

CAPÍTULO 14

Configuración de un Firewall

Una red nunca es segura; bajo esta premisa, si poseemos una red (o incluso si tenemos una única máquina conectada a Internet), debemos tomar todas las precauciones a nuestro alcance para impedir que los paquetes con código malicioso o no deseado circulen por ella.

Un cortafuegos o “firewall” es un dispositivo que filtra el tráfico entre dos o más redes; puede ser un dispositivo físico o un software que se ejecuta en un sistema operativo. Su funcionamiento se basa en una serie de reglas de filtrado, de manera que si se cumple una determinada regla se ejecute una determinada acción (por lo general aceptar el paquete o rechazarlo).

En Linux existe un cortafuegos incluido en todos los núcleos de la serie 2.4, denominado “netfilter”; la herramienta para manejarlo se denomina “iptables”, que es la que se utiliza para utilizar las reglas de filtrado. Todos los paquetes que pasen por nuestro Linux (ya sean creados internamente o provengan del exterior) serán comprobados por el cortafuegos (si está activado, evidentemente). Las acciones que puede tomar con los paquetes que pasan por él son DROP (descartar el paquete, con lo que éste desaparece) o ACCEPT (dejarle pasar y permitirle alcanzar el destino).

Hay que tener en cuenta que este filtrado de paquetes se realiza antes del control de acceso que ya hemos visto y para todos los paquetes de red (no sólo los servicios ejecutados a través de inetd con los archivos hosts.allow y hosts.deny), por lo que es una herramienta con una potencia y eficacia mayor al constituir la primera línea de defensa.

Otra utilidad del cortafuegos es que realiza operaciones de “ip_masquerading” o enmascaramiento IP, que es una técnica que permite la navegación a toda una red local con una única conexión a Internet sin necesidad de utilizar un servidor proxy; es una de las posibilidades que nos ofrece el sistema NAT (Network Address Translation, o Traducción de Direcciones de Red).

Configurar las reglas de un cortafuegos correctamente no es una tarea fácil, ya que requiere de amplios y profundos conocimientos del funcionamiento de la familia de protocolos TCP/IP. Además estas reglas

desaparecen al reiniciar la máquina, lo que obliga a tener que volver a introducirlas de nuevo; la solución para esto es escribir todas las reglas en un archivo y hacer que se ejecute en el arranque (a modo de servicio).

Afortunadamente tenemos una herramienta gráfica que hará nuestro trabajo más fácil; se trata de la “Configuración cortafuegos” en el menú Aplicaciones -> Herramientas del Sistema; esta herramienta se llama “lokkit” y se encarga de configurar las “iptables” sin tener que escribir ni una línea en la consola, tan sólo hay que responder una serie de preguntas. El programa está en castellano, así que es fácil realizar el proceso si tienes las ideas claras de cómo quieres configurar tu red o tu ordenador. Observa que en la primera pantalla te advierte que “No es un diseñador de cortafuegos para expertos”; esto no debe confundirte y hacerte creer que no es útil, sino que un experto preferirá introducir las reglas a mano; de todas formas verás que se pueden modificar las reglas configuradas por “lokkit” posteriormente.



La primera pregunta es la más difícil: hay que decidir si queremos una seguridad alta o baja (o no utilizar ninguna, pero ésta no es recomendable). La baja es recomendable en la mayoría de los casos ya que bloqueará la mayoría de los servicios y te permitirá utilizar muchas aplicaciones de Internet, mientras que la alta bloquea todos los accesos (tanto entrantes como salientes) salvo los que le especifiquemos; ésta es recomendable si piensas utilizar tu máquina como servidor de cara a Internet (si éste es tu caso deberías plantearte introducir las reglas a mano).

Selecciona entonces la “Seguridad Baja”; lo primero que te pregunta es si las interfaces de red encontradas son fiables o no, es decir, si pertenecen a la red local (que se supone libre de problemas) o a una conexión de Internet. Sigue el consejo de la pantalla y para la conexión a Internet selecciona que no; para el

resto depende de si quieres filtrarles el acceso a través de tu máquina o permitirles el paso.

