Introducción a Shorewall

Agustín Bartó (m4rgin4l)

Grupo de Usuarios de Software Libre de Córdoba - GrULiC

Tabla de contenidos

Requisitos....2
Breve repaso de Netfilter....2
Como pasan los paquetes por los filtros....2
Uso de iptables....4
Operaciones sobre una sola regla....4
Introducción a Shorewall....6
¿Qué es Shorewall?....6
Características y funcionalidades de Shorewall....6
¿Cuándo conviene utilizar Shorewall?....8
Conceptos principales....8
Zonas (zones)....8
Interfaces (interfaces)....9
Hosts (hosts)....12
Políticas (policy)....13
Reglas (rules)....14
Macros (macros)....18
Masquerading (masq)....20
shorewall.conf....21
Operación....21
Otros conceptos....22
Compilación de configuración....23
Redes privadas virtuales (VPNs)....23
Control de tráfico y congestión con Shorewall y tc....23
shorewall-shell, shorewall-lite, shorewall-perl....24
Ejemplos....25
Configuración básica con masquerading....25
Configuración básica multi-zona....30
Redirección de puertos....34
Para P2P....35
Para servidores internos....36
Proxy transparente....36
Firewall con zona desmilitarizada (DMZ)....37
Conclusiones....41
Agradecimientos....42

Requisitos

Para que puedas entender la mayor parte de los conceptos que se discuten en este documento, es necesario que tengas nociones elementales del funcionamiento de una red TCP/IP (paquetes, DNS, ruteo, etc.) Un buen punto de partida para comenzar a aprender sobre estos temas es el documento "Network Concepts HOWTO", el cual se encuentra disponible en el sitio de Netfilter traducido a varios idiomas.

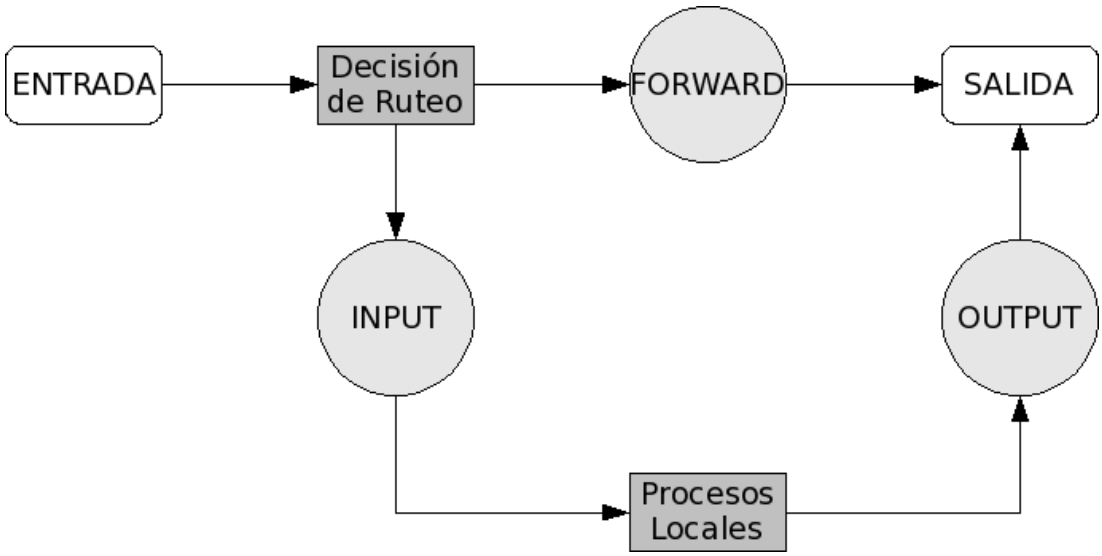
Breve repaso de Netfilter

Netfilter es la infraestructura de filtrado de paquetes de las versiones 2.4.x y 2.6.x del núcleo Linux. Habitualmente, el común de la gente se refiere a este conjunto de estructuras de datos, llamadas de sistema y herramientas de usuario como iptables, lo cual sería equivalente a llamar ls al subsistema de administración de sistemas de archivos. En realidad, iptables es una herramienta de modo de usuario para alterar la configuración interna de las estructuras de Netfilter, afectando así la manera en la que son tratados los paquetes de red al momento de entrar y salir del sub-sistema de red del núcleo Linux.

Para entender una herramienta como Shorewall es necesario conocer cómo se filtran los paquetes dentro del núcleo, y como se utiliza iptables para configurar este procedimiento. Una vez que entendamos esto, la utilidad de una herramienta como Shorewall debería ser evidente para la mayoría de los usuarios. La mayor parte de esta sección fue extraída del documento "Linux 2.4 Packet Filtering HOWTO", el cual puede obtenerse traducido a múltiples idiomas desde el sitio de Netfilter.

Como pasan los paquetes por los filtros

El núcleo empieza con tres listas de reglas en la tabla *filter* (hay otras tablas que agrupan cadenas específicas); estas listas se llaman cadenas cortafuegos o sencillamente cadenas. Se llaman **INPUT**, **OUTPUT** y **FORWARD**.



Estos tres círculos representan las tres cadenas que mencioné antes. Cuando un paquete alcanza un círculo en el diagrama, se examina esa cadena para decidir la suerte del paquete. Si la cadena dice que hay que descartar (**DROP**) el paquete, se le mata ahí mismo, pero si la cadena dice que hay aceptarlo (**ACCEPT**), continúa su camino por el diagrama.

Una cadena es una lista de reglas. Cada regla dice “si el paquete se parece a esto, entonces esto otro es lo que hay que hacer con él”. Si la regla no se ajusta al paquete, entonces se consulta la siguiente regla en la lista. Al final, si no hay más reglas por consultar, el núcleo mira la política de la cadena para decidir qué hacer. En un sistema consciente de la seguridad, esta política suele decirle al núcleo que descarte (DROP) el paquete.

1. Cuando llega un paquete (digamos, por la tarjeta Ethernet) el núcleo mira primero su destino: a esto se le llama ruteo o enrutamiento (routing).

2. Si está destinado a esa misma máquina, el paquete entra en el diagrama hacia la cadena INPUT. Si pasa de aquí, cualquier proceso que esté esperando por el paquete, lo recibirá.

3. En caso contrario, si el núcleo no tiene las capacidades de reenvío activadas, o no sabe hacia dónde reenviar el paquete, se descarta el paquete. Si está activado el reenvío, y el paquete está destinado a otra interfaz de red (si tenemos otra), entonces el paquete pasa directamente a la cadena FORWARD de nuestro diagrama. Si es ACCEPTado, entonces saldrá de la máquina.

4. Finalmente, si un programa que se ejecuta en la máquina puede enviar paquetes de red. Estos paquetes pasan por la cadena OUTPUT de forma inmediata: si los acepta (ACCEPT), entonces el paquete continúa hacia

afuera, dirigido a la interfaz a la que estuviera destinada.

Uso de iptables

Iptables dispone de una página de manual bastante detallada (man iptables), por si necesita más detalles particulares. Aquellos de ustedes que estén familiarizados con ipchains, posiblemente quieran echar un vistazo a Diferencias entre iptables e ipchains; son bastante similares.

Con iptables se pueden hacer muchas cosas diferentes. Empezamos con tres cadenas de uso interno: INPUT, OUTPUT y FORWARD, que no se pueden borrar. Veamos las operaciones que se pueden hacer en todas las cadenas:

1. Crear una nueva cadena (-N).
2. Borrar una cadena vacía (-X).
3. Cambiar la política de una cadena de uso interno (-P).
4. Listar las reglas de una cadena (-L).
5. Vaciar de reglas una cadena (-F).
6. Poner a cero los contadores de paquetes y bytes de todas las reglas de una cadena (-Z).

Las reglas de una cadena se pueden manipular de varias maneras:

1. Añadir una nueva regla a una cadena (-A).
2. Insertar una nueva regla en alguna posición de la cadena (-I).
3. Mover una regla a otra posición dentro de una cadena (-R).
4. Borrar una regla de un sitio en particular de una cadena (-D).
5. Borrar la primera regla que coincida con los parámetros dados en una cadena (-D).

Operaciones sobre una sola regla

Este es el pan de cada día del filtrado de paquetes: la manipulación de reglas. Lo más común es que utilice las órdenes de agregar (-A) y eliminar (-D). Las otras (-I para insertar y -R para cambiar de sitio) son sólo extensiones de estos conceptos.

Cada regla especifica un conjunto de condiciones que debe cumplir el paquete, y qué hacer si se ajusta a ellas (un “objetivo”). Por ejemplo, podríamos querer descartar todos los paquetes ICMP que viniesen de la dirección IP 127.0.0.1. De manera que en este caso nuestras condiciones son que el protocolo sea ICMP y que la dirección de origen del paquete sea 127.0.0.1. Nuestro objetivo será “DROP”.

127.0.0.1 es la interfaz “loopback”, de la que dispondrá incluso si no tiene una conexión de red real. Puede usar el programa “ping” para generar tales paquetes (sencillamente envía paquetes ICMP de tipo 8 (echo request) que todos las máquinas cooperantes deberían responder cortésmente con un paquete ICMP de tipo 0 (echo reply)). Esto lo hace útil para las pruebas.

```
# ping -c 1 127.0.0.1
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.2 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.2 ms
# iptables -A INPUT -s 127.0.0.1 -p icmp -j DROP
# ping -c 1 127.0.0.1
PING 127.0.0.1 (127.0.0.1): 56 data bytes

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 0 packets received, 100% packet loss
```

Aquí puede ver que el primer “ping” tuvo éxito (el “-c 1” le indica a ping que sólo envíe un paquete).

