo
- flexible
- Incluido en casi todas las distribuciones principales

2.7.2 Desventajas

- Poco amigable ya que no contiene modo gráfico
- La mayoría de documentación esta en Ingles
- Debido a la gran cantidad de información es complicado encontrar aspectos Puntuales

2.8 Conclusiones

Después de instalar, y analizar las distintas configuraciones de Shorewall, hemos podido observar que es una herramienta muy práctica, la misma que facilita de gran manera la configuración y puesta en marcha de un firewall. Como aspecto negativo podemos mencionar la falta de una herramienta gráfica para la administración del mismo. La configuración mediante el editor es poco amigable.

Shorewall es de gran ayuda y resulta más fácil de configurar que el tradicional Iptables, sin ninguna duda lo recomendaríamos para el uso en cualquier red.

CAPÍTULO III

IMPLEMENTACION Y PRUEBAS DEL FIREWALL

3 Implementación y pruebas del firewall

3.1 Introducción a Implementación y pruebas del firewall

En este capítulo mostraremos el diseño de nuestra red como también las configuraciones del software shorewall usadas. Para esto se brinda al lector configuraciones sencillas y pruebas simples del funcionamiento de Shorewall.

3.2 Diseño de la red

La red utilizada para el ejemplo consta de un computador con 2 tarjetas de red donde instalaremos el firewall, el mismo tendrá la siguiente configuración:
Eth0: 10.0.0.1/24
Eth1:192.168.0.1/24

También utilizaremos 3 computadores con las siguientes direcciones IP:

Computador 1:10.0.0.9/24 (Linux)
Computador 2:192.168.0.2/24 (Windows)
Computador 3:192.168.0.4 /24 (Linux)
El esquema de la red quedaría como se muestra en el gráfico siguiente:

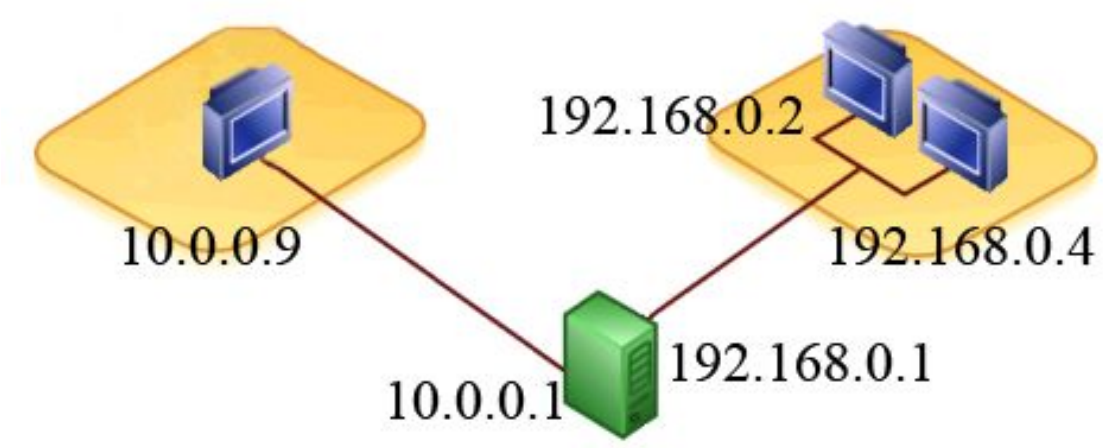

Figura 6.

3.3 Implementación del firewall mediante Shorewall

En el capítulo anterior pudimos observar una gran variedad de configuraciones y parámetros que se pueden cambiar en shorewall, la configuración que nosotros aplicamos para nuestro firewall fue la siguiente:

Para habilitar el enmascaramiento y entre las interfaces eth0 y eth1

Archivo **masq:**	#INTERFACE	SUBNET
	eth0	eth1

Para definir cuales serán nuestras zones IP versión 4 y zona firewall

Archivo **zones:**	#ZONE	TYPE
	fw	firewall
	net	ipv4
	loc	ipv4

Con esto especificamos a que interfaz pertenece cada zona, el parámetro detect para calcular la dirección broadcast automáticamente es utilizado

Archivo **interfaces:**	#ZONE	INTERFACE	
BROADCAST			
	loc	eth0	detect
	net	eth1	detect

Así indicamos que máquinas podrán comunicarse cuando Shorewall este detenido

Archivo **routestopped:**	#INTERFACE	HOST(S)
	eth0	10.0.0.9
	eth1	192.168.0.2
	eth1	192.168.0.4

Aquí definimos las políticas básicas para el tráfico.

