Instalación de Shorewall Firewall en Ubuntu (2 Interfaces)

En este tutorial se va a instalar Shorewall que es un potente Firewall (o mejor dicho interfaz para configurar el netfilter) para Linux, no solo funciona para Ubuntu sino para cualquier linux, solo que en este tutorial solo se va a instalar para estas 2 distribuciones.

La configuración que se va a realizar es para el caso de una computadora con dos interfaces de red .

Esta instalación está dirigida a Ubuntu tanto las versiones de Desktop como de Server.

Instalación de Shorewall 4.0

Shorewall viene incluido en los repositorios oficiales de Ubuntu por lo que para instalarlo ejecutamos:

```
# apt-get install shorewall shorewall-perl
```

Configuración de Shorewall para dos Interfaces

Una vez finalizada la instalación procedemos a cambiar la configuración.

Shorewall trae ficheros de configuración de ejemplo para 1,2 y hasta 3 interfaces en **/usr/share/doc/shorewall-common/examples/** que debemos copiar a la carpeta **/etc/shorewall** para esto ejecutamos los siguientes comandos (en este tutorial solo copiaremos los de dos interfaces):

```
# cd /usr/share/doc/shorewall/examples/two-interfaces

# cp -p interfaces rules zones policy masq routestopped /etc/shorewall
```

> **Nota:** Utilizamos la opción **-p** de copy para que se mantengan todos los privilegios de los archivos para más información consulta man cp.

Ahora que ya tenemos nuestros archivos de configuración base vamos a modificarlos:

Habilitar el enmascaramiento (SNAT)

Normalmente los equipos de la red local tienen Ips privadas y acceden a Internet utilizando todos una única IP pública del enrutador utilizando el mecanismo de enmascaramiento o SNAT.

Para habilitar el enmascaramiento mediante Shorewall debemos editar el fichero /etc/shorewall/masq y dejarlo de la siguiente forma:

```
#INTERFACE          SOURCE          ADDRESS          PROTO    PORT(S) IPSEC    MARK
eth0                eth1
```

En donde la primera columna (eth0) indica a través de que interfaz se hace el enmascaramiento y la segunda (eth1) donde están conectados los equipos cuya IP hay que enmascarar

Shorewall Zones

El primer archivo de configuración que vamos a modificar es el de zones (**/etc/shorewall/zones**).

Shorewall ve la red donde se encuentra como un conjunto de **zonas**, para el caso de dos interfaces de red que estamos haciendo vamos a tener tres zonas (la red local, Internet y el propio Firewall).

Primero ejecutamos el siguiente comando:

```
# nano /etc/shorewall/zones
```

Se verificara el archivo que tiene la linea de loc ipv4 net ipv4 justo después de fw firewall debe verse como el archivo que a continuación se muestra, ya los ejemplos lo traen por eso solo se va a verificar:

```
# Shorewall version 4.0 - Sample Zones File for two-interface configuration.
# Copyright (C) 2006 by the Shorewall Team
#
# This library is free software; you can redistribute it and/or
# modify it under the terms of the GNU Lesser General Public
# License as published by the Free Software Foundation; either
# version 2.1 of the License, or (at your option) any later version.
#
# See the file README.txt for further details.
#------------------------------------------------------------------------------
# For information about entries in this file, type "man shorewall-zones"
#
# The manpage is also online at
# http://shorewall.net/manpages/shorewall-zones.html
#
###############################################################################
#ZONE   TYPE    OPTIONS                 IN                      OUT
#                                       OPTIONS                 OPTIONS
fw      firewall
net     ipv4
loc     ipv4

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

Shorewall Interfaces

Ahora vamos a obtener el nombre de la interfaz externa (la que se conecte hacia internet) ejecutando el siguiente comando:

```
ip route ls
```

y obtendrás algo como esto:

```
192.168.1.0/24 dev eth0  proto kernel  scope link  src 192.168.1.9

192.168.10.0/24 dev eth1  proto kernel  scope link  src 192.168.10.1

default via 192.168.1.1 dev eth0  metric 100
```

Por supuesto que la dirección IP de tu computadora puede ser distinta al igual que el nombre de la interfaz en este caso eth0. Fijense que la **interfaz externa** viene dado por la línea **default via** 192.168.1.1 dev **eth0**.

Con esta información sabemos que la interfaz que me da acceso externo es eth0 (zona net) y la que me conecta a la red interna (loc) es eth1. Procederemos a modificar el archivo /etc/shorewall/interfaces, ejecutamos el siguiente comando:

```
#nano /etc/shorewall/interfaces
```

Y agregamos las siguientes líneas

```
#ZONE   INTERFACE       BROADCAST       OPTIONS
```

```
net     eth1            detect          dhcp,tcpflags,logmartians,nosmurfs,blacklist,routeback
loc     eth0            detect          tcpflags,logmartians,blacklist,routeback,nosmurfs
```

- ZONE: Aquí definimos la zona a la cual va a pertenecer la interfaz que vamos a definir, en este caso la zona es net que ya definimos anteriormente
- INTERFACE: El nombre de la interfaz
- BROADCAST: Es opcional. Aquí definimos que queremos que haga el Shorewall con los paquetes de Broadcast en este caso con la opción detect le decimos que detecte las direcciones de broadcast por nosotros. También podríamos colocar aquí la dirección IP de broadcast de nuestra red.
- OPTIONS: Esta es la parte más extensa, así que explicaré las opciones utilizadas aquí.
    - dhcp: Esta opción se debe colocar **si tu computadora obtiene su dirección IP vía DHCP, o si tu firewall está instalado en un servidor DHCP**.
    - tcpflags: Esta opción hace que Shorewall revise los paquetes por combinaciones ilegales de FLAGS (o banderas) TCP. Nunca está de más tenerlo.
    - logmartians: Esta opción hace que Shorewall registre paquetes con direcciones de origen imposibles, para esto tenemos que tener habilitado el routefilter en la interfaz lo cual veremos más adelante como hacerlo.
    - nosmurfs: Filtra paquetes smurfs (paquetes que tienen como dirección de origen una dirección de broadcast)
    - blacklist: Analiza los paquetes contra la lista negra que definiremos más adelante en el archivo blacklist del shorewall
    - routeback:Permite que Shorewall filtre paquetes que se devuelven a esta misma interfaz

Con esto el archivo de interfaces esta listo, lo guardamos y seguimos con la configuración.

Nota: Para más información del archivo de interfaces y sus opciones pueden ejecutar man shorewall-interfaces

Shorewall Policy

Aqui vamos a definir unas políticas que determina como Shorewall maneja la conexión entre las distintas zonas. Es de destacar que las instrucciones se ejecutan de arriba a abajo por lo que es importante mantener el orden para que se ejecuten adecuadamente.

Vamos a modificar el archivo de políticas que se encuentra **/etc/shorewall/policy** ejecutando el siguiente comando:

```
# nano /etc/shorewall/policy
```

Y lo modificamos para que quede así:

```
# Shorewall version 4.0 - Sample Policy File for two-interface configuration.
# Copyright (C) 2006 by the Shorewall Team
#
# This library is free software; you can redistribute it and/or
# modify it under the terms of the GNU Lesser General Public
# License as published by the Free Software Foundation; either
# version 2.1 of the License, or (at your option) any later version.
#
# See the file README.txt for further details.
#------------------------------------------------------------------------------
# For information about entries in this file, type "man shorewall-policy"
#
# The manpage is also online at
# http://shorewall.net/manpages/shorewall-policy.html
```

