Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

# Como montar un firewall paso a paso (I) (49830 lectures)

Per **Celso González**, ***PerroVerd*** (http://mitago.net)

Creado el 09/08/2002 15:37 modificado el 09/08/2002 15:37

*Este es el primero de una serie de artículos en los que iré explicando una serie de mecanismos útiles para proteger una máquina conectada a una red. El proposito de esta serie no es conseguir un firewall que funcione para todo el mundo, sino ir explicando las diferentes opciones y soluciones para ir resolviendo problemas.*

Aunque la mayor parte de este tutorial se va a centrar en iptables, la herramienta de filtrado de los kernels 2.4, vamos a empezar con una serie de cosas para las que no será necesario recompilar el kernel y son muy fáciles de probar.
Supongo que la gente tiene unos conocimientos básicos de redes, sabe hacer un script sencillo y manejar archivos de configuración.

Los kernels 2.4 permiten modificar determinados parámetros y variables dinamicamente a través del sistema de archivos /proc
Para poder cambiar estos valores tenemos que tener el kernel compilado con la opción CONFIG_SYSCTL, pero lo más probable es que si lo tengamos ya que viene marcada por defecto.

Para los ejemplos utilizaré esta configuración
Mi maquina firewall dispone de 2 tarjetas de red eth0 y eth1. eth0 es una red local a la que estan conectadas otras maquinas de mi oficina (en las que se supone que confio :), eth1 es la encargada de las comunicaciones con el exterior (internet) y en la que las restricciones son mayores. Las direcciones IP de estas tarjetas seran 192.168.0.1 para eth0 y una direccion 10.42.0.100 para eth1

## Evitar el spoofing

El spoofing consiste en modificar la dirección origen de un paquete de forma que la máquina que recibe el paquete se crea que proviene de una maquina de confianza, normalmente se usa 127.0.0.1
Por ejemplo, si yo soy un malo maloso y quiero atacar el firewall que estamos montando una forma de hacerlo sería haciendome pasar por uno de los equipos de la oficina de forma que utilizaría una dirección de tipo 192.168.0.x, como no estoy en la oficina esta petición entrará por eth1 y no por eth0, que es por donde debería venir como me muestra la tabla de rutas.

```
firewall:/# route
Kernel IP routing table
Destination  Gateway Genmask         Flags Metric Ref Use Iface
127.0.0.0       *     255.255.255.0   U     0      0     0 lo
192.168.0.0     *     255.255.255.0   U     0      0     0 eth0
10.42.0.0       *     255.255.0.0     U     0      0     0 eth1
default         *     0.0.0.0         U     0      0     0 eth1
```

El kernel de linux viene con un mecanismo de protección que implementa lo especificado en el RFC1812, para habilitarlo haremos lo siguiente:

```
firewall:/# for x  in /proc/sys/net/ipv4/conf/*; do
>              echo "1" > $x/rp_filter
>              done
```

Esta opción es **muy recomendable**

## Activar o desactivar el reenvío de paquetes

La decisión depende del uso que vayamos a dar a nuestra máquina:
Si la máquina va a servir de router para dar acceso a varios ordenadores de nuestra red local, por ejemplo, debemos activar el reenvio de paquetes.

```
firewall:/# echo "1" > /proc/sys/net/ipv4/ip_forward
```

Si nuestra máquina está sola **debemos** desactivar el reenvío de paquetes ya que nos estamos exponiendo a servir de puente para otras maquinas.

```
firewall:/# echo "0" > /proc/sys/net/ipv4/ip_forward
```

Esta opción es **muy recomendable**

## Desactivar source routed packets

Un paquete source routed (no se como traducir esto) es un paquete IP que especifica la ruta que debe usar el paquete por la red. De esta forma se puede intentar hacer creer que el paquete procede de una red de confianza. En fin, un rollo, los detalles los podeis ver en esta página(1).
Lo importante de esto es que este tipo de paquetes no se suelen utilizar nunca excepto para malos propósitos :)

```
firewall:/# echo "0" > /proc/sys/net/ipv4/conf/all/accept_source_route
```

Esta opción es **recomendable**

## Desactivar ICMP redirigidos

Un ICMP redirido se emplea para avisar al receptor que tiene que omitir algo de su tabla de rutas. Normalmente se emplea para informar que una ruta no es optima y cual es la nueva ruta a seguir. Esta opción posibilita a un atacante alterar la tabla de rutas del firewall a sus necesidades.

```
firewall:/# echo "0" > /proc/sys/net/ipv4/conf/all/accept_redirects
```

Esta opción es **recomendable**

## Habilitar protección contra mensajes erróneos

Esta opcion se emplea normalmente para evitar llenar los logs con mensajes inutiles. Algunos routers envian respuestas "extrañas" a la hora de responder a broadcasts y pueden llegar a aburrirnos con una gran cantidad de logs registrados.

```
firewall:/# echo "1" > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses
```

Esta opción es **indiferente**

## Evitar actuar de amplificador en un ataque Smurf

Esta opción se emplea para evitar responder a peticiones de broadcast. Si respondemos a estas peticiones podemos ser utilizados para generar un ataque de denegación de servicio contra otra máquina.

```
firewall:/# echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
```

Esta opción es **recomendable**

## Decidir si logeamos a los marcianos

Los marcianos son paquetes que no pueden venir de este mundo, normalmente paquetes spoofeados o erroneos. Puede

ser útil guardar un registro de estos paquetes pero pasa lo mismo que con los bogus que podemos cansarnos de verlos en los logs.

```
firewall:/# echo "1" > /proc/sys/net/ipv4/conf/all/log_martians
```

Esta opción es **indiferente**

Y con esto terminamos por hoy, únicamente indicar que en la mayoría de distribuciones hay scripts que asignan estos valores de forma automatica en el arranque (*/etc/sysctl.conf* y */etc/network/options*)

Para el que quiera ampliar esto puede mirar en:
/usr/src/linux/Documentation/sysctl/README
y en
/usr/src/linux/Documentation/networking/ip-sysctl.txt

---

**Lista de enlaces de este artículo:**

1. http://csrc.nist.gov/publications/nistpubs/800-10/node25.html

---

E-mail del autor: celso _ARROBA_ mitago.net