Configuración de Firewall Shorewall de dos interfaces con NAT en Ubuntu Server

Jorge Armando Medina

Computación Gráfica de México.
Documentación Técnica

2011/02/08

Resumen

Este documento describe los procedimientos para la configuración de un Firewall en Ubuntu Server usando la herramienta Shorewall en un sistema con dos interfaces de red, se describen los procedimientos para realizar tareas desde: configuración básica del firewall, diferentes configuraciones de NAT: como Port Forwarding, Transparent Proxy, Source NAT, NAT One-To-One, monitorización de conexiones y ancho de banda, y los comandos para la operación del firewall.

Tabla de contenidos

Introducción

Durante el transcurso del documento realizaremos diferentes tareas de configuración en un Firewall con funciones de enrutado en un sistema con GNU/Linux usando la distribución Ubuntu Server LTS 8.04.4, el sistema cuenta con dos interfaces de red, una conectada directamente a un router o modem del provedor de Internet y otra conectada al switch de la red local, en la red local están conectados varios servidores y PCs de usuario así como impresoras en red. Las tareas más comunes de configuración, administración y monitorización de un Firewall serán descritas en este documento, en la siguiente lista podemos ver las tareas a realizar:

- Configurar los parametros de red para sistema GNU/Linux dos interfaces de red (Multi-homed).
- Instalación de los pre requisitos del sistema GNU/Linux para operar como Router y Firewall.
- Instalación y configuración básica del Firewall Shorewall en un sistema con dos interfaces de red.
- Configuración de Ennmascaramiento de IP (MASQUERADING/SNAT) para dar salida a Internet a los usuarios de la LAN de forma segura y controlada.
- Crear reglas de Firewall para Proxy HTTP Transparente.
- Crear reglas de NAT Port Forwarding (DNAT) para redireccionar tráfico desde el Internet a sistemas en la red local.
- Crear reglas NAT One-to-One.
- Configuración de sistema de Logs para el registro de eventos del Firewall Shorewall.
- Monitorizando las conexiones al firewall y ancho de banda.
- Usando los comandos de operación del Firewall Shorewall.

Para realizar las tareas antes descritas se requieren conocimientos básicos de redes TCP/IP, conocimientos básicos de administración de sistemas GNU/Linux como: edición de archivos de texto, fluidez en la línea de comandos e instalación de paquetes.

Información de la red propuesta con el firewall Shorewall

En esta sección se describen el esquema de red en la que estará conectado el firewall Shorewall detallando las configuraciones de los diferentes equipos involucrados.

Diagrama del esquema de red propuesto

La conexión a la red local se realiza mediante un switch a la que estan también conectados los servidores, PCs e impresoras de red, la conexión a Internet se reaíza a través de un router provisto por el ISP, es un enlace de 2Mbps con un pool de direcciones IP públicas.

El siguiente diagrama describe el esquema de red:

Figura 1. Esquema de Red

En la siguiente sección se describen con más detalles los parametros de configuración de los equipos involucrados.

Información sobre los componentes de red

Los parametros básicos de red de Router del iSP se resume en la siguiente tabla:

Tabla 1. Infomación de parametros de red de Router ISP

Dirección	Valor
Interfaz de red	Ethernet
Dirección MAC	AA:CC:00:00:00:02
Dirección de Host	10.0.99.1
Mascara de Subred	255.255.255.0 ó 24bits

Los parametros de red del firewall de la conexión de Internet se resume en la siguiente tabla:

Tabla 2. Infomación de parametros de red de Firewall - Internet

Dirección	Valor
Interfaz de red	eth1
Dirección MAC	08:00:27:20:2b:09
Dirección de Host	10.0.99.220
Mascara de Subred	255.255.255.0 ó 24bits
Dirección de Broadcast	10.0.99.255
Dirección del Gateway	10.0.99.1
Dirección DNS Primario	127.0.0.1 (DNS Cache local)
Sufijo DNS	example.com

Los parametros de red del firewall de la conexión de la red local se resume en la siguiente tabla:

Tabla 3. Infomación de parametros de red de Firewall - red local

Dirección	Valor
Interfaz de red	eth0
Dirección MAC	08:00:27:4c:a3:f6
Dirección de subred	192.168.1.0/24
Dirección de Host	192.168.221.254
Mascara de Subred	255.255.255.0 ó 24bits
Dirección de Broadcast	191.168.221.255

Es importante que mantenga actualizada esta información si se realizan cambios en la configuración de cualquier componente de red involucrado.

Información de sistema operativo Ubuntu Server

En la siguiente tabla se describe la información del sistema operativo Ubuntu Server usado en la implementación del firewall:

Tabla 4. Información del sistema operativo Ubuntu Server

Elemento	Descripción
Sistema Operativo	Ubuntu Server LTS 8.04.4 amd64
Kernel	Linux 2.6.24-24-server
CPU	AMD Phenom(tm) II X2 550 Processor
Memoria	256MB
Disco duro	80GB SATA

Los programas instalados para la solución se describen en la siguiente tabla:

Tabla 5. Lista de paquetes adicionales

Paquete	Versión	Descripción
Kernel Linux	linux-image-2.6.24-24-server	Instalado por default en Ubuntu Server
iptables	1.3.8.0debian1-1ubuntu2	Instalado por default en Ubuntu Server
iproute	20071016-2ubuntu2	Instalado por default en Ubuntu Server
perl	5.8.8-12ubuntu0.4	Instalado por default en Ubuntu Server
shorewall	4.4.7	Instalado manualmente vía shorewall.net

Todos los programas son software libre.

Configuraciones de los parametros de red en Ubuntu Server

En el archivo `/etc/hostname` se define el nombre de host del servidor firewall.

```
proxy.example.com
```

En el archivo de configuración de parametros de red `/etc/network/interfaces` se definen las interfaces de red y sus parametros de configuración.

```
 The loopback network interface
auto lo
iface lo inet loopback

# Interfaz LAN
auto eth0
iface eth0 inet static
  address 192.168.221.254
  netmask 255.255.255.0

# Interfaz WAN
auto eth1
iface eth1 inet static
  address 10.0.99.220
  netmask 255.255.255.0
  gateway 10.0.99.1
```

En el archivo de configuración `/etc/hosts` se define la resolución de nombres de hosts local.

```
127.0.0.1               localhost.localdomain   localhost
192.168.221.254         proxy.example.com       proxy
```

En el archvo de configuración `/etc/resolv.conf` se definen los parametros de los servidores DNS.

```
search example.com
nameserver 127.0.0.1
```

Asegurese de tener correctamente configurados los parametros de red antes de iniciar la instalación y configuración del firewall Shoerwall.

Instalando los Pre requisitos para la instalación de Shorewall en Ubuntu Server

Una correcta implementación de un Firewall con Shorewall sobre Ubuntu Server o cualquier otra distribución GNU/Linux requiere de los siguientes componentes:

- **Netfilter** - El kernel instalado debe incluir soporte para filtrado de paquetes Netfilter, en Debian/Ubuntu el paquete de kernel ya incluye el soporte Netfilter de forma modular, los modulos de IPTables/Netfilter estan en el directorio `/lib/modules/`**uname -r**`/kernel/net/netfilter/`. Para más información sobre los parametros de configuración del kernel requeridos vea el documento Kernel Configuration en la documentación oficial de Shorewall.
- **IPTables** - El sistema debe incluir el paquete **iptables** el cual incluye el programa **iptables(8)**, **iptables-save(8)** e **iptables-restore(8)** los cuales son usados por Shorewall para ejecutar el script de reglas de firewall. Se recomienda por lo menos la versión de iptables 1.3.3.
- **iproute2** - El sistema debe tener instalado el paquete **iproute**, el cual incluye al programa **ip(8)** para mostrar y manipular rutas, dispositivos, policy routing y tueneles además del programa **tc(8)** el cual es usado para mostrar y manipular las configuraciones para el control de tráfico.
- **Perl** - Shorewall utiliza Perl para generar y compilar el script de reglas de firewall generado a partir de las reglas en los archivos de configuración.

Si no tiene todos estos paquetes se suguiere que los instale antes de instalar el paquete de Shorewall, por ejemplo:

```
# apt-get install iptables iproute perl
```

Para más información acerca de los pre requisitos de instalación vea la pagina Shorewall Requirements.

Instalación de Shorewall en Ubuntu Server

Instalaremos la versión estable más reciente de Shorewall, al momento de escribir este documento es Shorewall 4.4.7, descargue el paquete del sitio oficial de Shorewall llendo al menú Downloads=>Standard Download Sites y elija un repositorio de su preferencia.

Si desea ver la lista de de nuevas funcionalidades agregadas, cambios y problemas corregidos de la versión 4.4.7 vea el archivo releasenotes.txt.