```
#
#############################################################################
loc             net             ACCEPT
net             all             DROP            info
# THE FOLLOWING POLICY MUST BE LAST
all             all             REJECT          info
```

Lo que estamos diciendo aquí es que por defecto permitimos el tráfico desde la red local hay Internet y que ignoramos (DROP) o rechazamos (REJECT) el resto del tráfico.

Para más información pueden buscar las páginas de manual ejecutando man shorewall-policy.

Shorewall Rules

Las reglas sirven para agregar excepciones a las políticas que declaramos anteriormente, si dejamos las politicas como están sin agregar ninguna regla pues no podremos ni siquiera navegar así que vamos a modificar el archivo de rules ejecutando:

```
# nano /etc/shorewall/rules
```

Y lo modificamos para que quede así:

```
#
# Shorewall version 4.0 - Sample Rules File for two-interface configuration.
# Copyright (C) 2006,2007 by the Shorewall Team
#
# This library is free software; you can redistribute it and/or
# modify it under the terms of the GNU Lesser General Public
# License as published by the Free Software Foundation; either
# version 2.1 of the License, or (at your option) any later version.
#
# See the file README.txt for further details.
#------------------------------------------------------------------------------
# For information about entries in this file, type "man shorewall-rules"
#
# The manpage is also online at
# http://shorewall.net/manpages/shorewall-rules.html
#
###############################################################################
#################################
#ACTION         SOURCE          DEST            PROTO   DEST    SOURCE
ORIGINAL        RATE            USER/   MARK
#                                                       PORT    PORT(S)
DEST            LIMIT           GROUP
#
#       Accept DNS connections from the firewall to the network
#
DNS/ACCEPT      $FW             net
#
#       Accept SSH connections from the local network for administration
#
SSH/ACCEPT      loc             $FW
#
#       Allow Ping from the local network
#
Ping/ACCEPT     loc             $FW

#
# Drop Ping from the "bad" net zone.. and prevent your log from being flooded..
#
```

```
Ping/DROP       net             $FW

ACCEPT          $FW             loc             icmp
ACCEPT          $FW             net             icmp
#

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

Los nombres como Ping, SSH, etc nos describe el protocolo sobre el que vamos a efectuar la acción que puede ser ACCEPT. REJECT, DROP **entre otras**. Shorewall cuenta con varios MACROS, los MACROS no son más que reglas prehechas que estamos utilizando aquí como Ping, SSH, DNS, etc. Para ver una lista completa de los macros puedes ejecutar *shorewall show macros*.

Un ejemplo de regla definida mediante macros es:

```
DNS/ACCEPT      $FW             net
```

Primero ponemos el tipo de servicio y la acción, en este caso aceptamos peticiones de DNS. Luego ponemos el **origen** que en este caso es la zona **$FW** y luego colocamos el **destino** que es la zona **net**. Para la regla del ejemplo estamos permitiendo las peticiones de DNS del firewall hacia servidores de DNS que están en Internet.

Si quisieramos aplicar una regla sobre un puerto y protocolo específico (sin utilizar macros) la declaramos de la siguiente forma:

```
ACCEPT          $FW     net             tcp     873
REJECT          $FW     net             udp     443
```

Para una lista detallada de los puertos y sus respectivos protocolos puedes ir aquí

En los logs, si tiene algún puerto que este bloqueado y necesitas saber cual es, lo puedes encontrar en los logs /var/log/messages, con el siguiente comando lo ves en el momento.

```
tail -f /var/log/messages
```

Para más información acerca de las reglas puedes leer man shorewall-rules.

Reglas para redireccionamiento de puertos (DNAT)

Las reglas que vimos anteriormente permiten realizar acciones (ACCEPT, DROP y REJECT) de filtrado de paquetes. Si queremos redireccionar puertos para que desde fuera (net) se pueda acceder a servicios de la red local (loc) lo podemos hacer utilizando reglas cuya acción es del tipo DNAT. Vamos a verlo con un ejemplo:

```
#ACTION     SOURCE     DEST                    PROTO     DEST     SOURCE     ORIGINAL
#                                                        PORT     PORT(S)    DEST
DNAT        net        loc:192.168.55.3:80 tcp       8080
```

- Para indicar que es una regla para redireccionamiento de puertos en la primera columna como acción ponemos DNAT
- En la segunda columna ponemos el origen de la petición en este caso net ya que pretendemos acceder desde el exterior a un servicio de la red local.
- En la tercera columna se especifica la máquina en la que esta el servicio que queremos redireccionar y el puerto del servicio al que queremos poder acceder, en este caso la máquina local 192.168.55.3 por el puerto 80 (servidor web)
- Cuarta columna protocolo de los paquetes TCP
- Quinta columna DEST PORT puerto al que acceden en la IP pública (puede ser el mismo o

no que el del servicio) en este caso el 8080.