Archivo **policy:**	#SOURCE	DEST	POLICY
	fw	net	ACCEPT
	net	fw	DROP
	loc	net	DROP
	net	loc	DROP
	all	all	REJECT

El significado de las políticas es el siguiente:

Se acepta el tráfico desde el firewall hacia la red net
Se ignora el tráfico desde la red net hacia el firewall
Se ignora el tráfico desde la red loc hacia la red net
Se ignora el tráfico desde la red net hacia la red loc
Se rechaza todo el resto del tráfico

Hay que tomar en cuenta que el orden de las reglas en este archivo es importante.
En el archivo rules se definen todas las excepciones a estas reglas.

Para agregar shorewall a los niveles de ejecución 3 y 5 que son modo multiusuario con soporte de red y operación gráfica respectivamente escribimos lo siguiente en la ventana de comandos:

```
chkconfig –level 35 shorewall on
```

Con esto conseguimos que Shorewall se inicie al arrancar el sistema operativo, por su puesto sin olvidar el setear en “Yes” el parámetro STARTUP_ENABLED del archivo shorewall.conf para que surta efecto.

Después de todas estas configuraciones escribiremos en la ventana de comandos la siguiente línea para iniciar shorewall.

```
shorewall  start
```

Con nuestro firewall ya configurado pasaremos a realizar las pruebas y configurar el archivo /etc/shorewall/rules.
Para reiniciar el firewall después de cualquier configuración podemos escribir:

```
shorewall restart
```

3.4 Pruebas

Todas las pruebas son realizadas sobre el archivo /etc/shorewall/rules, después de haber definido las políticas en el archivo /etc/shorewall/policy.

Prueba 1.

En el siguiente ejemplo se aceptará el pedido de conexión TCP desde la zona net hacia la zona loc para el puerto 80 (http). Ej.

```
#ACTION     SOURCE      DEST        PROTO       DEST
#                                               PORT
#SELECTION ESBLISHED
#SELECTION RELATED
SELECTION NEW
ACCEPT      net         loc         tcp         80
```

Prueba 2.

Ahora bien si lo que se desea es conceder el pedido de un solo host y no de toda una zona se deberá especificar la dirección IP. Ej.

```
#ACTION     SOURCE      DEST        PROTO       DEST
#                                               PORT
#SELECTION ESBLISHED
#SELECTION RELATED
```

```
SELECTION NEW
ACCEPT      net:192.168.0.4 loc          tcp          80
```

Prueba 3.

Si lo que se desea es permitir a todas las máquinas menos una se debería escribir el signo "!" después de los dos puntos, seguido de la dirección de la máquina que no será aceptada. Ej.

```
#ACTION     SOURCE      DEST        PROTO       DEST
#                                               PORT
#SELECTION ESBLISHED
#SELECTION RELATED
SELECTION NEW
ACCEPT      net:!192.168.0.4 loc     tcp         80
```

Prueba 4.

En el siguiente ejemplo permitiremos hacer ping desde la red local hacia la zona net

```
#ACTION     SOURCE      DEST        PROTO       DEST
#                                               PORT
#SELECTION ESBLISHED
#SELECTION RELATED
SELECTION NEW
ACCEPT      loc:10.0.0.0/24 net      icmp        echo-request
```

Prueba 5.

Si deseamos reenviar todas las peticiones de http que la zona net hace a la dirección 192.168.0.1 hacia la dirección 10.0.0.9 deberíamos hacer lo siguiente.

```
#ACTION     SOURCE      DEST        PROTO       DEST        ORIGEN
#                                               PORT        DEST
#SELECTION ESBLISHED
#SELECTION RELATED
SELECTION NEW
DNAT        net         loc:10.0.0.9 tcp        80          192.168.0.1
```

Esto sería útil en el supuesto caso de que el servidor Web de una empresa este en una máquina de la subred con una dirección privada.