Instalamos Shorewall 4.4.7 usando el paquete tar.bz2 descargado desde el sitio web.

```
# mkdir -p ~/paquetes/shorewall
```

Descargamos el paquete:

```
# cd ~/paquetes/shorewall/
# wget http://www.shorewall.net/pub/shorewall/CURRENT_STABLE_VERSION_IS_4.4/
shorewall-4.4.7/shorewall-4.4.7.5.tar.bz2
```

Instalamos Shorewall en el sistema:

```
# tar jxvf shorewall-4.4.7.5.tar.bz2
# cd shorewall-4.4.7.5/
# ./install.sh
```

El script `install.sh` copiará los scripts, directorios y archivos de configuración para iniciar la configuración, la siguiente tabla muestra un resumen de los archivos y directorios más relevantes:

Tabla 6. Archivos y directorios relevantes de Shorewall

Archivo o Directorio	Proposito
/sbin/shorewall	Script de control del programa
/etc/init.d/shorewall	Script de control de ejecución
/etc/shorewall	Directorio principal de archivos de configuración
/etc/shorewall/ shorewall.conf	Archivo de configuración de parametros generales
/etc/shorewall/zones	Archivo de definiciones de zones de tráfico
/etc/shorewall/interfaces	Archivo de definición de interfaces de red
/etc/shorewall/policy	Archivo de configuración de politicas de tráfico predeterminadas
/etc/shorewall/hosts	Archivo de definición de hosts y subredes
/etc/shorewall/rules	Archivo de definición de reglas de filtrado de tráfico y NAT (exclusiones a la pólitica)
/etc/shorewall/ routestopped	Archivo que controla el flojo de tráfico a través del firewall cuando esta en estado 'stopped'.

Archivo o Directorio	Proposito
/etc/shorewall/nat	Archivo de configuración para reglas de NAT (NAT 1-1)
/etc/shorewall/params	Archivo de configuración para definir parametros y variables generales
/etc/shorewall/masq	Archivo de configuración para Enmascaramiento NAT (SNAT, MASQUERADING)
/usr/share/shorewall/	Directorio de archivos comunes como Acciones, Macros, Compilador de reglas Perl, funciones compartidas,
/etc/logrotate.d/ shorewall	Archivo de rotación de logs propios del script Shorewall
/etc/default/shorewall	Archivo de configuración de parametros de control de ejecución

Nota

A partir de shorewall 4.4.8 no se copian automáticamente los archivos de configuración al directorio `/e`
el directorio `configfiles`, por ejemplo:

```
# cp /usr/share/shorewall/configfiles/{zones,interfaces,policy,hosts,rules,routesto
```

En la siguiente sección veremos como configurar el firewall Shorewall desde el inicio.

Configuración del Firewall Shorewall

En esta sección veremos los diferentes parametros de configuración y reglas para la configuración de Shorewall.

Introducción a los archivos de configuración de Shorewall

Como se mencionó en la sección anterior, Shorewall usa un conjunto de archivos de configuración para la creación de reglas de firewall, enrutado, control de tráfico y ancho de banda. La mayoría de los archivos de configuración estan en el directorio `/etc/shorewall`, Shorewall generará un script de iptables usando los parametros de configuración y reglas definidos en dichos archivos.

Para facilitar la administración de los parametros y reglas del firewall, Shorewal permite el uso de variables de shell para hacer referencia a información de uso común entre los diferenes componentes del firewall.

Las variables de shell se definen en el archivo `/etc/shorewall/params` de la siguiente forma:

```
VARIABLE_FIJA=valor
VARIABLE_LISTA=valor1,valor2,valor3
```

Importante

Las listas separadas por comas son usadas en muchos contextos en los archivos de configuración, las reglas para escribir listas son:

- No debe de tener espacios en blanco

  ```
  Valida:   routefilter,dhcp,arpfilter
  ```

```
Invalida: routefilter,     dhcp,     arpfilter
```

- Las entradas en una lista pueden ir en cualquier orden

Un ejemplo práctico, es definir las variables de shell usadas para la configuración del firewall basado en la información de red antes descrita:

```
LOG=info
NET_IF=eth1
LOC_IF=eth0
LOC_SUBNET=192.168.221.0/24
```

Estas variables pueden ser referenciadas en los archivos de configuración anteponiendo el simbolo $ antes del nombre de la variable, por ejemplo, en el archivo `/etc/shorewall/interfaces`:

```
net $NET_IF  detect  dhcp,routefilter=1,logmartians=1
```

Recuerde siempre escribir las variables en mayusculas recuerde que puede usar las variables para definir ACLs para listas de direcciones IP que pueden ser usadas en las reglas tanto para el origen o petición de la petición, o lista de puertos., por ejemplo:

```
LOC_IP_GERENTES=192.168.221.100,192.168.221.110,192.168.221.120
```

Recuerde no usar espacios en blanco en las listas.

Definicion de parametros y variables de entorno para shorewall

Lo primero que se aconseja al iniciar la configuración del firewall Shorewall es crear las variables de shell para definir el entorno de red, las variables las escribimos en el archivo `/etc/shorewall/params`, por ejemplo:

```
# Log level
LOG=info

# Interfaz WAN
NET_IF=eth1
# Interfaz LAN
LOC_IF=eth0

# Subred LAN
LOC_SUBNET=192.168.221.0/24

# ACLs
LOC_IP_SYSADMIN=192.168.221.200
LOC_IP_GERENTES=192.168.221.100,192.168.221.110,192.168.221.120
```

Es importante que si define listas cada elemento debe estar separado por coma y sin espacios.

Para más información acerca del archivo de definición de parametros vea el manual de *shorewall-params(5)*.

Definición de Zonas de tráfico en Shorewall

Shorewall ve la red en la que es ejecutado como compuesta por zonas (zones). En el diagrama Esquema de Red se pueden apreciar 2 redes diferentes, Internet y LAN las cuales pueden ser vistas como zonas

en la terminología de Shorewall:

Figura 2. Entorno de red y zonas shorewall

Las zonas son declaradas y se les asigna un tipo en el archivo `/etc/shorewall/zones`. Dadas las redes descritas en la tabla de arriba podemos definir las siguientes zonas de tráfico.

```
###############################################################################
#ZONE   TYPE            OPTIONS         IN                      OUT
#                                       OPTIONS                 OPTIONS
fw      firewall
net     ipv4            # Zona Internet
loc     ipv4            # Zona Local
```

Note que Shorewal reconoce al sistema firewall como su propía zona. El nombre de la zona que designa al firewall en si (usualmente '*fw*' como se muestra en el archivo) es almacenado en una variable de shell `$FW` la cual puede ser usada a través de las configuraciones de Shorewall para referenciar la zona firewall.

> **Nota**
>
> La zona fw esta predefinida ya que es el requerimiento minimo para un firewall standalone, y también es usada para firewalls con más de una interfaz de red.

La zonas serán usadas como referencia para definir politicas y reglas de tráfico, usualmente usando una tráfico originado en una zona y con destino en otra, por ejemplo:

- Tráfico originado en el Internet (zona net) con destino algún servicio local en el firewall, ejemplo Servicio SSH, VPN entre otros
- Tráfico originado en el Internet (zona net) con destino algún host en la LAN (zona loc), este sería un clasico ejemplo de NAT (Network Address Translation) para Port Forwarding
- Tráfico originado en la LAN (zona loc) con destino el Internet (zona net), otro ejemplo de NAT, en este caso Source NAT ó Enmascaramiento de IP
- Tráfico originado en la LAN (zona loc) con destino el firewall (zona fw), por ejemplo servicios de red locales como DHCP, DNS y/o Proxy

Una forma de asignar direcciones de red como subredes y hosts es asociar una zona a una interfaz de red, esta asociación se realiza en el archivo `/etc/shorewall/interfaces` ó `/etc/shorewall/hosts` que se verán en las siguientes secciónes.

Para más información acerca del archivo de definición de zonas vea el manual de *shorewall-zones(5)*.

Asociando una zona a una interfaz de red en Shorewall

La forma más fácil de asociar direcciones de red y/o hosts a una zona es asociando una zona con una interfaz de red usando el archivo `/etc/shorewall/interfaces`, por ejemplo:

```
#ZONE   INTERFACE       BROADCAST       OPTIONS
net     $NET_IF         detect          dhcp,routefilter=1,logmartians=1
loc     $LOC_IF         detect          dhcp
```

El ejemplo define la zona *net* como todos los hosts IPv4 que se comunican con el firewall a través de la interfaz de red `$NET_IF` (eth1), la zona *loc* como todos los hosts IPv4 que se comunican con el firewall a través de la interfaz de red `$LOC_IF` (eth0). Es importante notar que la composición de una zona esta definida en terminos de la combinación de direcciones **e** interfaces. Cuando use el archivo `/etc/shorewall/interfaces` para definir una zona, todas las direcciones están incluidas; cuando quiera definir una zona limitada por un sub conjunto de del espacio de direcciones IPv4, debe usar el archivo `/etc/shorewall/hosts` o puede usar la opción `nets=` en el archivo `/etc/shorewall/interfaces`:

```
#ZONE   INTERFACE       BROADCAST       OPTIONS
net     $NET_IF         detect          dhcp,blacklist,logmartians=1,nets=(!
$LOC_SUBNET),nosmurfs,routefilter=1,tcpflags
loc     $LOC_IF         detect          dhcp,nets=($LOC_SUBNET)
```

El ejemplo de arriba define la zona net como todos los hosts IPv4 que se comunican con el firewall a través de la interfaz `$NET_IF` (eth1) excepto para la subred 192.168.221/0/24, la zona loc como los hosts 192.168.221.0/24 IPv4 que se comunican con el firewall a través de la interfaz de red `$LOC_IF` (eth0).