Por tanto, las peticiones hechas al puerto 8080 de la IP pública del cortafuegos serán redireccionadas al servidor web que está en la máquina de la red local 192.168.55.3

Activar el enrutamiento

Shorewall viene configurado por defecto para mantener el estado actual del enrutamiento del equipo, si queremos que nuestro equipo cortafuegos haga de enrutador hemos de modificar la configuración de Shorewall:

```
#nano /etc/shorewall/shorewall.conf
```

Modificamos el siguiente parámetro a si:

```
IP_FORWARDING=Yes
```

Ultimos Pasos

Ahora los últimos toques, vamos a modificar el archivo de configuración de Shorewall:

```
#nano /etc/shorewall/shorewall.conf
```

Asegurense que los siguientes valores están correctos:

```
STARTUP_ENABLED=Yes

ROUTE_FILTER=Yes
```

Con STARTUP_ENABLED le decimos al Shorewall que inicie con el sistema, y con ROUTE_FILTER del cual hablamos ya arriba en la parte de Interfaces

y por ultimo, que fue un problema que me sucedió y que no lo dicen en todos los tutoriales de Debian o Ubuntu

cambiar la linea startup=0 por startup=1 del archivo **/etc/default/shorewall**

```
#nano /etc/default/shorewall
```

quedando de la siguiente forma

```
# prevent startup with default configuration
# set the following varible to 1 in order to allow Shorewall to start

startup=1

# if your Shorewall configuration requires detection of the ip address of a ppp
# interface, you must list such interfaces in "wait_interface" to get Shorewall
to
# wait until the interface is configured. Otherwise the script will fail
because
# it won't be able to detect the IP address.
#
# Example:
#    wait_interface="ppp0"
# or
#    wait_interface="ppp0 ppp1"
# or, if you have defined  in /etc/shorewall/params
#    wait_interface=
```

```
#
# Startup options
#

OPTIONS=""

# EOF
```

Para iniciar manualmente a Shorewall y probar nuestra configuración ejecutamos:

```
# shorewall start
```

Con esto nos dará algo parecido a esto:

```
Compiling...
Compiling /etc/shorewall/zones...
Compiling /etc/shorewall/interfaces...
Determining Hosts in Zones...
Preprocessing Action Files...
Compiling ...
   Pre-processing /usr/share/shorewall/action.Drop...
   Pre-processing /usr/share/shorewall/action.Reject...
Compiling /etc/shorewall/policy...
Adding Anti-smurf Rules
Adding rules for DHCP
Compiling TCP Flags filtering...
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...
Compiling ...
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:...
Compiling /etc/shorewall/routestopped...
Shorewall configuration compiled to /var/lib/shorewall/.start
Starting Shorewall....
Initializing...
Setting up Route Filtering...
Setting up Martian Logging...
Setting up Traffic Control...
Preparing iptables-restore input...
Running /sbin/iptables-restore...
IPv4 Forwarding Enabled
done.
```

Si dice **done** al final todo quedo bien y si nos da algún error debemos leer que nos indica y tratar de corregirlo.
Shorewall registra todo a través del log del sistema para ver los logs podemos ejecutar los siguientes comandos:

- **shorewall show log** (Muestra los últimos 20 mensajes de netfilter)
- **shorewall logwatch** (Verifica los logs a un tiempo determinado)
- **shorewall dump** (Nos da un amplio reporte de los problemas encontrados por Shorewall)