Prueba 6

Si deseamos reenviar todas las peticiones de ftp que la zona net hace a la dirección 192.168.0.1 hacia la dirección 10.0.0.9 deberíamos hacer lo siguiente.

```
#ACTION     SOURCE      DEST          PROTO      DEST        ORIGEN
#                                                PORT        DEST
#SELECTION ESBLISHED
#SELECTION RELATED
SELECTION NEW
DNAT        net         loc:10.0.0.9  tcp        20,21       192.168.0.1
```

Esto sería útil en el supuesto caso de que se tenga un servidor ftp en una máquina de la subred con una dirección privada.

Prueba 7

Ahora bien si lo que deseamos es redireccionar los pedidos de conexión de correo electrónico, en el supuesto caso de que tengamos un servidor de SMTP e IMAP haremos lo siguiente.

```
#ACTION     SOURCE      DEST          PROTO      DEST        ORIGEN
#                                                PORT        DEST
#SELECTION ESBLISHED
#SELECTION RELATED
SELECTION NEW
DNAT        net         loc:10.0.0.9  tcp        53,25,143,80  192.168.0.1
DNAT        net         loc:10.0.0.9  udp        53            192.168.0.1
```

El puerto 53 en tcp y udp corresponde a DNS, el 25 a IMAP, el 143 a SMTP y 80 a http.

3.5 Conclusiones

Como pudimos ver en este capítulo shorewall es un software muy flexible y fácil de configurar, la gran variedad de opciones lo convierte en una herramienta muy poderosa. Hemos observado que shorewall nos puede ayudar a ahorrar mucho tiempo al momento de configurar un firewall, y puesto que es un software que esta en constante desarrollo sabemos que tendremos una gran variedad de literatura a manera de soporte.

4 Conclusiones

Los firewalls como lo hemos mencionado han llegado a ser prácticamente indispensables para cualquier empresa que posea una red, nos ayudan de gran manera a que la misma funcione de una forma más eficiente y segura.

Como todos sabemos la tarea de manejar un firewall puede ser muy complicada, pero gracias a la ayuda de algunas herramientas en este caso Shorewall hemos podido comprender las distintas configuraciones de una manera sencilla y práctica. Podemos decir que Shorewall es de gran utilidad para cualquier administrador, el mismo que gracias a su constante desarrollo y flexibilidad nos permitirá controlar de manera efectiva nuestra red; nos dimos cuenta que tanto en las configuraciones básicas como avanzadas shorewall presento muchas opciones sin dejar de lado su sencillez, al mismo que solo le falto una utilidad gráfica para ser un software completo.

5 Bibliografía:

1. http://www.linuxparatodos.net/. Barrios, Joel Como configurar un muro cortafuegos con Shorewall [en línea], Joel Barrios Dueñas, 99-2006, Disponible en World Wide Web: http://www.linuxparatodos.net.

2. Barto, Agustín. http://www.gerulic.org.ar. 2005. Agustín Barto. [citado 2006-08-15]. Disponible en World Wide Web: http://www.gerulic.org.ar.

3. Eastep, Tomas. http://www.shorewall.net 2001-2005 Tomas M. Eastep [citado: 2006-08-09]. Disponible en World Wide Web: http://www.shorewall.net

4. M.C. Ibarra, Francisco. Firewalls en Linux .Instituto Tecnológico Hermosillo. Francisco Ibarra Lemas. 7 de Junio del 2006 [citado 2006-09-15].

5. Arena, Facundo. Linux a fondo. Primera edición. Facundo Arena Héctor. 2004.

6. http://www.wikipedia.org. Cortafuegos. [en línea]. 2005. [citado 2006]. Disponible en World Wide Web: http://www.wikipedia.org.

7. Elorreaga, Daniel. Firewalls y seguridad en Internet. Universidad nacional autónoma de México. Daniel Ramón Elorreaga Daniel. 1997. Disponible en World Wide Web: http://monografias.com.

8. Semeria, Chuck. Firewalls and Internet Security. 3Com Corp. Chuck Semeria. 1997. Disponible en World Wide Web: http://www.3com.com/nsc/500619.html.

