Configuración de Shorewall

Shorewall es una herramienta de alto nivel que permite configurar netfilter de una forma más cómoda que utilizando directamente netfilter.

Esta guía describe los pasos necesarios para llevar a cabo una configuración relativamente simple en la que se dispone de un equipo (que hará las veces de firewall) con dos interfaces de red, una conectada directamente a internet y la otra a una red local.

La primera de las interfaces está configurada en modo bridge debido a que en dicha máquina se ejecutan varias máquinas virtuales que utilizan dicha interfaz de red.

Por otro lado, la red local utiliza un rango de IP privadas, por lo que es necesario hacer enmascaramiento de IP para convertir dichas IP a la IP pública del firewall.

Instalación de Shorewall

Para la instalación descrita basta con instalar el paquete shorewall.

```
emerge -av shorewall
```

Configuración de Shorewall

Los archivos de configuración de Shorewall están en el directorio `/etc/shorewall`. Los ficheros que será necesario modificar son:

- `/etc/shorewall/zones`
- `/etc/shorewall/interfaces`
- `/etc/shorewall/policy`
- `/etc/shorewall/masq`
- `/etc/shorewall/shorewall.conf`

El fichero `zones` define las zonas sobre las que va a actuar Shorewall y su tipo. Para la configuración anterior necesitamos definir 3 zonas: la máquina en sí (`fw`), la red externa (`net`) y la red local (`loc`):

/etc/shorewall/zones

```
#############################################################################
########
#ZONE TYPE        OPTIONS        IN            OUT
#                 OPTIONS            OPTIONS
fw  firewall
net ipv4
```

```
loc ipv4
```

El fichero `interfaces` define las interfaces de red utilizadas por aquellas zonas que no son del tipo `firewall`:

/etc/shorewall/interfaces

```
#ZONE     INTERFACE        OPTIONS
net     br0            routeback,bridge
loc     eno2
```

El fichero `policy` define las políticas. El siguiente ejemplo permite prácticamente cualquier comunicación (la única que realmente se impide es el acceso desde la red externa a la local):

/etc/shorewall/interfaces

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

El fichero `masq` permite definir qué rango de IP deben ser enmascaradas al salir por una determinada interfaz (la siguiente configuración determina la IP pública de forma automática):

/etc/shorewall/masq

```
#############################################################################
#########################################
#INTERFACE:DEST        SOURCE        ADDRESS        PROTO    PORT(S)
IPSEC    MARK    USER/    SWITCH    ORIGINAL
#                                        GROUP        DEST
br0         192.168.0.1/24
```

Por último, en el fichero `shorewall.conf` hay que comprobar el valor de las siguientes líneas:

/etc/shorewall/shorewall.conf

```
STARTUP_ENABLED=Yes
```

```
IP_FORWARDING=On
```

La primera permite generar las reglas de filtrado y poner en marcha el cortafuegos. La segunda es para permitir el envío de tráfico procedente de una interfaz a la otra, y viceversa.

Probar la configuración

Es posible probar una determinada configuración durante un tiempo prudencial y revertir el cortafuegos a su estado anterior pasado dicho tiempo. De esta forma, si las reglas no son correctas, se podría volver a acceder a la máquina. Para probar las reglas en `/etc/shorewall` durante 10 segundos se puede ejecutar el comando:

```
shorewall try /etc/shorewall 10s
```

Lanzar el cortafuegos

Una vez probados todos los casos, se puede poner en marcha el cortafuegos de forma definitiva con:

```
/etc/init.d/shorewall start
```

Para añadirlo al arranque (openrc en Gentoo):

```
rc-update add shorewall
```

Configuración avanzada

El fichero `/etc/shorewall/policy` es el encargado de definir las reglas por defecto para la conexión entre zonas. Las excepciones a dichas reglas se definen en el fichero `/etc/shorewall/rules`.

Para cada conexión entrante primero se comprobarán las reglas en `rules` y en caso de no encontrarse ninguna coincidencia, se acudirá entonces a las reglas por defecto. La configuración ideal, al contrario de lo planteado en este documento, es que las reglas por defecto sean lo más restrictivas posibles y que se indique en el fichero `rules` solo aquellas conexiones que realmente se quieren permitir.

Se puede consultar cómo redactar dichas reglas en la documentación del fichero rules.

Referencias

- Introduction to Shorewall
- Getting started with Shorewall
- Shorewall quick start guides