La comuna `BROADCAST` sirve para especificar la dirección de red Brodcast (dirección de difusión) de la interfaz en particular, si usa el valor especial `detect`, Shorewall detectará la o las direcciones de broadcast por tí usando el soporte de *Address Type Match* de iptables y del kernel Linux. Si el sistema usa una interfaz P-T-P como **ppp0** la columa se deja en blanco.

> **Nota**
>
> Para ver si su sistema firewall soporta la capacidad *Address Type Match* use **shorewall show capabilities**, deberá obtener: *Address Type Match: Available*.

En la columna `OPTIONS` se define una lista separada por comas de opciones de control para el tráfico de/para dicha zona. El orden en el que las opciones son listadas no es sigificante, solo asegurese de que no incluir espacios en blanco. Para conocer una lista de las opciones soportadas vea *shorewall-interfaces(5)*.

> **Importante**
>
> Si la interfaz de red obtiene la dirección IP vía DHCP o si el sistema firewall ofrece servicios de DHCP para la red local use la opción `dhcp`.

Las reglas acerca de que tráfico permitir y que tráfico rechazar es expresado en terminos de zonas.

Para más información acerca del archivo de de zonas vea el manual de *shorewall-interfaces(5)*.

Definiendo las Polítcas de tráfico en Shorewall

Como hemos mencionado anteriormente, las reglas de tráfico son definidas en terminos de zonas y ahora que ya tenemos una interfaz y hosts asociadas a las zonas podremos definir las politicas y reglas de firewall. Shorewall permite definir politicas y reglas de filtrado de una foma fácil y comoda para la fácil administración del firewall mediante el archivo `/etc/shorewall/policy`.

La politica predeterminada para las conexiones de una zona a otra se definen en el archivo `/etc/shorewall/policy`, y las politicas a elejir son:

- **ACCEPT** - Aceptar la conexión

- **DROP** - Ignorar la peticón de conexión, la petición de la conexión es rechazada silenciosamente.
- **REJECT** - Rechazar la conexión con un mensaje de error a la petición de la conexión. El cliente de conexión recibe un mensaje de Conexión rechazada ó Connection refused.

Las peticiones de conexión pueden ser registradas (logging) como parte de la politica y es altamente recomendado registrar en una bitácora las politicas DROP y REJECT.

Una buena practica de seguridad es definir una politica de la siguiente manera: *Por default rechazar todas las conexiónes a excepción de aquellas explicitamente permitidas*. De esta forma nos facilitará la vida al mantener el conjunto de reglas (Ruleset) para el sistema firewall.

> **Importante**
>
> Siempre es más fácil cerrar todos los "puertos" y solo permitir un conjunto bien definido en lugar de estar cerrando los 65k disponibles.

Las excepciones a las politicas predeterminadas son definidas en el archivo `/etc/shorewall/rules`. Para cada petición de conexión que entra en el firewall, la petición es primero checada contra las reglas definidas en el archvo `/etc/shorewall/rules`. Si ninguna regla hace coincidencia con la petición de la conexión entonces la primer politica en `/etc/shorewall/policy` que haga coincidencia es aplicada.

Las politicas se definen de la siguiente manera:

```
###############################################################################
#SOURCE         DEST            POLICY          LOG     LIMIT:          CONNLIMIT:
#                                               LEVEL   BURST           MASK

fw              net             REJECT          info

net             fw              REJECT          $LOG
```

Se aconseja documentar la politica de filtrado de el firewall en una tabla como la que se muestra a continuación.

Tabla 7. Politica de filtrado de tráfico del Firewall

Zona Origen	Zona Destino	Acción	Registrar en Logs	Description
fw	net	Rechazar (REJECT)	Sí	Rechazar el trafico originado en el Firewall con destino el Internet y registrar en los logs las conexiones rechazadas.
net	fw	Rechazar (REJECT)	Sí	Rechazar el trafico originado en el Internet (exterior) con destino al mismo firewall y registrar en los logs las conexiones rechazadas.
fw	loc	Rechazar (REJECT)	Sí	Rechazar el trafico originado en el firewall con destino a hosts en la Red Local y registrar en los logs las conexiones rechazadas.
loc	fw	Rechazar (REJECT)	Sí	Rechazar el trafico originado en la LAN con destino al firewall y registrar en los logs las conexiones rechazadas. Esta politica no afecta el trafico forwardeado hacía el Internet.

Zona Origen	Zona Destino	Acción	Registrar en Logs	Description
loc	net	Rechazar (REJECT)	Sí	Rechazar el trafico originado por los hosts en la LAN con destino el Internet y registrar en los logs las conexiones rechazadas.
net	all	Rechazar Silenciosamente (DROP)	Sí	Rechazar silenciosamente todo el trafico originado en Internet con destino a cualquier host o red no definida en una regla o politica. Regla Catch-up para prevenir ataques desde el internet. Es altamente recomendado registrar en los logs este trafico.
all	all	Rechazar (REJECT)	Sí	Rechazar todo el trafico con origen y destino una zona no definida ni en una politica ni regla. Regla CATCHUP para bloquear absolutamente todo. Es altamente recomendado registrar en los logs este trafico.

En base a la tabla de politicas de filtrado descrita arriba podemos describir las politicas en Shorewall usando el archivo `/etc/shorewall/policy`.

```
#############################################################################
#SOURCE         DEST            POLICY          LOG     LIMIT:          CONNLIMIT:
#                                               LEVEL   BURST           MASK

# Politica de Trafico originado en el Internet (net) con destino el Firewall (fw)
net             fw              REJECT          $LOG
# Politica de Trafico originado en el Firewall (fw) con destino el Internet (net)
fw              net             REJECT          $LOG

# Politica de Trafico originado en el Firewall (fw) con destino la LAN (loc)
fw              loc             ACCEPT          $LOG
# Politica de Trafico originado en la LAN (loc) con destino el Firewall (fw)
loc             fw              REJECT          $LOG

# Politica de Trafico originado en la LAN (loc) con destino el Internet (net)
loc             net             REJECT          $LOG

#
net             all             DROP            $LOG    8/sec:30
# THE FOLLOWING POLICY MUST BE LAST
all             all             REJECT          $LOG
```

Para más información acerca del archivo `/etc/shorewall/policy` vea la página del manual **shorewall-policy(5)**.

Definiendo Reglas de filtrado en Shorewall

En shorewall las reglas son excepciones a la politica predeterminada descrita en el archivo `/etc/shorewall/policy`. Las reglas de firewall son descritas en el archivo `/etc/shorewall/rules` y como se explicó anteriormente, para cada petición de conexión que entra en el firewall, la petición es primero checada contra las reglas definidas en el archvo

`/etc/shorewall/rules`. Si ninguna regla hace coincidencia con la petición de la conexión entonces la primer politica en `/etc/shorewall/policy` que haga coincidencia es aplicada.

Por ejemplo, si su politica net2fw es **REJECT** y desea conectarte al firewall desde Internet usando el Secure Shell (SSH) y poder hacer pings desde el Internet al firewall. Recuerde que SSH usa el protocolo TCP con puerto 22, para permitir estas conexiones cree la regla en /etc/shorewall/rules.

Se aconseja documentar las reglas permitidas en el sistema firewall usando una tabla como la siguiente:

Tabla 8. Reglas de filtrado de tráfico del Firewall

Acción	Zona Origen	Zona Destino	Protocolo	Puerto origen	Puerto Destino	Descripción
PERMITIR	Internet	Firewall	TCP		22	Permitir TCP/SSH Desde el Internet hacia el Firewall
PERMITIR	Internet	Firewall	ICMP		8	Permitir Pings

> **Importante**
>
> El campo destinado para el puerto origen puede dejarse vacio, lo cual indica que se permite cualquier puerto, esto se deseable ya que la mayoría de aplicaciones usan un puerto origen aleatorio.

Las reglas del firewall estan enumeradas en el orden en que son creadas. En el firewall el trayecto que lleva un paquete al atravesar por el firewall es el siguiente:

El firewall recibe un paquete y examina su direccion IP origen y destino y lo asocia a una zona, también examina el puerto origen y destino, con esa informacion determina el protocolo para ese trafico. En ese momento el firewall iniciara al principio de las reglas (numero 1) y se ira hasta el final de las reglas. Cuando un paquete hace coincidencia con una regla especificada, se pueden aplicar las acciones ACCEPT, REJECT, DROP y opcionalmente se puede especificar que dicho trafico sea registrado en los logs.

En la mayoría de casos tendrá que crear las reglas en las sección **NEW** del archivo de conifguración `/etc/shorewall/rules`.

