

El Día a Día del Administrador de Sistemas

FUERA DEL MURO

Si no tiene tiempo para trastear con reglas complicadas del cortafuegos, probablemente desee probar FireHOL.

POR CHARLY KÜHNAST

No hay mejor sitio que la casa de uno. Escucho un ruido algo apagado en el mueble de los trastos junto a la cocina. Al menos no suena muy fuerte hasta que abro la puerta. Cuando lo hago, me enfrento a algo con un sonido como el motor de un propulsor con problemas. Entre la lámpara de combustible, el abrillantador de zapatos y diversos estantes con tarros se encuentra la tecnología que me conecta con el mundo exterior. Junto a los modems proporcionados por mi compañía de telecomunicaciones y un asmático Cisco, que es el culpable de la mayor parte del ruido, se encuentra un PC desfasado, mi cortafuegos.

Originariamente mis reglas iptables se encargaban del enmascaramiento de las conexiones salientes de la LAN, con un par de reglas personalizadas para los servidores. Con el tiempo se han vuelto extremadamente complejas, y conforme lo hacían, me encontré a mí mismo buscando una herramienta para su gestión.

Finalmente encontré FireHOL [1]. En contraste con Firewall Builder [2], la herramienta FireHOL no

```

root@salami.kuehnast.com: /etc/firehol - Shell - Konsole
# Preparing for service 'ftp' of type 'server' under interface 'to-internet'
# Creating chain 'in_to-internet_ftp_s7' under 'in_to-internet' in table 'filter'
/sbin/iptables -t filter -N in_to-internet_ftp_s7
/sbin/iptables -t filter -A in_to-internet -j in_to-internet_ftp_s7
# Creating chain 'out_to-internet_ftp_s7' under 'out_to-internet' in table 'filter'
/sbin/iptables -t filter -N out_to-internet_ftp_s7
/sbin/iptables -t filter -A out_to-internet -j out_to-internet_ftp_s7
# Running complex rules function rules_ftp() for server 'ftp'
# Setting up rules for initial FTP connection server
/sbin/iptables -t filter -A in_to-internet_ftp_s7 -p tcp --sport 1024:65535 --dport ftp -m state --state NEW,ESTABLISHED -j ACCEPT
/sbin/iptables -t filter -A out_to-internet_ftp_s7 -p tcp --sport ftp --dport 1024:65535 -m state --state ESTABLISHED -j ACCEPT
# Setting up rules for Active FTP server
/sbin/iptables -t filter -A out_to-internet_ftp_s7 -p tcp --sport ftp-data --dport 1024:65535 -m state --state ESTABLISHED,RELATED -j ACCEPT
/sbin/iptables -t filter -A in_to-internet_ftp_s7 -p tcp --sport 1024:65535 --dport ftp-data -m state --state ESTABLISHED -j ACCEPT
# Setting up rules for Passive FTP server
/sbin/iptables -t filter -A in_to-internet_ftp_s7 -p tcp --sport 1024:65535 --dport 1024:65535 -m state --state ESTABLISHED,RELATED -j ACCEPT
/sbin/iptables -t filter -A out_to-internet_ftp_s7 -p tcp --sport 1024:65535 --dport 1024:65535 -m state --state ESTABLISHED -j ACCEPT
# > OK <
# FireHOL [router:to-internet] >

```

Figura 1: FireHOL reduce el esfuerzo de administración que implica la configuración del cortafuegos. Esta captura de pantalla muestra un fichero de control para una conexión FTP.

posee una interfaz gráfica de usuario. Por el contrario, hay que introducir directivas simples en un fichero de configuración y FireHOL se encarga de traducirlas a comandos iptables.

Si sólo se necesita enmascaramiento y se desea restringir el tráfico http, con esta simple configuración podrá obtenerse el resultado deseado:

```

interface eth0 home
    client all accept
interface eth1 internet
    client all accept
router to-internet 2
inface eth0 outface eth1
    masquerade
    route http accept

```

Las líneas *client all accept* permiten al cortafuegos establecer conexiones arbitrarias en la LAN y en Internet.

Para evitar restringir el enmascaramiento a http y abrir la puerta a cualquier protocolo, sólo hay que cambiar la última línea por:

```
route all accept
```

Basándose en esta directiva, FireHOL genera varias docenas de comandos iptables. Realiza un tratamiento especial para manejar protocolos complejos como FTP. La Figura 1 muestra parte del conjunto de reglas que se encargan de FTP.

FireHOL permite observar cómo trabaja, ofreciendo la función *explain* para facilitararlo. Se puede utilizar la consola interactiva para teclear las reglas en la sintaxis mostrada en el ejemplo y la herramienta responderá con la correspondiente regla iptables, que FireHOL aplicará si se le pide que lo haga.

Tras simplificar de forma considerable la gestión del cortafuegos de mi casa, ahora tengo tiempo para pensar en el ruido que sale del mueble de los trastos.

SYSADMIN

Snort60

Aprenda cómo localizar ataques con el sistema de detección de intrusiones Snort.

RECURSOS

[1] FireHOL: <http://firehol.sourceforge.net>

[2] Firewall Builder: <http://www.fvbuilder.org/>