Entonces añadimos (-A) a la cadena “INPUT”, una regla que especifica que los paquetes que vengan de 127.0.0.1 (“-s 127.0.0.1”) con protocolo ICMP (“-p icmp”) deberíamos saltar a DROP (“-j DROP”).

Luego probamos nuestra regla, usando el segundo ping. Habrá una pausa antes de que el programa se canse de esperar por una respuesta que nunca llegará.

Podemos borrar la regla de dos maneras. Primero, como sabemos que es la única regla en la cadena, podemos usar un borrado por número:

```
# iptables -D INPUT 1
```

Para borrar la regla número uno de la cadena INPUT.

La segunda manera es repetir la orden -A, pero cambiando -A por -D. Es útil cuando se tiene una compleja cadena de reglas y no queremos estar contándolas para averiguar que es la regla 37 la que queremos eliminar. En

este caso, usaríamos:

```
# iptables -D INPUT -s 127.0.0.1 -p icmp -j DROP
```

La sintaxis de -D debe tener exactamente las mismas opciones que la orden -A (o -I, o -R). Si hay varias reglas idénticas en la misma cadena, sólo se borrará la primera.

Introducción a Shorewall

¿Qué es Shorewall?

Shorewall es un lenguaje de alto nivel de propósito específico para manipular la infraestructura de control de paquetes del núcleo Linux, Netfilter.

Más específicamente, Shorewall es un *script* en lenguaje BASH (o en Perl en caso que deseemos utilizar shorewall-perl) que interpreta una serie de archivos de configuración a partir de los cuales hace sucesivas llamadas a iptables para definir el conjunto de reglas necesarias representadas por la configuración. Además de iptables, Shorewall también utiliza otras herramientas para controlar otros módulos de red núcleo Linux como modprobe (para cargar los módulos de Netfilter), iproute (para la definición de reglas de ruteo) y tc (para el control de tráfico de paquetes).

Características y funcionalidades de Shorewall[1]

- Permite el filtrado de paquetes *stateful* gracias a las capacidades de monitoreo de conexiones de Netfilter.
    - Puede utilizarse en múltiples aplicaciones de *router* (enrutador), *firewall* (corta-fuegos) o *gateway* (pasarela).
    - Completamente configurable mediante el uso de archivos de configuración.
    - Número de interfaces de red ilimitadas.
    - Permite dividir las redes en zonas, permitiendo extenso control sobre las conexiones establecidas entre ellas.
    - Múltiples interfaces por zona y múltiples zonas por interfaz.
    - Soporta zonas anidadas y solapadas.

1 Traducido de http://www.shorewall.net/shorewall_features.htm.

- Guías para ayudarnos a configurar *firewalls* rápidamente.
- Interfaz gráfica de configuración provista por Webmin 1.060 y versiones posteriores (http://www.webmin.com)
- Extensa documentación disponible en múltiples formatos.
- Administración de direccionamiento y ruteo flexibles (pudiendo combinar cada técnica en un único firewall):
  - Masquerading/SNAT.
  - Port Forwarding (DNAT).
  - NAT Uno-A-Uno.
  - Proxy ARP.
  - NETMAP.
  - Soporte para múltiples proveedores de Internet.
- Soporte para listas negras de sub-redes y direcciones IP individuales.
- Soporte operacional.
  - Comandos para iniciar, detener y limpiar el firewall.
  - Soporta monitoreo de estado con alarmas sonoras ante la detección de actividad de red particular.
  - Gran cantidad de comandos de información.
- Soporte de VPNs.
  - IPSEC, GRE, IPIP y túneles OpenVPN.
  - Clientes y servidores PPTP.
- Soporte para control de tráfico y congestión.
- Soporte para múltiples distribuciones de GNU/Linux.
  - Paquetes en formato RPM y Debian disponibles.
  - Provee scripts de instalación y actualización automáticos para los

usuarios que no pueden o no desean utilizar los paquetes RPM o Debian.

  - Incluido en la mini-distribución LEAF/Bering.

- Verificación de direcciones MAC (Media Access Control).
- Auditoria de tráfico.
- Soporte de *bridging*.

¿Cuándo conviene utilizar Shorewall?

A juzgar por la sección anterior, debería ser bastante claro que Shorewall es un firewall extremadamente flexible y configurable. Hasta ahora no he encontrado ninguna situación en donde Shorewall no pudiera adecuarse de manera fácil y rápida.

A pesar de esto, creo que Shorewall puede ser demasiado cuando uno solo quiere asegurar una estación de trabajo conectada a Internet. En estos casos yo generalmente recomiendo FirewallBuilder, FireStarter o herramientas similares (o las herramientas provistas por la distro como system-config-firewall de Fedora).

Shorewall realmente se destaca cuando queremos conectar dos zonas (una red hogareña contra la Internet) o más, siendo cada vez más conveniente a medida que la situación se torna cada vez más sofisticada, por ejemplo, conectar múltiples ISP con control de tráfico, DMZ y zonas internas distinguidas.

Ahora bien, habiendo tantas herramientas de gestión de firewalls disponibles, ¿Cuándo conviene construir un firewall utilizando iptables desde shell scripts?. La respuesta, yo creo, es bastante sencilla: Cuando queremos aprender el funcionamiento interno de Netfilter. Una vez que uno domina esta técnica es cuando realmente puede apreciar una herramienta como Shorewall.

Conceptos principales

Zonas (zones)

Una **zona** es una porción de una sub-red susceptible de generar o consumir paquetes de red. Este concepto engloba sub-redes completas, partes de ellas, hosts aislados e inclusive firewall mismo se considera una zona.

En Shorewall, las zonas se *declaran* utilizando el archivo `/etc/shorewall/zones`. El siguiente recuadro muestra un ejemplo de un

archivo zones.

```
#
# Shorewall version 4 - Zones File
#
# For information about this file, type "man shorewall-zones"
#
# For more information, see http://www.shorewall.net/Documentation.htm#Zones
#
###############################################################################
#ZONE   TYPE            OPTIONS         IN                      OUT
#                                       OPTIONS                 OPTIONS
fw firewall
loc ipv4
net ipv4
#LAST LINE - ADD YOUR ENTRIES ABOVE THIS ONE - DO NOT REMOVE
```

Este archivo *declara* tres zonas: fw, correspondiente al firewall mismo y loc y net correspondiente a zonas que utilizan ipv4.

Notar que en los párrafos anteriores destaqué la palabra "*declara*". La intención de esto es indicar la funcionalidad específica del archivo zones. Similar a lo que sucede con los lenguajes fuertemente tipados como Java o C, en Shorewall las zonas se *declaran* (se nominan y se describe cierto comportamiento específico que puede llegar a tener la zona) en el archivo zones, y se *definen* (se asocia el identificador de zona a un conjunto de hosts específico) en el archivo *interfaces*, o en el archivo *hosts*.

Como lo indica la cabecera del archivo (por defecto, todos los archivos de configuración de Shorewall tienen una cabecera que explica el formato), luego del nombre de la zona (que puede ser cualquier identificador válido), vienen el tipo, las opciones genéricas, las opciones de entrada y las opciones de salida.

Para conocer más acerca de las zonas, se puede leer el documento correspondiente en la referencia de Shorewall (también disponible como man-page): http://www.shorewall.net/manpages/shorewall-zones.html.

Interfaces (interfaces)

Las interfaces son las que establecen las conexiones (lógicas) entre las zonas. Una zona puede estar conectada a una o múltiples interfaces y una interfaz puede estar conectada a una o muchas zonas. En mi opinión, en la facilidad de combinar estos dos conceptos radica una de las principales fortalezas de Shorewall, permitiendo definir topologías extremadamente complicadas con dos o tres sentencias de configuración.

Shorewall solo permite definir interfaces reales y virtuales (éstas últimas con

ciertas limitaciones), y utilizar comodines en la definición cuando no es posible conocer el nombre de una interfaz al momento de la ejecución del firewall. Además en el archivo zones es posible asociar una zona a una interfaz, lo cual indica que todo el trafico que se origina o es destinado hacia una interfaz es considerado de la zona asociada. Esta es una de las formas de *definir* los integrantes de una zona.