En shorewall las reglas se definen, por ejemplo:

```
...
...
...
#############################################################################
#    Reglas de acceso para conexiones Nuevas (Estado NEW)                   #
#############################################################################
SECTION NEW

#
#       Trafico originado en el Internet con destino el Firewall: net2fw
#
ACCEPT:$LOG     net                     fw                      tcp     22
# SSH
ACCEPT          net                     fw                      icmp    8
# Ping

#
#       Trafico originado en el Firewall con destino el Internet: fw2net
```

```
#
ACCEPT          fw                      net                     tcp     21
# FTP
ACCEPT          fw                      net                     tcp     22
# SSH
ACCEPT          fw                      net                     tcp     80
# HTTP
ACCEPT          fw                      net                     tcp     53
# DNS Queries
ACCEPT          fw                      net                     udp     53
# DNS Queries
ACCEPT          fw                      net                     udp     123
# NTP
ACCEPT          fw                      net                     icmp    8
# PING

#
#       Trafico originado en la red LOC con destino el Firewall: loc2fw
#
ACCEPT:info     loc                     fw                      tcp     22
# SSH
ACCEPT          loc                     fw                      tcp     80
# HTTP
ACCEPT          loc                     fw                      udp     53
# DNS Queries
ACCEPT          loc                     fw                      udp     123
# NTP
ACCEPT          loc                     fw                      icmp    8
# PING

#
#       Trafico originado en la red LOC con destino el Internet: loc2net
#
ACCEPT          loc                     net                     tcp     80
# HTTP
ACCEPT          loc                     net                     tcp     110
# POP3
ACCEPT          loc                     net                     tcp     143
# IMAP
ACCEPT          loc                     net                     tcp     443
# HTTPS
ACCEPT          loc                     net                     tcp     587
# SMTP SUbmission
ACCEPT          loc                     net                     tcp     993
# IMAP sobre SSL
ACCEPT          loc                     net                     tcp     995
# POP3 sobre SSL
ACCEPT          loc:$LOC_IP_GERENTES    net                     tcp     1863
# MSN Messenger
ACCEPT          loc                     net                     tcp     5223
# Jabber SSL/TLS

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

Asegurese de verificar su firewall desde el Internet usando algun tipo de Port Scanner y también probar las reglas de tráfico originado en su Red Local con destino el Internet para proteger la seguridad de la red interna.

Para más información y ejemplos de las reglas de shorewall vea el manual de *shorewall-rules(5)*.

Aplicando las reglas de firewall

Antes de aplicar las reglas de shorewall basadas en los archivos recien editados asegurese de usar el sub comando `check` del programa **shorewall(8)** para validar las configuraciones recien creadas, por ejemplo:

```
# shorewall check
Checking...
Checking /etc/shorewall/zones...
Checking /etc/shorewall/interfaces...
Determining Hosts in Zones...
Preprocessing Action Files...
   Pre-processing /usr/share/shorewall/action.Drop...
   Pre-processing /usr/share/shorewall/action.Reject...
Checking /etc/shorewall/policy...
Adding rules for DHCP
Checking Kernel Route Filtering...
Checking Martian Logging...
Checking MAC Filtration -- Phase 1...
Checking /etc/shorewall/rules...
Generating Transitive Closure of Used-action List...
Processing /usr/share/shorewall/action.Reject for chain Reject...
Processing /usr/share/shorewall/action.Drop for chain Drop...
Checking MAC Filtration -- Phase 2...
Applying Policies...
Shorewall configuration verified
```

Si las configuraciones fueron verificadas ahora incie shorewall con el parametro `start` del programa **shorewall(8)**, por ejemplo:

```
# shorewall start
Compiling...
Compiling /etc/shorewall/zones...
Compiling /etc/shorewall/interfaces...
Determining Hosts in Zones...
Preprocessing Action Files...
   Pre-processing /usr/share/shorewall/action.Drop...
   Pre-processing /usr/share/shorewall/action.Reject...
Compiling /etc/shorewall/policy...
Adding rules for DHCP
Compiling Kernel Route Filtering...
Compiling Martian Logging...
Compiling MAC Filtration -- Phase 1...
Compiling /etc/shorewall/rules...
Generating Transitive Closure of Used-action List...
Processing /usr/share/shorewall/action.Reject for chain Reject...
Processing /usr/share/shorewall/action.Drop for chain Drop...
Compiling MAC Filtration -- Phase 2...
Applying Policies...
Generating Rule Matrix...
Creating iptables-restore input...
Compiling iptables-restore input for chain mangle:...
Shorewall configuration compiled to /var/lib/shorewall/.start
Processing /etc/shorewall/params ...
Starting Shorewall....
Initializing...
Processing /etc/shorewall/init ...
Processing /etc/shorewall/tcclear ...
Setting up Route Filtering...
```

```
Setting up Martian Logging...
Setting up Proxy ARP...
Setting up Traffic Control...
Preparing iptables-restore input...
Running /sbin/iptables-restore...
Processing /etc/shorewall/start ...
Processing /etc/shorewall/started ...
done.
```

Si desea ver el estado de shorewall use el sub comando `status` del programa **shorewall(8)**, por ejemplo:

```
# shorewall status
Shorewall-4.4.7.5 Status at proxy.example.com - Sun Feb 28 16:04:48 CST 2010

Shorewall is running
State:Started (Sun Feb 28 16:03:28 CST 2010)
```

En este caso el mensaje **Shorewall is running** nos indica que las reglas de firewall fueron aplicadas.

Para más información acerca del comando **shorewall** vea la página del manual de *shorewall(8)*.

Desactivando las reglas de filtrado de Shorewall

Si desea desactivar por completo las reglas de filtrado y enrutado generadas por el script de Shorewall debe usar sub comando **clear** del programa **shorewall(8)**, por ejemplo:

```
# shorewall clear
Processing /etc/shorewall/params ...
Clearing Shorewall....
Processing /etc/shorewall/stop ...
Processing /etc/shorewall/tcclear ...
Running /sbin/iptables-restore...
Processing /etc/shorewall/stopped ...
Processing /etc/shorewall/clear ...
done.
```

Podemos ver que el cambio tomo efecto usando shorewall status:

```
# shorewall status
Shorewall-4.4.7.5 Status at proxy.example.com - Sun Feb 28 16:09:04 CST 2010

Shorewall is stopped
State:Cleared (Sun Feb 28 16:08:31 CST 2010)
```

Si alguna vez tiene problemas en el sistema y desea descartar cualquier problema relacionado a las reglas del firewall desactive shorewall con el sub comando **clear**.

Configurando el Enmascaramiento de IP (SNAT) en Shorewall

Si desea que los equipos en la red local salgan a Internet de forma segura deberá de activar el enmascaramiento de IP usando el metodo *Source NAT* (**SNAT**).

El enmascaramiento IP básciamente permite 3 cosas:

1. Proteger una red privada, en el caso de que las direcciones IP de la red privada (LAN) use direcciones en el rango 192.168.1.0/24, en Internet los hosts no sabrán que direcciones tienen

dichos hosts, ya que la dirección IP en los paquetes originados en la LAN con destino el Internet será enmascarada con la dirección IP publica asignada a la Interfaz WAN. Además sirve para permitir que las maquinas en la LAN puedan usar servicios en el Internet sin necesidad que cada una de las maquinas en la LAN tengan una dirección IP publica ruteable.

2. Hacer Port Forwarding, esta tecnica de NAT es usada para redirigir el trafico originado en Internet hacía un equpo en la LAN o DMZ.
3. NAT 1-to-1 o Static NAT: esta es una mezcla entre los dos tipos anteriores, en el caso que el firewall tenga más de una dirección IP publica y queramos dirigir todo el trafico hacía una de estas direcciónes a un equpo en la LAN o DMZ y que además todo el trafico originado en estos hosts con destino a Internet use como dirección IP origen la IP del NAT estatico.

Para activar el enmascaramiento primero debe de activar el re envio de paquetes (IP Forwarding) en el sistema, Shorewall permite activar el IP Forwarding desde el archivo de configuración principal definiendo el parametro `IP_FORWARDING` en el archivo `/etc/shorewall/shorewall.conf`.

> **Importante**
>
> En Debian/Ubuntu el IP Forwarding esta desactivado o configurado de forma que mantenga la configuración actual del sistema.

Para activar el IP Forwarding cambie el parametro `IP_FORWARDING` a On en el archivo `/etc/shorewall/shorweall.conf`, por ejemplo:

```
IP_FORWARDING=On
```

Adicionalmente debe de activar el enmascaramiento de las direcciones IP de la red subred local con la dirección IP de la interfaz de red asociada a la zona net en el archivo de configuración `/etc/shorewall/masq`, por ejemplo:

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

# Enmascaramos el tráfico originado por la subred local con destino el Internet
$NET_IF                 $LOC_SUBNET
```

Si el sistema firewall tiene más de una dirección IP publica, y desea que el trafico de loc2net sea enmascarado con una dirección IP pública en particular y no la principal, entonces agregue dicha dirección IP en la columna ADDRESS.

Por ejemplo, el firewall tiene la dirección IP principal 10.0.99.220 y la dirección IP 10.0.99.221 adicional, configuremos Shorewall para que el trafico sea enmascarado usando la dirección IP adicional editando el archivo `/etc/shorewall/masq` de la siguiente manera:

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

# Enmascaramos el tráfico originado por la subred local con destino el Internet
$NET_IF                 $LOC_SUBNET     10.0.99.221
```

Para que la dirección IP **10.0.99.221** se active automáticamente en la interfaz `NET_IF` debe activar el

soporte ADD_SNAT_ALIASES en el archivo /etc/shorewall/shorewall.conf, por ejemplo:

```
ADD_SNAT_ALIASES=Yes
```

Para aplicar el enmascaramiento verifique las configuraciones de Shorewall:

```
# shorewall check
Checking...
Checking /etc/shorewall/zones...
Checking /etc/shorewall/interfaces...
Determining Hosts in Zones...
Preprocessing Action Files...
   Pre-processing /usr/share/shorewall/action.Drop...
   Pre-processing /usr/share/shorewall/action.Reject...
Checking /etc/shorewall/policy...
Adding rules for DHCP
Checking Kernel Route Filtering...
Checking Martian Logging...
Checking /etc/shorewall/masq...
Checking MAC Filtration -- Phase 1...
Checking /etc/shorewall/rules...
Generating Transitive Closure of Used-action List...
Processing /usr/share/shorewall/action.Reject for chain Reject...
Processing /usr/share/shorewall/action.Drop for chain Drop...
Checking MAC Filtration -- Phase 2...
Applying Policies...
Shorewall configuration verified
```

Ahora re aplique las regla de firewall y enmascaramiento de IP.