9. http://www.ibiblio.org. Configuración de Linux con Cortafuegos. 2005. Disponible en World Wide Web: http://www.ibiblio.org.

10. Stallings, William. Comunicaciones y redes de computadores. Séptima Edición. William Stallings. 2004. ISBN: 84-2005-4110-9.

6 Glosario:

Params
Usted puede usar el archivo /etc/shorewall/params para definir variables shell que puede usar luego en cualquier parte de los archivos de configuración Shorewall. Se sugiere que los nombres de variables comiencen con una letra mayúscula para distinguirla de las variables usadas internamente por el programa Shorewall

blacklist
Una lista de parámetros instalados en /etc/shorewall que se usa para bloquear las direcciones IP/subredes/MAC listadas.

ecn
Un archivo de parámetros instalado en /etc/shorewall y que se usa para selectivamente deshabilitar la Explicit Congestion Notification (ECN - RFC 3168).

functions
Un conjunto de funciones shell usadas por los programas shell firewall y shorewall. Instalado en /usr/share/shorewall.

modules
Un archivo de parámetros instalado en /etc/shorewall y que especifica módulos kernel y sus parámetros. Shorewall automáticamente cargará los módulos especificados en este archivo.

tos
Un archivo de parámetros instalado en /etc/shorewall que se usa para especificar cómo debe ajustarse el campo Type of Service (TOS) en los paquetes.

init.sh and init.debian.sh
Un guión de shell instalado en /etc/init.d que automáticamente arranca Shorewall al arrancar el sistema (boot). Este guión particular depende de qué distribución use.

hosts
Un archivo de parámetros instalado en /etc/shorewall y que se usa para describir máquinas individuales o subredes en zonas.

maclist
Un archivo de parámetros instalado en /etc/shorewall que se usa para verificar la dirección MAC (y posiblemente también la dirección IP) de los dispositivos.

firewall
Un programa shell que lee los archivos de configuración en /etc/shorewall y configura su firewall. Este archivo está instalado en /usr/share/shorewall.

nat
Un archivo de parámetros en /etc/shorewall que se usa para definir NAT uno-a-uno.

proxyarp
Un archivo de parámetros en /etc/shorewall que se usa para definir el Proxy Arp.

rfc1918
Un archivo de parámetros en /usr/share/shorewall que se usa para definir cómo se tratan los paquetes bajo la opción de interface norfc1918.

tcrules
Un archivo de parámetros en /etc/shorewall que se usa para definir las reglas de clasificación de paquetes para el Control de Tráfico/Modelado.

tcdevices
Un archivo de parámetros en /etc/shorewall que se usa para definir el ancho de banda de las interfaces sobre las cuáles desea habilitar el modelado de tráfico.

tcclasses
Un archivo de parámetros en /etc/shorewall que se usa para definir clases para el modelado de tráfico.

tcstart
un conjunto de funciones shell que se usan en Shorewall para configurar el modelado de tráfico. Este archivo está instalado en /usr/share/shorewall.

tunnels
Un archivo de parámetros en /etc/shorewall que se usa para definir túneles IPSec.

shorewall
Un programa shell (requiere Bourne shell o derivativo) que se usa para controlar y monitorear el firewall. Este debe estar ubicado en /sbin o en /usr/sbin (el guión install.sh script y el paquete rpm instala este archivo en /sbin).

accounting
Un archivo de parámetros en /etc/shorewall que se usa para definir reglas de contabilidad de tráfico.

version
Un archivo creado en /usr/share/shorewall que describe la versión instalada de Shorewall en su sistema.

actions y action.template
Archivos en /etc/shorewall y /usr/share/shorewall respectivamente que permiten definir sus propias acciones para las reglas en /etc/shorewall/rules.

actions.std y action.*
Archivos en /usr/share/shorewall que definen las acciones incluidas como parte estandar de Shorewall.

providers

Archivo de /etc/shorewall que se usa para definir múltiples Internet Service Providers y balanceo de carga.

routes

Archivo en /etc/shorewall que se usa para hablar con el destino experimental ROUTE de Netfilter patch-o-matic-ng.

Dhcp

Protocolo para el asignamiento dinámico de direcciones IP