Veamos un ejemplo:

```
#
# Shorewall version 4 - Interfaces File
#
# For information about entries in this file, type "man shorewall-interfaces"
#
# For additional information, see
# http://shorewall.net/Documentation.htm#Interfaces
#
###############################################################################
#ZONE   INTERFACE       BROADCAST       OPTIONS
loc  eth0 detect dhcp
net  ppp+ -      dhcp,norfc1918,nosmurfs,tcpflags
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Este archivo define dos interfaces: `eth0` y `ppp+` (lo cual se convertirá en ppp0, ppp1, ..., etc. según sea el caso cuando el firewall sea iniciado), cada una asociada a las zonas `loc` y `net` respectivamente, se indica que en la primera interfaz se debe detectar la dirección de broadcast y en la segunda que se debe ignorar (por tratarse de una interfaz punto-a-punto) y por último, en la sección de opciones se declaran ciertas condiciones que debe cumplir el tráfico que pasa por la interfaz. La siguiente tabla explica alguna de las opciones más importantes:

Nombre	Descripción
blacklist	Verificar paquetes entrantes por la interfaz contra la lista negra definida en /etc/shorewall/blacklist.
dchp	Esta opción se utiliza cuando: • La interfaz obtiene su dirección vía DHCP, • cuando la interfaz es utilizada por un servidor DHCP en el mismo firewall, • la interfaz tiene una dirección estática, pero la misma está en un segmento de LAN con muchos clientes DHCP,

	• la interfaz es parte de un bridge, con un servidor DHCP en un puerto y los clientes en otro.
logmartians	Habilitar el loggeo de paquetes marcianos (paquetes con direcciones de origen imposibles de acuerdo a la topología) del núcleo.
maclist	Verificar paquetes entrantes por la interfaz contra la lista definida en /etc/shorewall/maclist.
norfc1918	Indica que la interfaz no debe recibir paquetes con direcciones no-enunciables como las definidas en el RFC 1918 (http://www.faqs.org/rfcs/rfc1918.html).
nosmurfs	Filtrar paquetes “pitufos” (con una dirección broadcast como origen).
routeback	Indica que Shorewall debe incluir reglas para paquetes que ingresan y salen por la misma interfaz. Esta opción es requerida cuando se utilizan comodines que *matchean* múltiples interfaces y se desea filtrar trafico que fluye entre ellas.
tcpflags	Los paquetes que ingresan por esta interfaz se chequean para verificar la existencia de ciertos patrones de activación de banderas de TCP (como los “árboles de navidad”).
upnp	Los requerimientos entrantes por la interfaz pueden ser remapeados por UPNP.
...	Ver http://www.shorewall.net/manpages/shorewall-interfaces.html.

Como dije en un párrafo anterior, es posible que una interfaz esté conectada a múltiples zonas. En éste caso, en donde iría el nombre de la zona en la definición de interfaz se utiliza un guión (-),

```
-  eth0 detect dhcp
```

dejando la definición de la zona al archivo `/etc/shorewall/hosts`.

Para conocer más acerca de las interfaces, se puede leer el documento correspondiente en la referencia de Shorewall (también disponible como man-page): http://www.shorewall.net/manpages/shorewall-interfaces.html.

Hosts (hosts)

El archivo `/etc/shorewall/hosts` se utiliza para *definir* zonas en términos de sub-redes o *hosts* individuales. Para definir una zona en este archivo es necesario que la interfaz a la que pertenezcan los hosts no esté asociada a una zona particular en el archivo `interfaces`.

Supongamos que deseamos definir dos zonas `loc0`, y `loc1` correspondientes a dos sub-redes de direcciones 172.16.0.0/16 y 172.17.0.0/16 respectivamente. Supongamos además que el equipo posee dos interfaces `eth0`, y `eth1`, y que las zonas `loc0` y `loc1` estarán conectados a la interfaz eth0 y que la interfaz eth1 estará asociado a una zona `net`. Veamos primero el contenido del archivo interfaces:

```
#
# Shorewall version 4 - Interfaces File
#
# For information about entries in this file, type "man shorewall-interfaces"
#
# For additional information, see
# http://shorewall.net/Documentation.htm#Interfaces
#
###############################################################################
#ZONE   INTERFACE       BROADCAST       OPTIONS
-     eth0  detect      dhcp
net   eth1  detect      dhcp
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Esta definición nos permitirá asociar una o mas zonas a la interfaz `eth0` utilizando el archivo `hosts`:

```
#
# Shorewall version 4 - Hosts file
#
# For information about entries in this file, type "man shorewall-hosts"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-hosts.html
#
###############################################################################
#ZONE   HOST(S)                                  OPTIONS
loc0  eth0:172.16.0.0/16
loc1  eth0:172.17.0.0/16
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS LINE -- DO NOT REMOVE
```

Esta definición indica que las direcciones IP de la sub-red 172.16.0.0/16 conectada a la interfaz `eth0` pertenecerán a la zona `loc0` y las de la sub-red 172.17.0.0/16 conectada a la interfaz `eth0` pertenecerán a la zona `loc1`.

Para las opciones podemos utilizar casi las mismas que las utilizadas en el archivo `interfaces`.

Shorewall es extremadamente flexible a la hora de definir zonas de esta manera. No solamente podemos suministrar direcciones IP individuales (de hosts o sub-redes) sino que podemos utilizar rangos e inclusive conjuntos de IPs.

Una característica interesante de Shorewall es que es posible definir zonas solapadas. Cuando un IP puede pertenecer a más de una zona a la vez, **su pertenencia se decide de acuerdo al orden de la declaración de zonas en el archivo zones**.

Para conocer más acerca de este tema, se puede leer el documento correspondiente en la referencia de Shorewall (también disponible como man-page): http://www.shorewall.net/manpages/shorewall-hosts.html.

Políticas (policy)

Hasta el momento solo hemos hablado de como indicarle a Shorewall la topología (lógica) de la red que deseamos controlar y no hemos abordado la cuestión que define a todo firewall: los filtros.

Shorewall provee un lenguaje muy expresivo para definir y manipular filtros (como lo veremos en las siguientes dos secciones), pero antes de discutir este tema prefiero introducir las políticas, que son, de alguna manera, los filtros más genéricos que provee Shorewall.

Las políticas definen el comportamiento por defecto que debe cumplir Shorewall cuando ninguna de las reglas específicas (definidas en el archivo `/etc/shorewall/rules`) pueden aplicarse. Las definiciones de políticas en Shorewall se dan en términos de relaciones entre zonas y el objetivo (*target* de Netfilter) a cumplir por parte de ese tráfico. Veamos un ejemplo:

```
#
# Shorewall version 4 - Policy File
#
# For information about entries in this file, type "man shorewall-policy"
#
# See http://shorewall.net/Documentation.htm#Policy for additional information.
#
###############################################################################
#SOURCE         DEST            POLICY          LOG             LIMIT:BURST
#                                               LEVEL
fw    all   ACCEPT
loc   loc   ACCEPT
loc   net   ACCEPT
net   all   DROP        info
all   all   REJECT      info
```

```
#LAST LINE -- DO NOT REMOVE
```

En este ejemplo asumimos la existencia de tres zonas: `loc`, correspondiente a una red interna, `net` correspondiente a la Internet y, por supuesto, `fw` representando al firewall mismo y las políticas definidas son:

- Si el paquete sale desde el firewall y va hacia cualquier zona, aceptarlo (ACCEPT).
- Si el paquete viaja desde y hacia la zona loc (supongamos que loc esta asociada a dos interfaces internas), aceptarlo (ACCEPT).
- Si el paquete sale desde la zona loc (pasa por el firewall) y va hacia la zona net, aceptarlo (ACCEPT).
- Si desde la zona net se intenta iniciar una conexión a cualquier zona (loc, fw, o net), ignorarlo (DROP) y escribir una entrada en el log del núcleo. Este tipo de regla es muy importante cuando uno está conectado a la Internet dado que dificulta el escaneo de puertos.
- Para cualquier otra combinación de zonas, denegar explícitamente el acceso (REJECT) y escribir una entrada en el log del núcleo.

Además de la definición de reglas, este archivo también nos permite definir el nivel de log que queremos utilizar para la política y limitar las ráfagas de loggeo específicas (es posible definir globalmente estos valores en el archivo `/etc/shorewall/shorewall.conf`).

Para conocer más acerca de este tema, se puede leer el documento correspondiente en la referencia de Shorewall (también disponible como man-page): http://www.shorewall.net/manpages/shorewall-policies.html.

Reglas (rules)

Llegamos hasta el punto en donde veremos, a mi opinión la característica mas importante de cualquier herramienta de administración de firewalls: la definición de las reglas de filtrado.