```
# shorewall restart
Compiling...
Compiling /etc/shorewall/zones...
Compiling /etc/shorewall/interfaces...
Determining Hosts in Zones...
Preprocessing Action Files...
   Pre-processing /usr/share/shorewall/action.Drop...
   Pre-processing /usr/share/shorewall/action.Reject...
Compiling /etc/shorewall/policy...
Adding rules for DHCP
Compiling Kernel Route Filtering...
Compiling Martian Logging...
Compiling /etc/shorewall/masq...
Compiling MAC Filtration -- Phase 1...
Compiling /etc/shorewall/rules...
Generating Transitive Closure of Used-action List...
Processing /usr/share/shorewall/action.Reject for chain Reject...
Processing /usr/share/shorewall/action.Drop for chain Drop...
Compiling MAC Filtration -- Phase 2...
Applying Policies...
Generating Rule Matrix...
Creating iptables-restore input...
Compiling iptables-restore input for chain mangle:...
Shorewall configuration compiled to /var/lib/shorewall/.restart
Processing /etc/shorewall/params ...
   Shorewall is not running
Starting Shorewall....
Initializing...
Processing /etc/shorewall/init ...
```

```
Processing /etc/shorewall/tcclear ...
Setting up Route Filtering...
Setting up Martian Logging...
Setting up Proxy ARP...
Setting up Traffic Control...
Preparing iptables-restore input...
Running /sbin/iptables-restore...
IPv4 Forwarding Enabled
Processing /etc/shorewall/start ...
Processing /etc/shorewall/started ...
done.
```

Si desea controlar el tráfico originado en la red local hacía el Internet use las reglas para tráfico loc2net en el archivo `/etc/shorewall/rules` y `/etc/shorewall/policy`.

Configurando un Proxy HTTP Transparente en Shorewall

En esta sección describiremos el procedimiento para configurar Shorewall como Proxy HTTP Transparente (Interceptor), en donde en el mismo firewall se ejecuta un Proxy HTTP Squid escuchando en el puerto TCP 3128.

El proxy squid esta escuchando peticiones de los hosts en la red local en el puerto 3128, lo podemos ver en el parametro http_port del archivo de configuración de squid `/etc/squid/squid.conf`, por ejemplo:

```
http_port 3128
```

Para configurar el proxy transparente debemos configurar la regla para permitir que los hosts en la zona loc puedan acceder al puerto 3128 de la interfaz local del firewall, además, debemos permitir tráfico saliente desde el Firewall hacía el Internet ya que el proceso local squid debe acceder a sitios remotos usando el protocolo TCP/80, agregue las siguiente reglas en el archivo `/etc/shorewall/rules`:

```
#
#       Trafico originado en el Firewall (fw) con destino el Internet (net): fw2net
#
...
...
ACCEPT          fw                      net                     tcp     21
# FTP
ACCEPT          fw                      net                     tcp     80
# HTTP
...
...
...
#
#       Trafico originado en la LAN (loc) con destino el Firewall (fw)
#
...
ACCEPT          loc                     fw                      tcp     3128
# Squid Proxy HTTP
...
```

Ahora agregamos la que redireccionará todo el tráfico proveniente de la red local con destino el puerto TCP 80 en el Internet hacía el puerto 3128 local de squid:

```
#
#       Trafico originado en la LAN (loc) con destino el Internet (net): loc2net
```

```
#

# Proxy Transparente
REDIRECT        loc                     3128                    tcp     80
...
...
```

Tal vez sea necesario excluir algunos hosts destino o redes de la redirección, por ejemplo en el firewall se ejecuta un servidor web en el que se muestran gráficas de tráfico, para excluir la redirección del puerto TCP/80 hacía la dirección IP interna del firewall use la siguiente regla:

```
#
#       Trafico originado en la LAN (loc) con destino el Internet (net): loc2net
#

# Proxy Transparente
REDIRECT        loc                     3128                    tcp     80      -
!192.168.221.254
...
...
```

Si tiene algún servidor Web en la red interna y también desea agregarlo a la lista de destinos a excluir de la redirección puede usar una lista separada por comas, por ejemplo:

```
#
#       Trafico originado en la LAN (loc) con destino el Internet (net): loc2net
#

# Proxy Transparente
REDIRECT        loc                     3128                    tcp     80      -
!192.168.221.254,192.168.221.4
...
...
```

Para que el Squid funcione como Proxy Transparente con Shorewall debe tener configurado Squid cuando menos con los siguientes parametros:

```
http_port 3128 transparent

acl loc_subnet src 192.168.221.0/24
http_access allow loc_subnet
```

> **Nota**
>
> Estas configuraciones son para Squid 2.6 ó superior.

Recargue la configuración de shorewall para que los cambios tomen efecto:

```
# shorewall restart
```

Probablemente existe el requierimiento de excluir algunos sistemas internos de usar el proxy, es decir, hacer que esos sistemas vayan directo al Internet, para lograr dicha labor excluya la dirección IP del sistema interno en la regla y agregue una regla para permitir el acceso directo al puerto TCP/80 en el Internet:

```
ACCEPT          fw                      net                     tcp     80
REDIRECT        loc:!192.168.221.200    3128                    tcp     80      -
```

```
!192.168.221.254,192.168.221.4
ACCEPT          loc:192.168.221.200     net                     tcp     80
```

Recargue la configuración de shorewall para que los cambios tomen efecto.

Creando una regla de DNAT Port Forwarding en Shorewall

Es comun tener el requierimiento de acceder desde el Internet a algún servicio que se ejecuta en un sistema en la red privada, por ejemplo: una aplicación web, una conexión SSH a un servidor Linux interno o una conexión de escritorio remoto de Windows, este tipo de configuraciones en un Firewall se le suele llamar Port Forwarding o PAT (Port Address Translation), tecnicamente es un tipo de NAT en el cual se re direcciona el tráfico con destino uno o varios puertos en la interfaz de red WAN hacía uno o más puertos en un sistema en la red privada LAN.

Para crear una regla NAT de tipo Port Forwarding que en la terminología de Netfilter y Shorewall son reglas DNAT (Destination NAT) ya que re escriben el destino de la petición original agregue una regla como la siguiente:

```
DNAT     net                    loc:192.168.221.5:443    tcp     443
```

> **Importante**
>
> Para que esta regla funcione debe tener activado el soporte de `IP_FORWARDING` en `/etc/shorewall/shroweall.conf`.

La regla anterior dice algo así como, cualquiero petición de conexión originada en el Internet con destino al puerto TCP 443 en la dirección IP predeterminada del Firewall re dirigelo hacía el puerto TCP/443 del sistema en la red local con dirección IP 192.168.221.5.

También puede crear una regla DNAT usando un puerto diferente del lado del Internet, por ejemplo:

```
DNAT     net                    loc:192.168.221.5:22    tcp     3842
```

Si desea restringuir el acceso desde el Internet al servicio interno puede agregar la dirección del host remoto o red remota en la definición del origen net, por ejemplo:

```
DNAT     net:4.2.2.2            loc:192.168.221.5:443    tcp     443
```

La regla anterior dice algo así como, cualquiero petición de conexión originada en el Internet por el host 4.2.2.2 con destino al puerto TCP 443 en la dirección IP predeterminada del Firewall re dirigelo hacía el puerto TCP/443 del sistema en la red local con dirección IP 192.168.221.5.

Si tiene una dirección IP pública que desea reservar para las conexiones desde el exterior al servidor Web de la red interna puede crear una regla DNAT con un destino original difernte a la dirección IP pública del Firewall, por ejemplo:

```
DNAT     net                    loc:192.168.221.5:80     tcp     80     -
10.0.99.222
```

La regla anterior dice algo así como, cualquiero petición de conexión originada en el Internet con destino al puerto TCP/80 en la dirección IP 10.0.99.222 del Firewall re dirigelo hacía el puerto TCP/80 del sistema en la red local con dirección IP 192.168.221.5.

> **Importante**

Shorewall no agregará la dirección IP automáticamente ni al reiniciarlo, debe agregar un alias de IP a la interfaz `NET_IF` en `/etc/network/interfaces`.

Recargue la configuración de shorewall para que los cambios tomen efecto:

```
# shorewall restart
```

Este tipo de reglas es solo recomendado para un escenario simple, para un sistema más complejo y seguro se recomienda mover los servidores con servicios públicos a una Zona Desmilitarizada (DMZ) o use algún tipo de VPN para acceder a los servicios internos de forma segura.

Creando reglas NAT One-to-One en Shorewall

El Nat One-to-One es una manera de hacer que sistemas atrás del firewall y configurados con una dirección IP privada aparezcan como si tuvieran una dirección IP pública. Las reglas NAT One-to-One en realidad son una combinación de una regla DNAT y IP Masquerading.

En este caso vamos a configurar una regla NAT One-to-One para asignar una dirección IP pública dedicada para los servicios de correo electrónico hospedados en un servidor en la red privada, la regla NAT One-to-One que configuraremos hará lo siguiente:

- Todo el tráfico originado en el Internet dirigido a la dirección IP pública **10.0.99.223** sea re direccionado hacía el servidor SMTP con la dirección IP privada **192.168.221.4** (tal como una regla DNAT)
- Todo el tráfico originado en el servidor SMTP con la dirección IP privada con destino el Internet (incluyendo respuestas a peticiones desde el Internet) sea enmascarado con la dirección IP pública 10.0.99.221 (tal como una regla de SNAT)

Para configurar la regla NAT One-to-One descrita arriba edite el archivo de configuración `/etc/shorewall/nat` y agregue la siguiente línea:

```
#############################################################################
#EXTERNAL       INTERFACE       INTERNAL        ALL             LOCAL
#                                               INTERFACES
10.0.99.223     $NET_IF         192.168.221.4   no              no
```

Importante

Para que esta regla funcione debe tener activado el soporte de `IP_FORWARDING` en `/etc/shorewall/shroweall.conf`.

Esta regla solo realizará las tareas de re escribir la dirección IP origen y destino de los paquetes que coincidan con las peticiones, más sin embargo no permite ninguna conexión externa desde el Internet hacía el servidor de correos, para permitir el tráfico de los servicios de correo agregue las reglas en el archivo `/etc/shorewall/rules`, por ejemplo:

```
#############################################################################################
#########################################################
#ACTION         SOURCE                  DEST                    PROTO   DEST
SOURCE          ORIGINAL        RATE            USER/   MARK    CONNLIMIT
TIME
#                                                                       PORT
PORT(S)         DEST            LIMIT           GROUP
ACCEPT         net                     loc:192.168.221.4       tcp     443     -
```

```
10.0.99.223
ACCEPT          net                     loc:192.168.221.4       tcp     25      -
10.0.99.223
ACCEPT          net                     loc:192.168.221.4       tcp     587     -
10.0.99.223
ACCEPT          net                     loc:192.168.221.4       tcp     465     -
10.0.99.223
ACCEPT          net                     loc:192.168.221.4       tcp     110     -
10.0.99.223
ACCEPT          net                     loc:192.168.221.4       tcp     143     -
10.0.99.223
ACCEPT          net                     loc:192.168.221.4       tcp     993     -
10.0.99.223
ACCEPT          net                     loc:192.168.221.4       tcp     995     -
10.0.99.223
```

Para que la dirección IP **10.0.99.221** se active automáticamente en la interfaz `NET_IF` debe activar el soporte `ADD_IP_ALIASES` en el archivo `/etc/shorewall/shorewall.conf`, por ejemplo:

```
ADD_IP_ALIASES=Yes
```

Recargue la configuración de shorewall para que los cambios tomen efecto:

```
# shorewall restart
```

Este tipo de reglas es solo recomendado para un escenario simple, para un sistema más complejo y seguro se recomienda mover los servidores con servicios públicos a una Zona Desmilitarizada (DMZ).

Sobre el registro de eventos en Shorewall y Netfilter

Hay que hacer notar que shorewall por si solo no genera los logs del firewall, shorewall utiliza las funcionalidades de logs del subsistema Netfilter, el cual por default envía los logs al sistema syslog utilzando el facility *kern*, en Debian/Ubuntu dichos mensajes van al archivo de logs `/var/log/messages`. Este comportamiento tiene algunas limitaciones que se describen a continuación:

- Si pones, por ejemplo, *kern.info* en `/etc/syslog.conf` para redirigir los logs del firewall a un archivo diferente, esto tambien recibira mensajes de nivel 5 (notice) hasta 0 (emerg).
- Todos los mensajes de *kern.info* iran a su destino, y no solo los mensajes de Netfilter.

Shorewall permite el uso del target ULOG de iptables/netfilter, cuando ULOG es usado, Shorewall redireccionara los mensajes de Netfilter/iptables que usen el target ULOG a un proceso llamado **ulogd** y este escribira los registros por ejemplo en un archivo aparte, o en una base de datos, de esta forma tendremos un mejor control de los logs del sistema operativo y del firewall. En la siguiente sección se ve la integración de Shorewall y ulogd.

Configurando el registro de eventos con Shorewall y ulogd

Como se menciono en la sección anterior, en la configuracion predeterminada de shorewall, todos los eventos de conexiones rechazados o permitidos son registrados en el archivo de log `/var/log/messages`, esto significa que se mezclan mensajes generales del sistema, como mensajes del kernel u otros servicios. Para diferenciar los eventos del firewall, se recomienda instalar el programa ulogd, el cual se encarga de recibir los mensajes del firewall, mejor dicho, los mensajes de

registro de LOG del firewall y los manda a un archivo individual, por ejemplo: `/var/log/firewall.log` el cual será mantenido de forma independiente a los logs del demonio syslog.

Si deseamos enviar los logs de iptables/netfilter a un archivo independiente y no usar el sistema syslog instalaremos el servicio ulogd para dirigir los logs al archivo `/var/log/firewall.log`.

Instalamos ulogd:

```
# aptitude install ulogd
```

Ahora editamos el archivo de configuración de ulogd `/etc/ulogd.conf` para permitir la carga del plugin **ulogd_LOGEMU** e indicarle en que archivo escribir los logs:

```
...
plugin="/usr/lib/ulogd/ulogd_LOGEMU.so"

[LOGEMU]
file="/var/log/firewall.log"
sync=1
```

Ahora reinicie el demonio ulogd para que los ambios tomen efecto:

```
# invoke-rc.d ulogd restart
```

Indiquemos a shorewall que los mensajes del firewall estan en el archivo `/var/log/firewall.log` usando el parametro `LOGFILE` del archivo de configuración `/etc/shorewall/shorewall.conf`.

```
LOGFILE=/var/log/firewall.log
```

El parametro `LOGFILE=/var/log/firewall.log` le dice al programa **shorewall(8)** donde buscar los logs del firewall para cuando se usen los comandos **show log** y/o **logwatch**.

También debemos de configurar los parametros `TCP_FLAGS_LOG_LEVEL` y `SMURF_LOG_LEVEL` para que usen el target ULOG.

```
TCP_FLAGS_LOG_LEVEL=$LOG

SMURF_LOG_LEVEL=$LOG
```

Ahora cambie el valor de la variable de shell LOG en el archivo `/etc/shorewall/params` para que ahora apunte al tarjeta ULOG, por ejemplo:

```
LOG=ULOG
```

Ahora reinicie Shorewall para que los cambios tomen efecto y los logs del firewall se empiecen a escribir en el archivo `/var/log/firewall.log`.

```
# shorewall restart
```

Ahora puede hacer una prueba haciendo telnet a un servicio externo el cual no este permitido, por ejemplo:

```
# telnet 4.2.2.2
Trying 4.2.2.2...
```

```
telnet: Unable to connect to remote host: Connection refused
```

Y vea el evento registrado en el log `/var/log/firewall.log`.

```
# tail /var/log/firewall.log
Feb 28 16:56:41 fwproxy Shorewall:fw2net:REJECT: IN= OUT=eth1 MAC= SRC=10.0.99.220
DST=4.2.2.2
 LEN=60 TOS=10 PREC=0x00 TTL=64 ID=47678 CE DF PROTO=TCP SPT=51691 DPT=23
 SEQ=4142977104 ACK=0 WINDOW=5840 SYN URGP=0
```

Ahora debemos de crear o personalizar el archivo de logrotate de ulogd para que los logs tanto del proceso ulogd `/var/log/ulog/ulogd.log` y del firewall `/var/log/firewall.log` sean rotados periodicamente.

Edite el archivo `/etc/logrotate.d/ulogd` par que quede de la siguiente forma:

```
/var/log/ulog/ulogd.log /var/log/firewall.log  {
    missingok
    sharedscripts
    create 640 root adm
    postrotate
        /etc/init.d/ulogd reload
    endscript
}
```

Ahora si puede usar el legendario tail para monitorizar los logs del firewall, por ejemplo:

```
# tail -f /var/log/firewall.log
```

Se recomienda usar Multitail para monitorizar los logs del firewall usando un esquema de coloreado de logs con muchas otras capacidades para la monitorización de logs.

Instalando Multitail para monitorización y coloreado de Logs de firewall

Instalaremos el paquete multitail:

```
# aptitude install multitail
```

Edite el archivo /etc/multitail.conf para personalizar el esquema de coloreado para los logs del firewall, al final agregue:

```
#
# Shorewall: Linux iptables firewall
#
colorscheme:shorewall:Linux IPtables (2.6.x kernel)
cs_re:cyan::
cs_re:blue:^... .. ..:..:..
cs_re_s:red:Shorewall.*: .*(DPT=[0-9]*)
cs_re_s:yellow:Shorewall.*: (IN=[^ ]*)
cs_re_s:magenta:Shorewall.*: .*(OUT=[^ ]*)
cs_re_s:cyan:Shorewall.*: .*(SRC=[^ ]*)
cs_re_s:red:Shorewall.*: .*(DST=[^ ]*)
cs_re_s:green:Shorewall.*: .*(PROTO=[^ ]*)
cs_re_s:green:Shorewall:.*:.*(ACCEPT)
cs_re_s:red:Shorewall:.*:.*(REJECT)