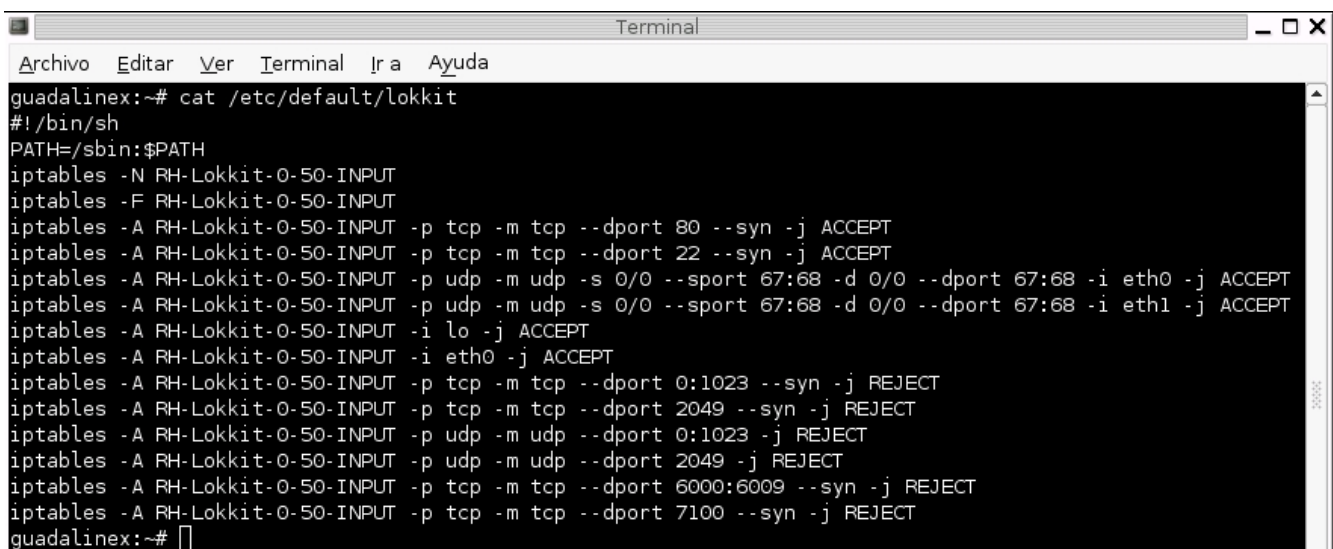
En la siguiente debes responder si tu máquina configura su dirección IP de forma dinámica, para que puedas comunicarte con el servidor y obtenerla (porque si la bloqueas no podrás utilizar la interfaz); la mayoría (no todos) de los proveedores de Internet proporcionan IPs dinámicas mediante DHCP, así que para la conexión a Internet responde que sí.

Ahora vas a tener que decidir si se podrá acceder a tu máquina desde el exterior, para seleccionar los servicios uno a uno. Ten en cuenta que hay servicios que puede ser buena idea permitirles acceso para usarlos tú mismo, así que lo más sensato es responder que sí.

Seguidamente “lokkit” va a reconocer los servicios de que dispones en tu máquina y te va a preguntar uno por uno si quieres permitir el acceso o no desde el exterior (desde tu propia red siempre podrás acceder a ellos). Por ejemplo puedes activar el servidor Web (si lo tienes configurado y listo para funcionar) y el ssh, pero no actives ni el SMTP ni el telnet.

La última pantalla advierte que debes tener cuidado, porque si activas el cortafuegos y estás accediendo de forma remota a tu máquina te puedes quedar sin acceso inmediato a ella; se supone que estás sentado delante del ordenador del que estás configurando el cortafuegos, así que pulsa “Terminar” para que se activen las reglas de filtrado y comenzar a utilizar el cortafuegos.

Otra de las ventajas de utilizar “lokkit”, a parte de lo fácil que ha sido hacerlo de forma gráfica, es que almacena las reglas en el archivo /etc/default/lokkit, para que estén disponibles en el caso de que el servicio “lokkit” sea ejecutado al iniciar la máquina; para el caso que hemos realizado aquí, puedes ver en la imagen las órdenes necesarias para crear las reglas.