En Shorewall, los filtros se rigen por el contenido del archivo `/etc/shorewall/rules` en un principio, y `/etc/shorewall/policy` como se expliqué en la sección anterior. Dado que el archivo `rules` es uno de los mas complicados (dada la flexibilidad) comencemos por analizar un archivo sin definición de reglas como el que se obtiene con la instalación por defecto:

```
#
# Shorewall version 4 - Rules File
```

```
#
# For information on the settings in this file, type "man shorewall-rules"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-rules.html
#
###############################################################################
#########################################
#ACTION         SOURCE          DEST            PROTO   DEST    SOURCE
ORIGINAL        RATE            USER/   MARK
#                                                       PORT    PORT(S)
DEST            LIMIT           GROUP
#SECTION ESTABLISHED
#SECTION RELATED
SECTION NEW
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Las reglas se agrupan en tres secciones (que deben incluirse en el orden en que se indica), dependiendo del estado de la conexión:

- SECTION ESTABLISHED: Correspondiente a reglas que se aplican a paquetes que pertenecen a conexiones establecidas.
- SECTION RELATED: Correspondiente a reglas que se aplican a paquetes que inician una nueva conexión relacionada a una establecida. El ejemplo canónico de esto es la apertura de la conexión de transferencia cuando la conexión de control ya esta establecida en el protocolo FTP.
- SECTION NEW: Correspondiente a reglas que se aplican a paquetes que inician una nueva conexión o a conexiones invalidas.

Luego dentro de cada sección se declara una regla por renglón la cual (como lo indica la cabecera) suministrando los siguientes valores en orden separados por espacios vacíos:

- Acción (ACTION): Indica la acción a seguir cuando una conexión *matchea* contra la regla especificada y permite indicar como *loggear* la conexión. Algunas posibles acciones son:
  - ACCEPT: Aceptar la conexión.
  - DROP: Ignorar la conexión:
  - REJECT: Rechazar explícitamente la conexión:
  - REDIRECT: Redirigir la conexión a otro host/puerto.
  - LOG: Loggear la conexión.

    - QUEUE: Encolar la conexión.

    - Macros: Reemplazar los parámetros en un macro predefinido (ver siguiente sección).

- Fuente (SOURCE): Fuente de los paquetes. Puede ser un identificador de zona, de interfaz, una dirección IP (incluidas las subredes), un rango o una lista de direcciones. Es posible por ejemplo, suministrar un nombre de zona y un conjunto específico de IPs para los cuales la regla aplica (dentro de dicha zona).

- Destino (DEST): Destino de los paquetes. La especificación es similar a la anterior.

- Protocolo (PROTO): Protocolo de la conexión, por ejemplo: tcp. (opcional)

- Puerto de destino (DEST PORT): Puerto de destino. Puede ser una lista o rango de nombres. Es posible utilizar identificadores de servicios. (opcional)

- Puertos de origen (SRC PORT(S)): Puertos de origen utilizados por el cliente. La especificación es similar a la anterior. (opcional)

- Destino original (ORIGINAL DEST): Si la acción es DNAT o REDIRECT y este campo es incluido y es diferente del IP dado en la columna SERVER (DEST), entonces las conexiones destinadas a esta dirección y puerto serán enviados al IP y puerto especificado en la columna DEST. (opcional)

- Límite de cadencia (RATE LIMIT): Permite limitar la cantidad de ocurrencias por segundo de la regla. En caso que se supere el limite establecido no es posible activar esta regla. (opcional)

- Usuario/Grupo (USER/GROUP): Identifica al ID del usuario y del grupo de un **programa corriendo en el firewall**. Solo puede aplicarse cuando la dirección de origen es el firewall mismo.

- Marca (MARK): Identifica la marca que debe poseer (o no si la regla está negada) el paquete para activar la regla.

Creo que la mejor manera de entender como funcionan las reglas es a través del uso de algunos ejemplos prácticos[2]:

1) Aceptar pedidos de conexiones SMTP desde la zona desmilitarizada (identificada por la zona `dmz`) hacia la Internet (identificada por la zona `net`)

2 La documentación de Shorewall siempre sigue la misma filosofía, siempre presentando ejemplos prácticos sencillos y artículos completos para describir alguna situación particular.

```
#ACTION SOURCE  DEST PROTO      DEST    SOURCE  ORIGINAL
#                              PORT    PORT(S) DEST
ACCEPT  dmz     net       tcp  smtp
```

2) Reenviar todos los pedidos de conexiones SSH y HTTP desde la Internet (al firewall) a un host particular dentro de la zona `loc`.

```
#ACTION SOURCE  DEST            PROTO   DEST    SOURCE  ORIGINAL
#                                       PORT    PORT(S) DEST
DNAT    net     loc:192.168.1.3 tcp     ssh,http
```

3) Reenviar todos los pedidos de conexión HTTP desde la Internet al sistema local 192.168.1.3 con un límite de 3 conexiones por segundo y una ráfaga máxima de 10.

```
#ACTION SOURCE DEST            PROTO  DEST  SOURCE  ORIGINAL RATE
#                                     PORT  PORT(S) DEST     LIMIT
DNAT    net    loc:192.168.1.3 tcp    http  -       -        3/sec:10
```

4) Redirigir todo las conexiones web originadas localmente al puerto 3128 en el firewall (suponemos que hay un proxy HTTP corriendo en el firewall en el puerto 312), salvo por las que están destinadas a la dirección 192.168.2.2.

```
#ACTION  SOURCE DEST      PROTO DEST    SOURCE  ORIGINAL
#                                PORT    PORT(S) DEST
REDIRECT loc    3128      tcp   www      -      !192.168.2.2
```

5) Reenviar todos los pedidos a la dirección 130.252.100.69 desde la Internet, a la dirección 192.168.1.3.

```
#ACTION  SOURCE DEST            PROTO   DEST    SOURCE  ORIGINAL
#                                       PORT    PORT(S) DEST
DNAT      net   loc:192.168.1.3 tcp     80      -       130.252.100.69
```

6) Aceptar todas las conexiones SSH al firewall desde la Internet, solo si provienen desde las direcciones 130.252.100.69 y 130.252.100.70. (Notar el uso del caracter \ para continuar en la siguiente línea).

```
#ACTION  SOURCE DEST            PROTO   DEST    SOURCE  ORIGINAL
#                                       PORT    PORT(S) DEST
ACCEPT   net:130.252.100.69,130.252.100.70 $FW \
                                tcp     22
```

7) Aceptar todas las conexiones al puerto 2222 del firewall y redireccionarlas al

puerto 22 del sistema local 192.168.1.3.

```
        #ACTION  SOURCE DEST                PROTO   DEST    SOURCE  ORIGINAL
        #                                           PORT    PORT(S) DEST
        DNAT     net    loc:192.168.1.3:22  tcp     2222
```

8) Redireccionar todos los pedidos al puerto 80 a los puertos 81 a 90 eligiendo aleatoriamente.

```
        #ACTION  SOURCE DEST                PROTO DEST    SOURCE  ORIGINAL
        #                                         PORT    PORT(S) DEST
        REDIRECT net    $FW::81-90:random   tcp   www
```

9) Aceptar pings de la red local al firewall (macro).

```
        #ACTION  SOURCE DEST                PROTO DEST    SOURCE  ORIGINAL
        #                                         PORT    PORT(S) DEST
        Ping/ACCEPT loc fw
```

10) Redireccionar todos las conexiones al puerto 10022/tcp del firewall desde la Internet al puerto 22 y loggear la conexión en nivel info.

```
        #ACTION  SOURCE DEST                PROTO DEST    SOURCE  ORIGINAL
        #                                         PORT    PORT(S) DEST
        REDIRECT:info net ssh tcp 10022
```

Para conocer más acerca de las reglas, se puede leer el documento correspondiente en la referencia de Shorewall (también disponible como man-page): http://www.shorewall.net/manpages/shorewall-rules.html.

Macros (macros)

En el ejemplo 9 de la sección anterior se muestra como es posible utilizar una macro predefinida en el archivo de reglas. La macro Ping (`/usr/share/shorewall/macro.Ping`) se define como:

```
#
# Shorewall version 4 - Ping Macro
#
# /usr/share/shorewall/macro.Ping
#
#       This macro handles 'ping' requests.
#
###############################################################################
#ACTION SOURCE  DEST    PROTO   DEST    SOURCE  RATE    USER/
#                               PORT(S) PORT(S) LIMIT   GROUP
```

```
PARAM   -       -       icmp    8
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Esta definición dice que cada vez que se utilice el macro “Ping”, se debe reemplazar PARAM por el parámetro suministrador al macro (ACCEPT en el ejemplo), respetando el resto de la regla y definiendo el protocolo de destino como icmp y el puerto 8. Con esto, el ejemplo 9 de la sección anterior es traducida al momento de la compilación como:

```
        #ACTION  SOURCE DEST                PROTO DEST    SOURCE  ORIGINAL
        #                                          PORT    PORT(S) DEST
        ACCEPT   loc    fw                  icmp  8
```

Logrando el efecto deseado (que se acepten los pings desde la red local al firewall).

Para poder utilizar un macro “MiMacro” el mismo debe estar definido en el archivo `/usr/share/shorewall/macro.MiMacro` siguiente el formato especificado, el cual es muy similar al de las reglas.

En esta introducción no voy a ahondar en la tarea de definir macros, pero quisiera cerrar la sección listando los macros disponibles por defecto en Shorewall 4 y presentar ejemplos de uso de los mismos:

Macros disponibles (Shorewall 4.0.13):

AllowICMPs, Amanda, Auth, BitTorrent, CVS, Distcc, DNS, Drop, DropDNSrep, DropUPnP, Edonkey, Finger, FTP, Gnutella, GRE, HTTP, HTTPS, ICQ, IMAP, IMAPS, IPIP, IPP, IPPserver, IPsec, Ipsecah, IPsecnat, Jabberd, JabberPlain, JabberSecure, Jetdirect, L2TP, LDAP, LDAPS, MySQL, NNTP, NNTPS, NTP, NTPbrd, PCA, Ping, POP3, POP3S, PostgreSQL, Printer, Rdate, RDP, Reject, RNDC, Rsync, SixXS, SMB, SMBBI, SMBswat, SMTP, SMTPS, SNMP, SPAMD, SSH, Submission, SVN, Syslog, Telnet, Telnets, TFTP, Time, Trcrt, VNC, VNCL, Web, Webmin, Whois

Ejemplos:

1) Prohibir el acceso a la web de algunos hosts de la zona local:

```
        #ACTION  SOURCE DEST                PROTO DEST    SOURCE  ORIGINAL
        #                                          PORT    PORT(S) DEST
        Web/REJECT loc:172.16.5.0/24 net
```

2) Redirigir todo el tráfico BitTorrent a un host dentro de la red:

```
        #ACTION  SOURCE DEST                PROTO DEST    SOURCE  ORIGINAL
```

```
        #                                               PORT    PORT(S) DEST
        BitTorrent/DNAT net loc:192.168.1.5
```

3) Aceptar conexiones a un servidor MySQL corriendo en el firewall y loggear la actividad con nivel INFO.

```
        #ACTION  SOURCE DEST                PROTO DEST    SOURCE  ORIGINAL
        #                                         PORT    PORT(S) DEST
        MySQL/ACCEPT:info all fw
```

Para conocer más acerca de los macros, se puede leer el documento correspondiente en la referencia de Shorewall (tambien disponible como man-page): http://www.shorewall.net/manpages/shorewall-macros.html.