# FIREWALL
cs_re_s:blue:Shorewall:.*(fw2net)
```

```
cs_re_s:blue:Shorewall:.*(fw2loc)
cs_re_s:blue:Shorewall:.*(fw2dmz)
cs_re_s:blue:Shorewall:.*(fw2vpn)

# LOC
cs_re_s:blue:Shorewall:.*(loc2fw)
cs_re_s:blue:Shorewall:.*(loc2net)
cs_re_s:blue:Shorewall:.*(loc2dmz)
cs_re_s:blue:Shorewall:.*(loc2vpn)

# DMZ
cs_re_s:blue:Shorewall:.*(dmz2fw)
cs_re_s:blue:Shorewall:.*(dmz2net)
cs_re_s:blue:Shorewall:.*(dmz2loc)
cs_re_s:blue:Shorewall:.*(dmz2vpn)

# VPN
cs_re_s:blue:Shorewall:.*(vpn2fw)
cs_re_s:blue:Shorewall:.*(vpn2net)
cs_re_s:blue:Shorewall:.*(vpn2loc)
cs_re_s:blue:Shorewall:.*(vpn2dmz)

# NET
cs_re_s:red:Shorewall:.*(net2fw)
cs_re_s:red:Shorewall:.*(net2loc)
cs_re_s:red:Shorewall:.*(net2dmz)
cs_re_s:red:Shorewall:.*(net2all)
```

Antes de poder usar multitail con este esquema se recomienda crear un archivo de configuración para el control de ejecución de multitail para el usuario root para desactivar el chequeo de correos.

```
# echo "check_mail:0" >> ~/.multitailrc
```

Ahora puede ejecutar el comando multitail con el esquema shorewall, por ejemplo:

```
# multitail -cS shorewall -i /var/log/firewall.log
```

Usando multitail y el esquema shorewall los logs del firewall se deben de ver algo así:

Figura 3. Multitail Shorewall Logs

Si lo desea, puede crear un alias del shell para facilitar la monitorización de los logs, edite el archivo de alias del shell bash, por ejemplo:

```
# vim ~/.bash_aliases
```

Agregue el alias fwlogs:

```
# Firewall Shorewall logs
alias fwlogs='multitail -cS shorewall -i /var/log/firewall.log'
```

Para que los alias definidos en el archivo `~/.bash_aliases` sean creados al inicio de sesión edite el ~/.bashrc:

```
# vim ~/.bashrc
```

Y descomente el bloque **if** que hace source al archivo `~/.bash_aliases`:

```
# Alias definitions.
# You may want to put all your additions into a separate file like
# ~/.bash_aliases, instead of adding them here directly.
# See /usr/share/doc/bash-doc/examples in the bash-doc package.

if [ -f ~/.bash_aliases ]; then
    . ~/.bash_aliases
fi
```

Ahora re inicie la sesión o haga source del archivo `~/.bashrc` para cargar los nuevos aliases:

```
# . ~/.bash_aliases
```

Y use el alias **fwlogs** para sus tareas rutinarias de monitorización de logs.

Usando iftop para monitorizar el uso del ancho de banda

Es impoirtante que monitorice constantemente el uso del ancho de banda, ya sea de conexiones entrantes o salientes, un ejemplo, checar que los usuarios no consuman todo el ancho de banda en descargas de Internet.

Instale el paquete iftop:

```
# apt-get install iftop
```

Creamos 3 archivos de configuración para el control de la ejecución de iftop, cada configuración monitorizará el tráfico asociado a las zonas.

Creamos archivo de configuración para tráfico loc2net `~/.iftoprc.loc2net`:

```
interface: eth0
#dns-resolution: yes
port-resolution: yes
#show-bars: yes
port-display: on
use-bytes: yes
#show-totals: yes
max-bandwidth: 2M
#filter-code: not dst host 192.168.221.1
filter-code: not port 53 and not port 22
```

Ahora use el programa iftop así para monitorizar el tráfico de la red local hacía el Internet.

```
# iftop -c /root/.iftoprc.lan2net
```

La interfaz de iftop se verá algo así:

Figura 4. Iftop tráfico loc2net

Creamos archivo de configuración para tráfico fw2net `~/.iftoprc.fw2net`:

```
interface: eth1
#dns-resolution: yes
port-resolution: yes
```

```
#show-bars: yes
port-display: on
use-bytes: yes
#show-totals: yes
max-bandwidth: 2M
#filter-code: not dst host 192.168.221.1
#filter-code: not port 53 and not port 22
```

Ahora use el programa iftop así para monitorizar el tráfico de la red local hacía el Internet.

```
# iftop -c /root/.iftoprc.fw2net
```

Puede crear un alias en el archivo `~/.bash_aliases`:

```
# Monitoreo trafico y ancho de banda
alias iftop-loc2net="iftop -c /root/.iftoprc.loc2net"
alias iftop-fw2net="iftop -c /root/.iftoprc.fw2net"
```

Haga source al archivo `~/.bash_aliases` para detectar los aliases.

Administración del firewall Shorewall

En esta sección veremos las operaciones de administración más comunes de un firewall Shorewall en Ubuntu Server.

Verificando la configuración de Shorewall

Cuando modifique los archivos de configuración de Shorewall siempre es recomendable verificar que los archivos no contienen errores de sintaxis, use el sub comando check para verificar las configuraciones:

```
# shorewall check
```

Si las configuraciones estan bien entonces verá el mensaje **Shorewall configuration verified** el cual le indica que las configuraciones están bien, y puede ejecutar el comando requerido para aplicar las nuevas reglas, de lo contrario corriga el error.

Controlando la ejecución de Shorewall

En esta sección veremos los comandos para controlar la ejecución de Shorewall.

Iniciando Shorewall

Cuando se ejecuta el programa shorewall con el parametro start Shorewall compila las reglas generadas a partir de los archivos de configuración y genera un script para ser ejecutado, una vez que el script fué ejecutado shorewall termino su trabajo, es decir, no hay ningun demonio llamado shorewall, entonces el filtrado es realizado por el subsistema de filtrado Netfilter del kernel de Linux.

Use el comando shorewall start para inicializar el confunto de reglas de filtrado y configuraciones de enrutado básico en el sistema.

```
# shorewall start
```

Si el comando devuelve el mensaje **done.** significa que el script se compilo correctamente y las reglas

fueron aplicadas.

Para mayor seguridad al iniciar el firewall use el sub comando **safe-start**.

Activando el firewall Shorewall al inicio del sistema

Para que las reglas del firewall Shorewall sean aplicadas al inicio del sistema de forma automática edite el archivo `/etc/default/shorewall` y cambie el valor del parametro `startup` a **1**, por ejemplo:

```
startup=1
```

El instalador de shorewall configuro el sistema para que shorewall sea iniciado automáticamente siempre y cuando el parametro startup en el archivo `/etc/default/shorewall` este en 1.

Deteniendo Shorewall

Se desea detener las reglas del firewall puede usar el sub comando stop, por ejemplo:

```
# shorewall stop
```

El comando stop detiene el firewall. Todas las conexiones existentes son rechazadas, excepto aquelas listadas en `/etc/shorewall/routestopped` o permitidas por la opción `ADMINISABSENTMINDED` en el archivo de configuración /etc/shorewall/shorewall.conf. El único tráfico nuevo permitido a través del firewall is de sistemas listados en `/etc/shorewall/routestopped` o permitidas por la opción `ADMINISABSENTMINDED` la cual permite que las conexiones activas en el momento en el que Shorewall se detuvo continuarán trabajando así como las nuevas conexiones originadas en el firewall y tráfico DHCP si es que la opción dhcp se uso en alguna interfaz.

El formato del archivo `/etc/shorewall/routestopped` es el siguiente:

TODO

Re iniciando Shorewall

Si modifico las reglas o politicas del firewall debe de reiniciar o recargar las reglas usando el sub comando **restart**, recuerde siempre ejecutar **shorewall check** antes de aplicar cambios a las reglas del firewall.