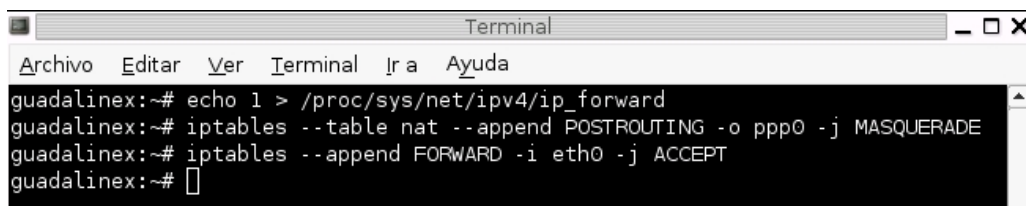
A terminal window titled "Terminal" with a menu bar (Archivo, Editar, Ver, Terminal, Ir a, Ayuda). The terminal shows the command `cat /etc/default/lokkit` and its output, which lists iptables rules for the RH-Lokkit-0-50-INPUT chain. The rules allow access to ports 80, 22, and 67:68 on both eth0 and eth1 interfaces, while rejecting access to ports 0:1023, 2049, 6000:6009, and 7100.

```
guadalinux:~# cat /etc/default/lokkit
#!/bin/sh
PATH=/sbin:$PATH
iptables -N RH-Lokkit-0-50-INPUT
iptables -F RH-Lokkit-0-50-INPUT
iptables -A RH-Lokkit-0-50-INPUT -p tcp -m tcp --dport 80 --syn -j ACCEPT
iptables -A RH-Lokkit-0-50-INPUT -p tcp -m tcp --dport 22 --syn -j ACCEPT
iptables -A RH-Lokkit-0-50-INPUT -p udp -m udp -s 0/0 --sport 67:68 -d 0/0 --dport 67:68 -i eth0 -j ACCEPT
iptables -A RH-Lokkit-0-50-INPUT -p udp -m udp -s 0/0 --sport 67:68 -d 0/0 --dport 67:68 -i eth1 -j ACCEPT
iptables -A RH-Lokkit-0-50-INPUT -i lo -j ACCEPT
iptables -A RH-Lokkit-0-50-INPUT -i eth0 -j ACCEPT
iptables -A RH-Lokkit-0-50-INPUT -p tcp -m tcp --dport 0:1023 --syn -j REJECT
iptables -A RH-Lokkit-0-50-INPUT -p tcp -m tcp --dport 2049 --syn -j REJECT
iptables -A RH-Lokkit-0-50-INPUT -p udp -m udp --dport 0:1023 -j REJECT
iptables -A RH-Lokkit-0-50-INPUT -p udp -m udp --dport 2049 -j REJECT
iptables -A RH-Lokkit-0-50-INPUT -p tcp -m tcp --dport 6000:6009 --syn -j REJECT
iptables -A RH-Lokkit-0-50-INPUT -p tcp -m tcp --dport 7100 --syn -j REJECT
guadalinux:~#
```

Aquí puedes ver la complejidad de la que hablaba antes; además el orden en el que se introducen las reglas es importante, y de cambiarlas podría hacer que algún paquete se “colara” en nuestro sistema. Hay quien dice que la configuración de un cortafuegos es un “arte” reservado a unos pocos privilegiados; de cualquier forma, para la mayoría de la gente no suele ser necesaria una configuración tan exhaustiva.

Para activar el “ip-masquerading” desgraciadamente debemos hacerlo a mano, aunque se pueden añadir las reglas al archivo /etc/default/lokkit (ten en cuenta que si ejecutar la herramienta de configuración deberás introducirlas de nuevo). En este caso además de crear un par de reglas debemos habilitar el reenvío de paquetes, lo que se realiza escribiendo un “uno” en el archivo apropiado (que puedes ver en la imagen); si este archivo no existe, es necesario recompilar el núcleo y activar la opción “ip_forwarding”.

Las dos reglas que necesitamos sirven la primera para enmascarar todos los paquetes y los encamine hacia la interfaz ppp0, mientras que la segunda sirve para aceptar los paquetes que vengan de la interfaz eth0 para que puedan ser reenviarlos.



```
Terminal
Archivo  Editar  Ver  Terminal  Ir a  Ayuda
guadalinux:~# echo 1 > /proc/sys/net/ipv4/ip_forward
guadalinux:~# iptables --table nat --append POSTROUTING -o ppp0 -j MASQUERADE
guadalinux:~# iptables --append FORWARD -i eth0 -j ACCEPT
guadalinux:~#
```

He supuesto que te conectas a Internet a través de un módem (ya sea módem convencional, ADSL o módem cable) que utiliza la interfaz ppp0 para acceder a Internet, y además tienes una tarjeta de red (eth0) para acceder a una red local. De esta forma todos los paquetes que lleguen a la máquina con este cortafuegos serán encaminados a través de Internet pero con la IP del cortafuegos, de manera que de cara al exterior no se tiene conocimiento de la red local; cuando los paquetes se reciben como respuesta a alguna petición, el sistema los reenvía a su destinatario.

Ejercicios

- 1) Configura el cortafuegos con un nivel seguridad alta
- 2) Saca una copia del archivo de configuración y llámalo /root/seg_alta
- 3) Configura el cortafuegos con un nivel de seguridad bajo

- 4) Saca una copia del archivo de configuración y llámalo /root/seg_baja
- 5) Observa las diferencias entre los dos archivos

Soluciones

- 2) `cp /etc/default/lokkit /root/seg_alta`
- 4) `cp /etc/default/lokkit /root/seg_baja`
- 5) Podrás observar cómo ambas configuraciones parecen muy complejas; si has respondido del mismo modo en ambos casos verá como en el caso del nivel alto las reglas son más restrictivas que en el otro caso.