Masquerading (masq)

Una situación extremadamente común para los que poseemos redes hogareñas conectadas a Internet, es tener que aplicar masquerading a los hosts dado que uno solo posee una sola IP enunciable conectada a Internet.

Shorewall permite aplicar esta técnica mediante el archivo de configuración /etc/shorewall/masq:

```
#
# Shorewall version 4 - Masq file
#
# For information about entries in this file, type "man shorewall-masq"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-masq.html
#
#############################################################################
#INTERFACE              SOURCE          ADDRESS         PROTO   PORT(S)
IPSECMARK
ppp0 eth0
ppp1 eth1:192.168.0.0/24
ipsec0 !172.16.0.0/16
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

Estas tres definiciones de masquerading indican que:

- Todo el tráfico que se origine desde la interfaz `eth0` y deba salir por la interfaz `ppp0`, será modificado para tomar como dirección de origen el IP de la interfaz `ppp0`.

- Todo el tráfico proveniente desde la subred 192.168.0.0/24 por la interfaz

`eth1` destinado a pasar por la interfaz `ppp1`, será modificado para tomar como dirección de origen el IP de la interfaz `ppp1`.

- Todo el tráfico que NO se origine en la subred 172.16.0.0/16 (sin importar la interfaz por donde ingrese) y que esté destinado a pasar por la interfaz `ipsec0`, será modificado para tomar como dirección de origen el IP de la interfaz `ipsec0`.

Para conocer más acerca de este tema, se puede leer el documento correspondiente en la referencia de Shorewall (tambien disponible como man-page): http://www.shorewall.net/manpages/shorewall-masq.html.

shorewall.conf

Hasta el momento discutimos conceptos y archivos de configuración específicos a algún aspecto particular de firewall, pero hay cuestiones que no hacen a la tarea específica del filtrado que pueden ser configuradas, por ejemplo la generación de logs.

En Shorewall, la tarea de configuración de éstos aspectos genéricos recae sobre `/etc/shorewall/shorewall.conf`. La más importante de las opciones incluidas en este archivo es STARTUP_ENABLED a la cual debemos suministrar el valor “Yes” a esta variable, dado que de otro modo Shorewall se rehusará a ejecutar.

Otra opción importante (habilitada por defecto) es ADMINISABSENTMINDED, la cual evita que si activamos el firewall remotamente, no corte conexiones activas en dicho momento.

Para conocer más acerca de este tema, se puede leer el documento correspondiente en la referencia de Shorewall (tambien disponible como man-page): http://www.shorewall.net/manpages/shorewall.conf.html.

Operación

Normalmente utilizamos las facilidades de ejecución de servicios de las distribuciones para controlar la activación de Shorewall. A continuación veremos algunos de estos comandos en el caso que usemos RHEL, CentOS o Fedora:

1) Habilitar la ejecución automática de Shorewall para los runlevels multiusuario:

```
# chkconfig --level 345 shorewall on
```

2) Activar Shorewall:

```
# service shorewall start
```

3) Desactivar Shorewall:

```
# service shorewall start
```

Además de estos comandos, es posible controlar Shorewall utilizando el comando `shorewall`. Este comando, además de controlar la ejecución del firewall, permite habilitar o deshabilitar hosts e interfaces en zonas de reglas dinámicas, validar la configuración, y obtener información de estadísticas de ejecución. Estos son algunos de los comandos más usados:

- `shorewall clear`: Eliminar todas las reglas instaladas por Shorewall.
- `shorewall help`: Imprimir ayuda.
- `shorewall reset`: Re-inicializar los contadores de paquetes.
- `shorewall restart`: Reiniciar el firewall.
- `shorewall show`: Presenta información respecto de la configuración actual del firewall.
- `shorewall start`: Inicia el firewall
- `shorewall stop`: Detiene el firewall.
- `shorewall status`: Presienta información del estado de ejecución del firewall.

Para conocer más acerca de este tema, se puede leer el documento correspondiente en la referencia de Shorewall (también disponible como man-page): http://www.shorewall.net/manpages/shorewall.html.

Otros conceptos

Shorewall provee mucho más que lo presentado en éste documento. Shorewall posee una extensa documentación, tanto de referencia como tutoriales en donde se presentan todas las opciones de configuración y uso de Shorewall. La documentación puede accederse en http://www.shorewall.net/Documentation.html.

En esta sección presentaremos brevemente algunos conceptos que van más allá de un texto introductorio y que pueden ser de utilidad para los lectores:

Compilación de configuración

A partir de Shorewall 3, es posible compilar la configuración en un único script utilizando el comando `shorewall compile`. Esto permite generar un firewall autocontenido que no necesita Shorewall para correr.

Es posible utilizar el firewall compilado en combinación con shorewall-lite para configurar múltiples firewalls de manera centralizada. La idea se basa en utilizar una única configuración y `shorewall-lite` (instalado en cada firewall esclavo) puede interpretarla para configurarse.

Redes privadas virtuales (VPNs)

Shorewall permite tratar de manera distinta al tráfico por redes privadas virtuales y provee soporte para algunas de las implementaciones más populares como IPSec, PPTP y OpenVPN. Para obtener más información al respecto consultar: http://www.shorewall.net/VPNBasics.html.

Control de tráfico y congestión con Shorewall y tc

Desde la versión 2.5.5 Shorewall provee soporte para control de tráfico. Anteriormente Shorewall sólo se encargaba de invocar un script específico (tcstart) conteniendo las llamadas explícitas a `tc`.

No es el objetivo de éste documento ser un tutorial sobre control de tráfico ni mucho menos. El tema es extremadamente extenso y requiere muchos conocimientos tanto de TCP/IP como de los protocolos específicos para QoS.

Si se desea conocer más al respecto de éste tema les recomiendo los siguientes documentos:

- El documento “Linux Advanced Routing and Traffic Control HOWTO”: http://www.lartc.org. No es el más claro de los documentos, pero es la referencia fundamental sobre los temas tratados.

- La guía de usuario de HTB (Hierarchical Token Bucket): http://luxik.cdi.cz/~devik/qos/htb/manual/userg.htm.

- La documentación de NetFilter disponible en http://www.netfilter.org/documentation.

- La documentación al sobre QoS y Traffic Shaping de Shorewall:

http://www.shorewall.net/traffic_shaping.htm.

shorewall-shell, shorewall-lite, shorewall-perl

A partir de la versión 4 de Shorewall se introdujeron dos herramientas adicionales (opcionales) conocidas como `shorewall-lite` y `shorewall-perl`, y el paquete de la herramienta principal fue renombrado de shorewall a `shorewall-shell`.

Como vimos en una sección anterior, el propósito de `shorewall-lite` es permitir centralizar la configuración de los firewalls en una red. Utilizando shorewall se compila una configuración que luego es ejecutada remotamente por `shorewall-lite`.

`shorewall-perl` es una reimplementación del compilador de Shorewall escrito en Perl. Como toda alternativa a una solución establecida, presenta algunas ventajas y desventajas:

- El compilador de mucho más rápido que su contraparte escrito en BASH.
- El script generado utiliza `iptables-restore` para inicializar la configuración de Netfilter lo que hace que la carga del firewall sea mucho más rápida.
- El compilador hace chequeos de la configuración mucho más profundos.
- Los mensajes de error son más claros y precisos indicando el nombre y la linea en el archivo donde se produjo el inconveniente.
- Todos los futuros desarrollos de Shorewall estarán orientados a `shorewall-perl` y solo se portarán en `shorewall-shell` las modificaciones que sean fáciles de implementar.
- `shorewall-perl` provee funcionalidades específicas de firewall que no están disponibles en `shorewall-shell`.
- `shorewall-perl` presenta bastantes incompatibilidades con shorewall-shell.
- `shorewall-perl` tiene más dependencias que shorewall-shell.
- `shorewall-perl` está escrito en Perl.

Ejemplos

En esta sección presentaré algunos ejemplos sencillos para quienes desean probar Shorewall sin demasiado esfuerzo. No abordaré topologías complicadas sino aquellas que pueden encontrarse frecuentemente en redes hogareñas e industriales.

En el sitio de Shorewall además de la documentación de referencia, se pueden encontrar artículos y guías de usuario cuyo objetivo es lograr alguna tarea específica, como por ejemplo: ¿Cómo conectarse a múltiples ISP?, ¿Cómo usar Shorewall con IPP2?, y MUCHISIMOS más.

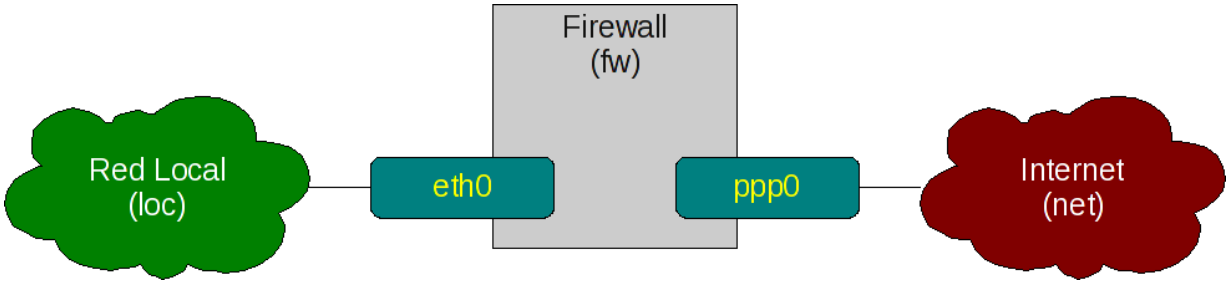
Cada ejemplo se estructurará de la siguiente manera:

- Se presenta la topología básica.
- Se elicitan los requerimientos específicos de la tarea del firewall.
- Se presentan los archivos de configuración indicando particularidades donde fuese necesario.
- Se discuten posibles alteraciones a la configuración.

Configuración básica con masquerading

Hoy en día es extremadamente común tener una conexión de banda ancha (sea xDSL, o cable modem) con dos o tres equipos conectados a través de un modem-router o equipos similares. Este tipo de equipos es extremadamente conveniente dado que provee la seguridad y funcionalidad suficientes para casi todas las situaciones y no consume tanta electricidad como una PC, sin embargo, algunas veces necesitamos control total sobre la manera en la que nos conectamos a la Internet.

En éstos casos específicos la topología habitual es presentada en el siguiente diagrama:



Aquí tenemos, una red local, el firewall con dos interfaces y la Internet. La idea es dar acceso total a Internet a los equipos de la red local haciendo

masquerading e implementar el máximo de seguridad posible. Asumimos que hay un servidor DHCP corriendo en el firewall para las máquinas dentro de la red local y que poseemos un servidor web y ssh en el firewall que deseamos acceder desde la Internet.

En este ejemplo supuse que la conexión a Internet es vía ADSL utilizando PPPoE (PPP over Ethernet), por ende la interfaz de salida será pppX. En caso que utilicemos otro modo de conexión (CableModem, por ejemplo), solo hay que hacer un cambio trivial en la configuración, como veremos más adelante.

/etc/shorewall/zones:

```
#
# Shorewall version 4 - Zones File
#
# For information about this file, type "man shorewall-zones"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-zones.html
#
###############################################################################
#ZONE TYPE        OPTIONS           IN                OUT
#                             OPTIONS                 OPTIONS

fw    firewall
loc   ipv4
net   ipv4

#LAST LINE - ADD YOUR ENTRIES ABOVE THIS ONE - DO NOT REMOVE
```

/etc/shorewall/interfaces:

```
#
# Shorewall version 4 - Interfaces File
#
# For information about entries in this file, type "man shorewall-interfaces"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-interfaces.html
#
###############################################################################
#ZONE INTERFACE   BROADCAST   OPTIONS

loc   eth0        detect      dhcp

# Utilizando ADSL via PPPoE (notar el comodin)
net   ppp+        -           dhcp,norfc1918,nosmurfs,tcpflags

# Utilizando cable modem en la interfaz eth1
#net  eth1        detect      dhcp,norfc1918,nosmurfs,tcpflags

#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

/etc/shorewall/masq:

```
#
# Shorewall version 4 - Masq file
#
# For information about entries in this file, type "man shorewall-masq"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-masq.html
#
###############################################################################
#INTERFACE       SOURCE          ADDRESS         PROTO PORT(S)     IPSEC
# MARK

# Utilizando ADSL via PPPoE
ppp+              eth0

# Utilizando CableModem en la interfaz eth1
#eth1             eth0

#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

/etc/shorewall/policy:

```
#
# Shorewall version 4 - Policy File
#
# For information about entries in this file, type "man shorewall-policy"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-policy.html
#
###############################################################################
#SOURCE          DEST        POLICY          LOG         LIMIT:BURST
#                                LEVEL

# Desde la red local a cualquier otra zona
loc               all        ACCEPT

# Desde el firewall a cualquier otra zona
fw                all        ACCEPT

# Desde la Internet a cualquier otra zona (ignorar y loggear)
net               all        DROP            info

# Otro caso (rechazar y loggear)
all               all        REJECT          info

#LAST LINE -- DO NOT REMOVE
```

/etc/shorewall/rules:

```
#
# Shorewall version 4 - Rules File
#
# For information on the settings in this file, type "man shorewall-rules"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-rules.html
#
###############################################################################
#########################################
#ACTION          SOURCE          DEST        PROTO DEST  SOURCE
# ORIGINAL  RATE        USER/ MARK
#                                       PORT  PORT(S)          DEST
$ LIMIT          GROUP
#SECTION ESTABLISHED
#SECTION RELATED
SECTION NEW

Web/ACCEPT all fw
SSH/ACCEPT all fw

#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

/etc/shorewall/shorewall.conf:

NOTAR QUE NO ES EL ARCHIVO COMPLETO

```
###############################################################################
#  /etc/shorewall/shorewall.conf V4.0 - Change the following variables to
#  match your setup
#
#  This program is under GPL
#  [http://www.gnu.org/licenses/old-licenses/gpl-2.0.txt]
#
#  This file should be placed in /etc/shorewall
#
#  (c) 1999,2000,2001,2002,2003,2004,2005,
#      2006,2007 - Tom Eastep (teastep@shorewall.net)
#
#  For information about the settings in this file, type "man shorewall.conf"
#
#  Additional information is available at
#  http://www.shorewall.net/Documentation.htm#Conf
###############################################################################
#                  S T A R T U P   E N A B L E D
###############################################################################

STARTUP_ENABLED=Yes
```

... (Continua /etc/shorewall/shorewall.conf)

```
###############################################################################
#                        L O G G I N G
###############################################################################

LOGFILE=/var/log/messages

LOGFORMAT="Shorewall:%s:%s:"

LOGTAGONLY=No

LOGRATE=10/minute

LOGBURST=5
```

... (Continua /etc/shorewall/shorewall.conf)

```
#LAST LINE -- DO NOT REMOVE
```

Esta configuración asume que no limitaremos las conexiones de la zona local al firewall, ni del firewall a la Internet, lo cual es relativamente común, pero no muy seguro. Los siguientes archivos de configuración intentan corregir esta situación. Los archivos que no se incluye se asumen que poseen el mismo contenido que antes.

/etc/shorewall/policy:

```
#
# Shorewall version 4 - Policy File
#
# For information about entries in this file, type "man shorewall-policy"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-policy.html
#
###############################################################################
#SOURCE          DEST        POLICY           LOG         LIMIT:BURST
#                                  LEVEL

# Desde la red local a la Internet
loc               net         ACCEPT

# Desde la red local al firewall (rechazar explicitamente)
loc               fw          REJECT

# Desde la Internet a cualquier otra zona (ignorar y loggear)
net               all         DROP             info
```

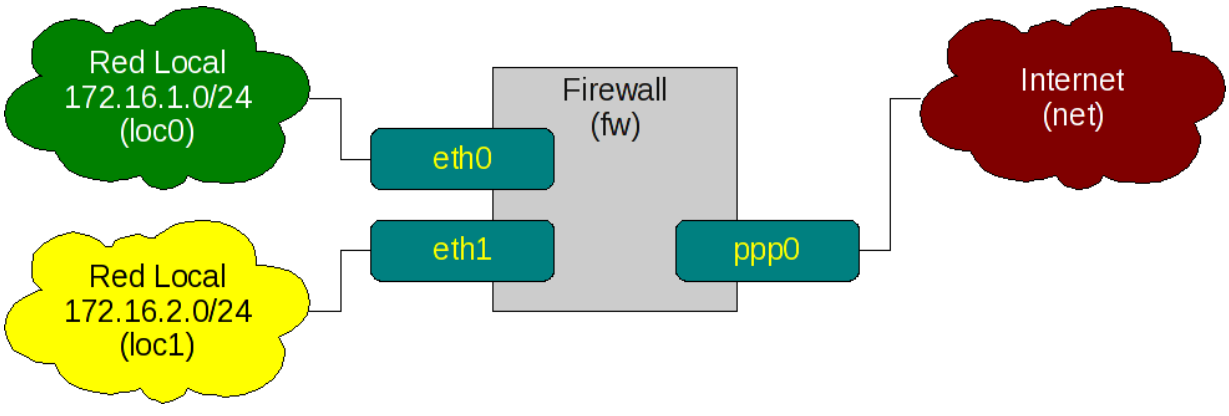
```
# Otro caso (rechazar y loggear)
all               all        REJECT           info

#LAST LINE -- DO NOT REMOVE
```

/etc/shorewall/rules:

```
#
# Shorewall version 4 - Rules File
#
# For information on the settings in this file, type "man shorewall-rules"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-rules.html
#
##############################################################################
###########################################
#ACTION           SOURCE            DEST        PROTO DEST  SOURCE
# ORIGINAL  RATE        USER/ MARK
#                                          PORT  PORT(S)          DEST
$ LIMIT           GROUP
#SECTION ESTABLISHED
#SECTION RELATED
SECTION NEW

DNS/ACCEPT loc fw
DNS/ACCEPT fw all

Web/ACCEPT all fw
SH/ACCEPT all fw

#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Configuración básica multi-zona

Continuando el ejemplo anterior, supongamos que ahora le damos Internet a unos vecinos, pero solo queremos que ellos tengan acceso a Web y ningún otro protocolo. Una primera solución es agregar una interfaz al firewall y conectar por ella los vecinos:



Veamos como quedarían los archivos de configuración:

/etc/shorewall/zones:

```
#
# Shorewall version 4 - Zones File
#
# For information about this file, type "man shorewall-zones"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-zones.html
#
###############################################################################
#ZONE TYPE        OPTIONS           IN                OUT
#                             OPTIONS                OPTIONS

fw    firewall
loc0  ipv4
loc1  ipv4
net   ipv4

#LAST LINE - ADD YOUR ENTRIES ABOVE THIS ONE - DO NOT REMOVE
```

/etc/shorewall/interfaces:

```
#
# Shorewall version 4 - Interfaces File
#
# For information about entries in this file, type "man shorewall-interfaces"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-interfaces.html
#
###############################################################################
#ZONE INTERFACE   BROADCAST   OPTIONS

loc0  eth0        detect      dhcp
loc1  eth1        detect      dhcp
net   ppp+        -           dhcp,norfc1918,nosmurfs,tcpflags

#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

/etc/shorewall/masq:

```
#
# Shorewall version 4 - Masq file
#
# For information about entries in this file, type "man shorewall-masq"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-masq.html
#
```

```
###############################################################################
#INTERFACE       SOURCE            ADDRESS           PROTO PORT(S)     IPSEC
# MARK

ppp+              eth0
ppp+              eth1

#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

/etc/shorewall/policy:

```
#
# Shorewall version 4 - Policy File
#
# For information about entries in this file, type "man shorewall-policy"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-policy.html
#
###############################################################################
#SOURCE          DEST        POLICY           LOG         LIMIT:BURST
#                                 LEVEL

loc0              all        ACCEPT
# No olvidar el tráfico inter-zona local
loc1              loc0       ACCEPT
loc1              all        REJECT
fw                all        ACCEPT
net               all        DROP             info
all               all        REJECT           info

#LAST LINE -- DO NOT REMOVE
```

/etc/shorewall/rules:

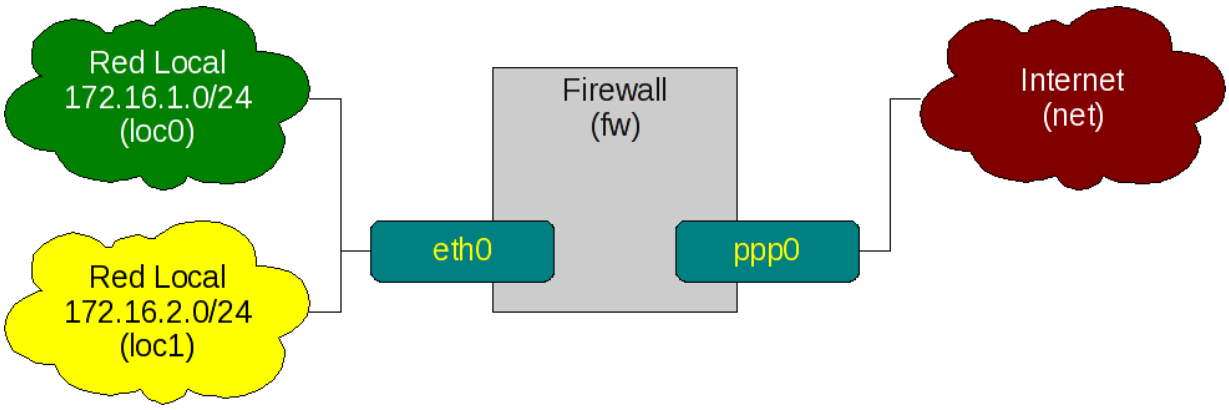
```
#
# Shorewall version 4 - Rules File
#
# For information on the settings in this file, type "man shorewall-rules"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-rules.html
#
###############################################################################
###########################################
#ACTION          SOURCE            DEST        PROTO DEST  SOURCE
# ORIGINAL  RATE        USER/ MARK
#                                        PORT  PORT(S)          DEST
$ LIMIT           GROUP
#SECTION ESTABLISHED
#SECTION RELATED
SECTION NEW
```

```
# Dado que la politica generica loc1 era REJECT, la siguiente linea habilita
# solo el acceso a la web.
Web/ACCEPT loc1 all

Web/ACCEPT all fw
SSH/ACCEPT loc0 fw

#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

/etc/shorewall/shorewall.conf:

Igual que antes.

Ahora bien, en caso que no deseemos agregar una interfaz (real o virtual) al firewall, podemos utilizar el soporte para interfaces multizona de Shorewall. La topología para esta solución sería:



Bajo esta nueva configuración solo es necesario modificar el archivo `interfaces` y `hosts` y `masq`:

/etc/shorewall/interfaces:

```
#
# Shorewall version 4 - Interfaces File
#
# For information about entries in this file, type "man shorewall-interfaces"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-interfaces.html
#
###############################################################################
#ZONE INTERFACE   BROADCAST   OPTIONS

-     eth0        detect      dhcp
net   ppp+        -           dhcp,norfc1918,nosmurfs,tcpflags

#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

/etc/shorewall/masq:

```
#
# Shorewall version 4 - Masq file
#
# For information about entries in this file, type "man shorewall-masq"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-masq.html
#
#############################################################################
#INTERFACE        SOURCE            ADDRESS           PROTO PORT(S)     IPSEC
# MARK

ppp+              eth0

#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

/etc/shorewall/hosts:

```
#
# Shorewall version 4 - Hosts file
#
# For information about entries in this file, type "man shorewall-hosts"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-hosts.html
#
#############################################################################
#ZONE HOST(S)                              OPTIONS
loc0  eth0:172.16.1.0/24
loc1  eth0:172.16.2.0/24
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS LINE -- DO NOT REMOVE
```

El resto de los archivos de configuración no se modifican.

Redirección de puertos

Otra situación relativamente común es la necesidad de redireccionar conexiones. En esta sección presentaremos tres casos típicos de reglas de redireccionamiento tanto para conexiones desde la Internet, como desde la red local. En todos los casos las reglas se deben introducir en la sección “NEW” del archivo `/etc/shorewall/rules`. Suponemos una topología similar a la discutida en el primero de los ejemplos donde los hosts locales se encuentran en la sub-red 172.16.1.0/24.

Para P2P

Supongamos que nuestro firewall no es capaz de correr programas P2P por la razón que sea (poco espacio en disco, poco poder de cómputo, etc.). Una posibilidad es elegir una máquina dentro de la red local (Por ej.: 172.16.1.100) como cliente de dichos protocolos. Para poder hacer esto, y dado que estamos haciendo *masquerading*, es necesario redireccionar las conexiones entrantes de los protocolos P2P a la máquina cliente mediante el uso de las siguientes reglas:

/etc/shorewall/rules:

```
#
# Shorewall version 4 - Rules File
#
# For information on the settings in this file, type "man shorewall-rules"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-rules.html
#
###############################################################################
#############################################
#ACTION         SOURCE          DEST            PROTO   DEST    SOURCE
ORIGINAL        RATE            USER/   MARK
#                                                       PORT    PORT(S)
DEST            LIMIT           GROUP
#SECTION ESTABLISHED
#SECTION RELATED
SECTION NEW
BitTorrent/DNAT net             loc:172.16.1.100
Edonkey/DNAT    net             loc:172.16.1.100
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

El ejemplo solo incluye los protocolos ED2K y BitTorrent, pero existen macros para otros protocolos también. Supongamos que deseamos ser explícitos respecto de las conexiones que estamos direccionando (por ejemplo, si no deseamos utilizar los puertos estándar), podemos escribir:

/etc/shorewall/rules:

```
#
# Shorewall version 4 - Rules File
#
# For information on the settings in this file, type "man shorewall-rules"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-rules.html
#
###############################################################################
#############################################
#ACTION         SOURCE          DEST            PROTO   DEST    SOURCE
```

```
ORIGINAL        RATE            USER/   MARK
#                                                       PORT    PORT(S)
DEST            LIMIT           GROUP
#SECTION ESTABLISHED
#SECTION RELATED
SECTION NEW
DNAT net loc:172.16.1.100 tcp 6881:6889,4661,4662,4711
DNAT net loc:172.16.1.100 udp 6881:6889,4665,4672
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Para servidores internos

El caso de redireccionar conexiones a servidores internos, es idéntico al anterior, pero para otros protocolos. Supongamos ahora que queremos redirigir las conexiones de web y SMTP a un servidor interno (172.16.1.5). Como particularidad supondremos que el servidor SMTP no está escuchando en el puerto 25/tcp sino 10025/tcp. Las reglas quedarían de la siguiente manera:

/etc/shorewall/rules:

```
#
# Shorewall version 4 - Rules File
#
# For information on the settings in this file, type "man shorewall-rules"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-rules.html
#
###############################################################################
#############################################
#ACTION         SOURCE          DEST            PROTO   DEST    SOURCE
ORIGINAL        RATE            USER/   MARK
#                                                       PORT    PORT(S)
DEST            LIMIT           GROUP
#SECTION ESTABLISHED
#SECTION RELATED
SECTION NEW
Web/DNAT net loc:172.16.1.5
SMTP/DNAT net loc:172.16.1.5:10025
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Proxy transparente

Continuando con el ejemplo multizona (con una sola interfaz), ahora supongamos que además de solo permitirles a los vecinos acceder a la Web, ahora haremos que pasen por un proxy HTTP de manera transparente. Supongamos que el proxy está ejecutándose en el mismo firewall en el puerto 3128/tcp, así la regla de redirección sería:

/etc/shorewall/rules:

```
#
# Shorewall version 4 - Rules File
```

```
#
# For information on the settings in this file, type "man shorewall-rules"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-rules.html
#
###############################################################################
#########################################
#ACTION          SOURCE            DEST        PROTO DEST  SOURCE
# ORIGINAL  RATE        USER/ MARK
#                                          PORT  PORT(S)          DEST
$ LIMIT           GROUP
#SECTION ESTABLISHED
#SECTION RELATED
SECTION NEW

# Con la ultima opcion evitamos redirecciones de conexiones con destinos locales
Web/REDIRECT loc1 3128 tcp www - !172.16.0.0/16

Web/ACCEPT all fw
SSH/ACCEPT loc0 fw

#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

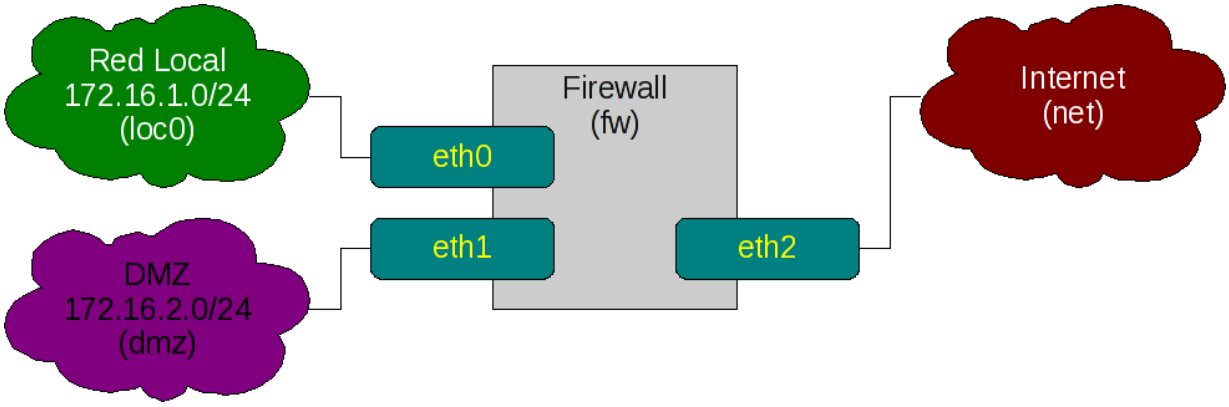
Firewall con zona desmilitarizada (DMZ)

El siguiente párrafo fue extraído del artículo sobre zonas desmilitarizadas de Wikipedia en inglés[3]:

> En una red, los equipos más vulnerables son aquellos que proveen servicios a usuarios fuera de la LAN, como servidores de correo electrónico, web o DNS. Dado el potencial a que estos equipos sean comprometidos, éstos son ubicados en su propia sub-red para proteger al resto de la red en el eventual caso que un intruso ingrese exitósamente. Los equipos en la zona desmilitarizada (DMZ) no deberían poder iniciar conexiones directas con otros equipos dentro de la red interna, aunque la comunicación con otros equipos dentro de la DMZ o las redes externas está permitido. Esto permite a los equipos de la DMZ proveer servicios a la red interna y externa, mientras un firewall se encarga de controlar el tráfico entre los servidores de la DMZ y los clientes internos.

Una forma de implementar una DMZ, es mediante una topología prácticamente a la del ejemplo multi-zona que vimos anteriormente:

3 http://en.wikipedia.org/wiki/Demilitarized_zone_(computing)



Existen otras formas de implementarlo, particularmente utilizando dos niveles de firewall, pero prefiero mantener el ejemplo lo más simple posible.

Vamos a suponer que la zona desmilitarizada tiene un web server (172.16.2.2) un servidor de nombres (172.16.2.3) y un servidor mail (172.16.2.4), los cuales prestan servicios para la red interna y externa.

Veamos una posible configuración de Shorewall que cumpla con los requerimientos.

/etc/shorewall/zones:

```
#
# Shorewall version 4 - Zones File
#
# For information about this file, type "man shorewall-zones"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-zones.html
#
###############################################################################
#ZONE TYPE        OPTIONS           IN                OUT
#                                OPTIONS                OPTIONS

fw    firewall
loc   ipv4
dmz   ipv4
net   ipv4

#LAST LINE - ADD YOUR ENTRIES ABOVE THIS ONE - DO NOT REMOVE
```

/etc/shorewall/interfaces:

```
#
# Shorewall version 4 - Interfaces File
#
# For information about entries in this file, type "man shorewall-interfaces"
#
```

```
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-interfaces.html
#
###############################################################################
#ZONE INTERFACE   BROADCAST   OPTIONS

loc   eth0        detect           dhcp
dmz   eth1        172.16.2.255
net   eth2        detect           dhcp,norfc1918,nosmurfs,tcpflags

#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

/etc/shorewall/masq:

```
#
# Shorewall version 4 - Masq file
#
# For information about entries in this file, type "man shorewall-masq"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-masq.html
#
###############################################################################
#INTERFACE        SOURCE           ADDRESS          PROTO PORT(S)     IPSEC
# MARK

eth2             eth0
eth2             eth1

#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

/etc/shorewall/policy:

```
#
# Shorewall version 4 - Policy File
#
# For information about entries in this file, type "man shorewall-policy"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-policy.html
#
###############################################################################
#SOURCE           DEST        POLICY           LOG         LIMIT:BURST
#                                 LEVEL

fw               all         ACCEPT
loc              all         ACCEPT
# No se pueden iniciar conexiones desde la DMZ
dmz              all         REJECT
net              all         DROP             info
all              all         REJECT           info

#LAST LINE -- DO NOT REMOVE
```

/etc/shorewall/rules:

```
#
# Shorewall version 4 - Rules File
#
# For information on the settings in this file, type "man shorewall-rules"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-rules.html
#
###############################################################################
#########################################
#ACTION          SOURCE            DEST        PROTO DEST  SOURCE
# ORIGINAL  RATE        USER/ MARK
#                                         PORT  PORT(S)          DEST
$ LIMIT          GROUP
#SECTION ESTABLISHED
#SECTION RELATED
SECTION NEW

# Permitir iniciar conexiones a algunos de los servidores en la DMZ.
DNS/ACCEPT        dmz              all
SMTP/ACCEPT       dmz              all

# Redestinar las conexiones de la internet al firewall a los servidores
# respectivos dentro de la DMZ.
Web/DNAT          net               dmz:172.16.2.2
DNS/DNAT          net               dmz:172.16.2.3
SMTP/DNAT         net               dmz:172.16.2.4

#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

/etc/shorewall/shorewall.conf:

NOTAR QUE NO ES EL ARCHIVO COMPLETO

```
###############################################################################
#  /etc/shorewall/shorewall.conf V4.0 - Change the following variables to
#  match your setup
#
#  This program is under GPL
#  [http://www.gnu.org/licenses/old-licenses/gpl-2.0.txt]
#
#  This file should be placed in /etc/shorewall
#
#  (c) 1999,2000,2001,2002,2003,2004,2005,
#      2006,2007 - Tom Eastep (teastep@shorewall.net)
#
#  For information about the settings in this file, type "man shorewall.conf"
#
#  Additional information is available at
```

```
#  http://www.shorewall.net/Documentation.htm#Conf
###############################################################################
#                  S T A R T U P   E N A B L E D
###############################################################################

STARTUP_ENABLED=Yes
```

... (Continua /etc/shorewall/shorewall.conf)

```
###############################################################################
#                         L O G G I N G
###############################################################################

LOGFILE=/var/log/messages

LOGFORMAT="Shorewall:%s:%s:"

LOGTAGONLY=No

LOGRATE=10/minute

LOGBURST=5
```

... (Continua /etc/shorewall/shorewall.conf)

```
#LAST LINE -- DO NOT REMOVE
```

Por razones de simpleza no quise fortalecer la seguridad del firewall. Lo importante de este ejemplo es la sección resaltada en el archivo `policy`: Lo principal es limitar las conexiones que pueden iniciarse desde la DMZ. El resto de la configuración es idéntica a otros ejemplos presentados.

Si quisiéramos incrementar el nivel de seguridad deberíamos rechazar las conexiones al firewall (por política) y habilitar (mediante reglas) el acceso a algunas máquinas restringidas.

Conclusiones

Shorewall es una herramienta impresionante. Aunque manipular Netfilter directamente mediante iptables puede ser una experiencia enriquecedora, llega un momento en donde se hace casi imposible tener una visión global del firewall a la vez que uno se dedica al detalle fino de la manipulación de paquetes. Shorewall facilita enormemente la tarea del administrador y, en mi

opinión, a pesar de agregar un nivel de complejidad más al sistema, la abstracción introducida por el lenguaje redunda en una mayor seguridad.

Espero que este documento (y la charla asociada) les sirva de ayuda. Como siempre, si tienen alguna consulta respecto de éstos temas, no duden en enviar un correo a la lista grulic@grulic.org.ar o visiten el canal IRC #grulic en freenode.net (me pueden encontrar con el nick “m4rgin4l”).

Agradecimientos

Quiero agradecer a toda la comunidad que desarrolla y mantiene Shorewall y en particular a Tom Eastep (el autor de Shorewall) por no darse por vencido.