```
# shorewall restart
```

Para mayor seguridad use el sub comando **safe-restart**.

Desactivando Shorewall

Si desea desactivar por completo las reglas de filtrado y enrutado generadas por el script de Shorewall debe usar sub comando **clear** del programa **shorewall(8)**, por ejemplo:

```
# shorewall clear
Processing /etc/shorewall/params ...
Clearing Shorewall....
Processing /etc/shorewall/stop ...
Processing /etc/shorewall/tcclear ...
Running /sbin/iptables-restore...
```

```
Processing /etc/shorewall/stopped ...
Processing /etc/shorewall/clear ...
done.
```

Podemos ver que el cambio tomo efecto usando **shorewall status**.

Iniciando y Re iniciando Shorewall de forma segura

Re iniciar Shorewall usando el sub comando shorewall restart algunas veces puede ser algo arriesgado si llega a cometer algun error en las reglas de filtrado, un problema común es que rechace el tráfico de SSH y ya no pueda acceder al sistema de forma remota.

Shorewall provee los sub comandos safe-start y safe-restart para re iniciar el firewall de forma segura. Estos sub comandos verifican y aplican las nuevas reglas solo si usted las aprueba explicitamente precionando Y en el shell, por ejemplo:

```
# shorewall safe-restart
Compiling...
Compiling /etc/shorewall/zones...
Compiling /etc/shorewall/interfaces...
Determining Hosts in Zones...
Preprocessing Action Files...
   Pre-processing /usr/share/shorewall/action.Drop...
   Pre-processing /usr/share/shorewall/action.Reject...
Compiling /etc/shorewall/policy...
Adding rules for DHCP
Compiling Kernel Route Filtering...
Compiling Martian Logging...
Compiling /etc/shorewall/masq...
Compiling MAC Filtration -- Phase 1...
Compiling /etc/shorewall/rules...
Generating Transitive Closure of Used-action List...
Processing /usr/share/shorewall/action.Reject for chain Reject...
Processing /usr/share/shorewall/action.Drop for chain Drop...
Compiling MAC Filtration -- Phase 2...
Applying Policies...
Generating Rule Matrix...
Creating iptables-restore input...
Compiling iptables-restore input for chain mangle:...
Shorewall configuration compiled to /var/lib/shorewall/.start
Starting...
Processing /etc/shorewall/params ...
Starting Shorewall....
Initializing...
Processing /etc/shorewall/init ...
Processing /etc/shorewall/tcclear ...
Setting up Route Filtering...
Setting up Martian Logging...
Setting up Proxy ARP...
Setting up Traffic Control...
Preparing iptables-restore input...
Running /sbin/iptables-restore...
Setting up dynamic rules...
IPv4 Forwarding Enabled
Processing /etc/shorewall/start ...
Processing /etc/shorewall/started ...
done.
Do you want to accept the new firewall configuration? [y/n] y
```

```
New configuration has been accepted
```

Si por alguna razón se bloquea la comunicación SSH con el firewall y no puede presionar y en los próximos **60 segundos** entonces Shorewall usará las reglas que aplico en el último start o restart.

SI no aprobo los cambios entonces podrá volver a conectarse al firewall y corregir los cambios.

Mostrando información relevante del firewall Shorewall

Mostrando la versión de Shorewall:

```
# shorewall version
4.4.7.5
```

Mostrando los capacidades del firewall:

```
# shorewall show capabilities
Shorewall has detected the following iptables/netfilter capabilities:
   NAT: Available
   Packet Mangling: Available
   Multi-port Match: Available
   Extended Multi-port Match: Available
   Connection Tracking Match: Available
   Extended Connection Tracking Match Support: Not available
   Old Connection Tracking Match Syntax: Not available
   Packet Type Match: Available
   Policy Match: Available
   Physdev Match: Available
   Physdev-is-bridged Support: Available
   Packet length Match: Available
   IP range Match: Available
   Recent Match: Available
   Owner Match: Available
   Ipset Match: Not available
   CONNMARK Target: Available
   Extended CONNMARK Target: Available
   Connmark Match: Available
   Extended Connmark Match: Available
   Raw Table: Available
   IPP2P Match: Not available
   CLASSIFY Target: Available
   Extended REJECT: Available
   Repeat match: Available
   MARK Target: Available
   Extended MARK Target: Available
   Extended MARK Target 2: Not available
   Mangle FORWARD Chain: Available
   Comments: Available
   Address Type Match: Available
   TCPMSS Match: Available
   Hashlimit Match: Available
   Old Hashlimit Match: Available
   NFQUEUE Target: Available
   Realm Match: Available
   Helper Match: Available
   Connlimit Match: Not available
   Time Match: Not available
   Goto Support: Available
   LOGMARK Target: Not available
```

```
   IPMARK Target: Not available
   LOG Target: Available
   Persistent SNAT: Not available
   TPROXY Target: Not available
   FLOW Classifier: Not available
```

Mostrando el estado de ejecución de Shorewall:

```
# shorewall status
Shorewall-4.4.7.5 Status at proxy.example.com - Sun Feb 28 21:56:52 CST 2010

Shorewall is running
State:Started (Sun Feb 28 16:56:22 CST 2010)
```

Mostrando las zonas:

```
# shorewall show zones
Shorewall 4.4.7.5 Zones at proxy.example.com - Mon Mar  1 01:36:55 CST 2010

fw (firewall)
net (ipv4)
   eth1:0.0.0.0/0!192.168.221.0/24
loc (ipv4)
   eth0:192.168.221.0/24
   eth0:224.0.0.0/4
```

Mostrando las politicas de filtrado:

```
# shorewall show policies
Shorewall 4.4.7.5 Policies at proxy.example.com - Sun Feb 28 21:55:57 CST 2010

fw      =>      net     REJECT using chain fw2net
fw      =>      loc     ACCEPT using chain fw2loc
net     =>      fw      REJECT using chain net2fw
net     =>      loc     DROP using chain net2loc
loc     =>      fw      REJECT using chain loc2fw
loc     =>      net     REJECT using chain loc2net
```

Mostrando la información de red TCP/IP:

```
# shorewall show ip
Shorewall 4.4.7.5 IP at proxy.example.com - Sun Feb 28 21:46:29 CST 2010

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    inet 127.0.0.1/8 scope host lo
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    inet 192.168.221.254/24 brd 192.168.221.255 scope global eth0
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    inet 10.0.99.220/24 brd 10.0.99.255 scope global eth1
```

Mostrando las conexiones establecidas:

```
# shorewall show connections
Shorewall 4.4.7.5 Connections (5 out of 8192) at proxy.example.com - Sun Feb 28
21:58:21 CST 2010

udp      17 3 src=10.0.99.220 dst=201.155.229.129 sport=123 dport=123 packets=1
bytes=76
 src=201.155.229.129 dst=10.0.99.220 sport=123 dport=123 packets=1 bytes=76 mark=0
```

```
secmark=0 use=1
tcp      6 431999 ESTABLISHED src=10.0.99.199 dst=10.0.99.220 sport=58485 dport=22
packets=9370 bytes=701623
 src=10.0.99.220 dst=10.0.99.199 sport=22 dport=58485 packets=6382 bytes=1093776
[ASSURED] mark=0 secmark=0 use=1
udp      17 29 src=10.0.99.5 dst=255.255.255.255 sport=68 dport=67 packets=20
bytes=6560
 [UNREPLIED] src=255.255.255.255 dst=10.0.99.5 sport=67 dport=68 packets=0 bytes=0
mark=0 secmark=0 use=1
udp      17 26 src=10.0.99.3 dst=255.255.255.255 sport=68 dport=67 packets=19
bytes=6232
 [UNREPLIED] src=255.255.255.255 dst=10.0.99.3 sport=67 dport=68 packets=0 bytes=0
mark=0 secmark=0 use=1
udp      17 27 src=10.0.99.6 dst=255.255.255.255 sport=68 dport=67 packets=23
bytes=7544
 [UNREPLIED] src=255.255.255.255 dst=10.0.99.6 sport=67 dport=68 packets=0 bytes=0
mark=0 secmark=0 use=1
```

Mostrando los hits:

```
# shorewall hits
Shorewall 4.4.7.5 Hits at proxy.example.com - Sun Feb 28 21:59:45 CST 2010

   HITS IP              DATE
   ---- --------------- ------
      7 10.0.99.220     Feb 28

   HITS IP              PORT
   ---- --------------- -----
      7 10.0.99.220     23

   HITS DATE
   ---- ------
      7 Feb 28

   HITS  PORT SERVICE(S)
   ---- ----- ----------
      7    23 telnet
```

Para más información del comando shorweall vea el manual de *shorewall(8)*.

Recursos adicionales

Para obtener más información, consulte los siguientes recursos:

- Sitio oficial Netfilter/IPTables:

  http://www.netfilter.org/
- Sitio oficial Shorewall

  http://shorewall.net/
- Pagina del manual
  - iptables(8)
  - shorewall(8)
  - shorewall.conf(5)

- shorewall-params(5)
- shorewall-zones(5)
- shorewall-interfaces(5)
- shorewall-policy(5)
- shorewall-rules(5)
- shorewall-masq(5)
- shorewall-nat(5)
- ulogd(8)
- multitail(1)

- Introducción a Shorewall:
  http://shorewall.net/Introduction.html
- Shorewall QuickStart Guides (HOWTOs):
  http://shorewall.net/shorewall_quickstart_guide.htm
- Configuration Files Tips and Hints:
  http://shorewall.net/configuration_file_basics.htm
- Shorewall FAQs:
  http://www.shorewall.net/FAQ.htm
- Shorewall - Kernel Configuration
  http://www.shorewall.net/kernel.htm
- Shorewall - Requirements
  http://www.shorewall.net/shorewall_prerequisites.htm
- Using Shorewall with Squid
  http://www.shorewall.net/Shorewall_Squid_Usage.html
- Shorewall One-to-one NAT
  http://www.shorewall.net/NAT.htm
- Página del Projecto ulogd en Netfilter
  http://netfilter.org/projects/ulogd/index.html
- Canal de soporte en la red IRC:
  #shorewall at freenode.net
- IPTables Tutorial por Oskar Andreasson
  http://www.frozentux.net/documents/iptables-tutorial/
- NIST Firewall Guide and Policy Recommendations - Guidelines on Firewalls and Firewall Policy
  http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf